DEFENDING DATA PRIVACY CLASS ACTION LITIGATION

Excerpted from Chapter 26 (Data Privacy) of
E-Commerce and Internet Law: A Legal Treatise With Forms, Second Edition,
a 4-volume legal treatise by Ian C. Ballon (Thomson/West Publishing 2015)

SANTA CLARA UNIVERSITY LAW PRESENTS

"HOT TOPICS IN INTERNET, CLOUD, AND PRIVACY LAW"

SANTA CLARA UNIVERSITY LAW SCHOOL
APRIL 23, 2015

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:
1900 University Avenue, 5th Fl.
East Palo Alto, CA 914303
Direct Dial: (650) 289-7881
Direct Fax: (650) 462-7881

Los Angeles:
1840 Century Park East
Los Angeles, CA 90067
Direct Dial: (310) 586-6575
Direct Fax: (310) 586-0575

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

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2015 Annual Update), a 4-volume legal treatise by Ian C. Ballon, published by West LegalWorks Publishing, 395 Hudson Street, New York, NY 10014, (212) 337-8443, www.ianballon.net.

GT GreenbergTraurig

Ian C. Ballon

Shareholder
Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
JD, LLM, CIPP

Ballon@gtlaw.com
Google+, LinkedIn, Twitter, Facebook: Ian Ballon

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 represents Internet, technology, and entertainment companies in copyright, intellectual property and Internet litigation, including the defense of privacy and behavioral advertising 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 4-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) and serves as Executive Director of Stanford Law School's Center for E-Commerce.

Mr. Ballon, who practices in both Silicon Valley and LA, has brought or defended novel suits involving computer software, user generated content, rights in the cloud and in social media, links, frames, sponsored links, privacy and security, database protection, screen scraping and content aggregation, digital music, the Digital Millennium Copyright Act, rights of privacy and publicity, the enforceability of Internet Terms of Use and Privacy Policies and preemption under the CDA. A list of recent cases may be found at www.GTLaw.com/People/IanCBallon.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2013 edition of Best Lawyers in America. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award and named new media lawyer of the year in 2012 by the Century City Bar Association. 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 and Top 100 lawyers in California and is consistently listed as a top Northern California and Southern California litigator. Mr. Ballon also holds the CIPP certificate for 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. All of these developments,

[37] *See supra* § 26.13[6].

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 liability 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

senger data.[3]

---

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 claim, 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 (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

More recent cases have focused 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.[4]

In 2010, for example, a number of suits were brought al-

---

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 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., Opperman v. Path, Inc.*, Case No. 13-CV-00453-JST, 2014 WL 1973378 (N.D. Cal. May 14, 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); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434 (D. Del. 2013) (granting defendants' motions to dismiss allegations that defendants "tricked" users' internet browsers into accepting "cookies" which allowed defendants to track users' internet activities and communications and display targeted advertising); *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); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011) (dismissing ECPA and state law claims arising out of the alleged transmission of personal information about users from a social network to third party advertisers); *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).

leging 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]

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 of-

---

[5]In contrast to browser cookies, flash cookies may 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 Clearsrpring 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 alleged use of flash cookies to store a user's browsing history). The *Specific Media* case ultimately was dismissed by the plaintiff.

fer 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).

Plaintiffs' counsel typically sue under statutes that authorize prevailing parties to recover statutory damages and attorneys' fees, since actual damages are *de minimis* or nonexistent. Consequently, many of these suits are brought in federal court under federal statutes that provide for statutory damages or attorneys' fee awards (or both). Putative privacy class action suits have been brought under the Electronic Communications Privacy Act (ECPA),[9] 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,[10] which like ECPA, is largely an anti-hacking statute. Some suits also have been brought under the Video Privacy Protection Act.[11] 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)[12] as the basis for federal subject matter jurisdiction. In the absence of injury or damage,

---

[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).

[9]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].

[10]18 U.S.C.A. § 1030; *supra* § 26.09; *see generally infra* § 44.08.

[11]18 U.S.C.A. § 2710; *see generally supra* § 26.13[10].

[12]28 U.S.C.A. § 1332(d).

however, many of these cases may not survive in federal court.

To have standing to bring suit in federal court, a plaintiff must have suffered an "injury in fact," which must be (a) "concrete and particularized" and (b) "actual or imminent, not conjectural or hypothetical."[13] To establish injury in fact, "allegations of possible future injury are not sufficient."[14] The threatened injury must be "certainly impending. . . ."[15] In addition to showing injury in fact, (1) a plaintiff must 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

---

[13]*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 an Article III federal court therefore 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*, 131 S. Ct. 2355, 2362–63 (2011).

[14]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (2013) (internal quotation marks omitted).

[15]*Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1146-47 (2013); *see generally infra* § 27.07 (analyzing *Clapper* in connection with security breach putative class action suits); *see also infra* § 27.07 (analyzing *Clapper* and discussing standing in the context of data security suits).

by a favorable decision."[16] In short, standing depends on a showing of injury in fact, causation and redressability.[17] 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.[18]

A number of privacy-related putative class action suits have been dismissed for lack of standing. In many cases—particularly those involving alleged behavioral advertising practices[19] the failure to provide notice[20] or other alleged

---

[16]*Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal citations and quotations omitted); *see also Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1147 (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*).

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

[18]*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).

[19]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 440-42 (D. Del. 2013) (granting defendants' motions to dismiss where plaintiffs alleged that defendants "tricked" users' internet browsers into accepting "cookies" which allowed defendants to track users' internet activities and communications and display targeted advertising; holding that plaintiffs did not allege injury-in-fact sufficient to confer Article III standing); *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 referrer 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 alleging 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).

[20]*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 stand-

privacy violations[21]—there simply is no injury from the complained of activity. Even in data breach cases, standing may be an issue if there has been no allegation of injury.[22]

---

ing), *aff'd mem.*, 554 Fed.Appx. 654 (9th Cir. 2014); *see generally supra* § 26.13[6][D] (analyzing section 1798.83 and cases construing it).

[21]*See, e.g.*, *In re Science Applications International Corp. (SAIC) Backup Tape Data that Theft Litigation*, __ F. Supp. 2d __, 2014 WL 1858458 (D.D.C. May 9, 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 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 company thanking him for applying for a loan were sufficient to demonstrate causation; and (7) allegations that 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); *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)).

[22]*See, e.g.*, *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*, 132 S. Ct. 2395 (2012); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092-95 (N.D. Cal. 2013) (dismissing

Where standing has been established in putative privacy class action suits, it is usually because a plaintiff can show entitlement to monetary damages[23] or at least that sensitive personal data has been compromised which increases the risk of future harm,[24] although a minority of courts may find standing merely based on the allegation of breach of a federal[25] or even state[26] statute that does not require a show-

---

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 data security putative class action cases).

[23]*See, e.g.*, *Perkins v. LinkedIn Corp.*, __ F. Supp. 2d __, 2014 WL 2751053 (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).

[24]*See, e.g.*, *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 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); *Doe I v. AOL*, 719 F. Supp. 2d 1102, 1109–11 (N.D. Cal. 2010) (finding injury in fact where a database of search queries was posted online containing AOL members' names, social security numbers, addresses, telephone numbers, user names, passwords, and bank account information, which could be matched to specific AOL members); *see generally infra* § 27.07 (analyzing standing in data security putative class action cases).

[25]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434 (D. Del. 2013) (granting defendants' mo-

ing of damage or injury to state a claim, based on Ninth

---

tions to dismiss; holding that plaintiffs did not allege injury-in-fact sufficient to confer Article III standing, but because a statutory violation, in the absence of any actual injury, may in some circumstances create standing under Article III, the court addressed whether plaintiffs had pled sufficient facts to establish a plausible invasion of the rights created by the various statutes asserted, concluding ultimately that plaintiffs failed to state claims under the ECPA, CIPA, CCL, CLRA, and the California Constitution, in addition to failing to allege the threshold loss of $5,000 required by the CFAA); *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 referrer 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 "intercepted, disclosed, or intentionally used," and does not require any further injury).

[26]*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).

Circuit law.[27]

---

[27]Courts in the Sixth, Eighth and Ninth Circuits will find standing where a plaintiff alleges a violation of a statute that does not require a separate showing of actual damage, but courts in the Fourth and Federal Circuits may not absent separate injury-in-fact. *See generally infra* § 27.07 (analyzing standing in the context of data security cases).

In *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed*, 132 S. Ct. 2536 (2012), the Ninth Circuit 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) (distinguishing *ACLU v. NSA*, 493 F.3d 644, 648 (6th Cir.2007), *cert. denied*, 552 U.S. 1179 (2008), where the Sixth Circuit found that plaintiffs lacked standing on similar facts, because *ACLU* was decided on a more developed record on summary judgment, whereas *Jewel* was decided on a motion to dismiss and a plaintiff's well pleaded allegations are deemed true in evaluating Rule 12 motions); *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); *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 have construed *Edwards* and *Jewel* as requiring that even where a plaintiff states a claim under a federal statute that does not require a showing of damage, plaintiffs must 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

Less commonly, Article III standing also may be established based on invasion of a constitutional right.[28]

Even where a plaintiff has standing, claims based on al-

---

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 take 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, do not accept the proposition that alleging an injury-in-law by stating a claim and establishing statutory standing to sue satisfies the standing requirements of Article III. *See David v. Alphin*, 704 F.3d 321, 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 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.").

The U.S. Supreme Court had granted *certiorari* in *Edwards* to decide the issue of standing, but then dismissed the appeal based on the determination that certiorari had been improvidently granted. *See Edwards v. First American Corp.*, 132 S. Ct. 2536 (2012).

In October 2014, the U.S. Supreme Court solicited input from the Solicitor General on whether to grant Spokeo's petition for *certiorari* in *Robins v. Spokeo, Inc.*, 742 F.3d 409 (9th Cir. 2014).

[28]*See 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).

leged data privacy violations may not fit well into existing federal statutes.

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.[29]

In behavioral advertising 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, however, is not considered the *contents* of a communication, which is defined under ECPA as "information concerning the substance, purport, or meaning of that communication."[30] On this basis alone, claims premised on disclosure will not be actionable

---

[29]*See infra* §§ 44.06, 44.07.

[30]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 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); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 443-44 (D. Del. 2013) (explaining that URLs and "personally identifiable information that is automatically generated by the communication" is not "contents" for the purposes of the Wiretap Act); *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."); *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)."); *U.S. v. Parada*, 289 F. Supp. 2d 1291, 1304 (D. Kan. 2003) (denying a criminal motion to suppress evidence on the basis that phone numbers stored on a cell phone were not the contents of a communication that could be unlawfully intercepted or disclosed under 18 U.S.C.A. § 2511 because "mere phone numbers that are recorded because a third party pulsed in a number from their phone are not communications" whereas "the contents would be the substance of the conversation"); *Hill v. MCI WorldCom Communications, Inc.*, 120 F. Supp. 2d 1194, 1195–96 (S.D. Iowa 2000) (holding that electronically stored phone records, including "names, addresses, and phone numbers of parties [the plaintiff] called," do not constitute the contents of communications under ECPA); *see generally infra* § 50.06[4] (analyzing contents and non-contents under ECPA in greater detail and discussing additional cases).

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 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)). This analysis, however, is either incomplete or incorrect. *See infra* § 50.06[4][B] (analyzing the case). A plaintiff should not be able to unilaterally expand the scope of protection afforded by ECPA by characterizing non-content records as the contents of a communication. Alternatively, the court's order denying the defendant's motion to dismiss may be viewed as one where the court applied a lax pleading standard, where later in the litigation the plaintiff would have to establish that Pandora only had access to this non-content data by virtue of accessing a stored communication where the data was recorded, which seems unlikely.

under either Title I or Title II.[31]

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 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.

Behavioral advertising claims premised on unauthorized *interception*[32] under Title I have failed where there has been no interception[33] or no interception by the defendant.[34] Collecting user data such as a customer's requested URL, the

---

[31]For similar reasons, claims 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). *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); *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 *17 (D.N.J. July 2, 2014) (dismissing with prejudice plaintiffs' CIPA claim because allegations that Google placed cookies to intercept data could not state a claim where the alleged interception did not involve the contents of any communication); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 444-45 (D. Del. 2013) (dismissing Wiretap and CIPA claims because plaintiffs' allegations did not demonstrate that Google intercepted any contents or meaning).

[32]*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).

[33]*See, e.g.*, *Opperman v. Path, Inc.*, No. 3:13-cv-00453-JST, 2014 WL 1973378, at *29 (N.D. Cal. May 14, 2014) (dismissing Wiretap Act claim based on a 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

referer[IB1] URL (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.[35]

The Stored Communications Act, which is Title II of ECPA,

---

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 claim on the same grounds as 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); *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).

[34]*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*, 133 S. Ct. 2743 (2013).

[35]*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*, 133 S. Ct. 2743 (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).

prohibits both unauthorized access (or exceeding authorized access) in section 2701,[36] subject to exceptions for access by the person or entity providing a wire or electronic communications service[37] and by a user of that service with respect to a communication of or intended for that user;[38] and knowingly divulging the contents of a communication while in electronic storage in section 2702,[39] subject to exceptions including to an addressee or intended recipient of such communication,[40] where authorized[41] and with lawful consent.[42] 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."[43] However, a provider of an electronic communication service may divulge the contents of a communication to an addressee or intended recipient of such communication.[44] 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.[45] In *In re Facebook Privacy Litigation*,[46] 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

---

[36]18 U.S.C.A. § 2701(a).

[37]18 U.S.C.A. § 2701(c)(1).

[38]18 U.S.C.A. § 2701(c)(2).

[39]18 U.S.C.A. § 2702(a).

[40]18 U.S.C.A. § 2702(b)(1).

[41]18 U.S.C.A. § 2702(b)(2).

[42]18 U.S.C.A. § 2702(b)(3).

[43]18 U.S.C.A. § 2702(a)(1).

[44]18 U.S.C.A. § 2702(b)(1).

[45]18 U.S.C.A. § 2702(b)(3).

[46]*In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011).

> 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).[47]

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.[48]

In *Low v. LinkedIn Corp.*,[49] 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 advertisement 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).[50] 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

---

[47] *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713–14 (N.D. Cal. 2011) (footnote omitted).

[48] *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).

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

[50] 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).

were not sent to LinkedIn by plaintiffs for storage or processing.[51]

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."[52] "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, . . ."[53] 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 provided" within the meaning of the Stored Communications Act.[54]

Similarly, behavioral advertising claims premised on information stored on user devices will suffer 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 ac-

---

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

[52]18 U.S.C.A. § 2701(a)(1).

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

[54]*See, e.g.*, *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.

cess), 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 . . . ."[55] *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."[56] Where the information accessed is stored on a user's device (such as a cookie[57] or universally unique device identifier (UUID)[58] used in connection with advertising or email stored on a user's own computer[59] or personal email stored on a Blackberry mobile device[60]), the information is not in *electronic storage* as defined in the Act.[61]

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

---

[55]18 U.S.C.A. § 2701(a).

[56]18 U.S.C.A. § 2510(17).

[57]*See, e.g.*, *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"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1058–59 (N.D. Cal. 2012); *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).

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

[59]*See, e.g.*, *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1204–05 (S.D. Cal. 2008).

[60]*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.").

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

these facilities could be accessed by hackers."[62] 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."[63] 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."[64] 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).[65] For purposes of ECPA, consumers or other *end users* are not the *users* referenced by the statute.[66] In the nomenclature of the statute, end users, or consumers, are referred to as *customer*

---

[62]*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).

[63]18 U.S.C.A. § 2701(c)(2).

[64]18 U.S.C.A. § 2510(13).

[65]*See, e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1060 (N.D. Cal. 2012) (holding that "because the communications [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).

[66]*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:

or *subscribers*.[67]

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.[68] 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.[69]

Courts have dismissed putative privacy class action suits where consent was inferred from TOU or a Privacy Policy.[70]

In contrast to Title II, Title I addresses communications in

> 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).

[67] *See infra* § 50.06[4] (analyzing ECPA in greater detail).

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

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

[70] *See, e.g.*, *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 Ad-

transit (or temporary, intermediate storage). In *In re iPhone Application Litigation*,[71] 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

---

ditional Terms of Service for Yahoo Mail and Yahoo Messenger agreement); *Perkins v. LinkedIn Corp.*, __ F. Supp. 2d __, 2014 WL 2751053, at *13-15 (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); *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*, 133 S. Ct. 2743 (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); *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 declining 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). Consent also may be relevant to the issue of class certification. *See, e.g.*, *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.").

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

electronic transmission . . .” of an electronic communication.[72]

Title I claims also may fail where they are brought over information that is “readily accessible to the general public,”[73] such as material posted on a website[74] 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 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.”[75]

Given the number of parties involved in behavioral 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, at least not under Title I.[76]

---

[72]18 U.S.C.A. § 2510(17).

[73]*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 . . . .”).

[74]*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).

[75]*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).

[76]*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) (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

To state a civil claim for a CFAA violation, a plaintiff must allege $5000 in damages,[77] which is a threshold that bars many 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.[78] Courts also have been reluctant to treat

---

"does not impose civil liability on aiders or abettors."), *cert. denied*, 133 S. Ct. 2743 (2013); *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 liability, 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].

[77]18 U.S.C.A. §§ 1030(c)(4)(A)(i), 1030(g). A civil CFAA claim where $5,000 in damages 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).

[78]*See, e.g., also In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 447-48 (D. Del. 2013) (granting defendants' motions to dismiss, including a claim brought under the CFAA for failure to allege the threshold loss of $5,000 required to state a civil claim under the CFAA); *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. C11-366-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 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

the disclosure of personal information as having economic value,[79] at least in the absence of any evidence to the contrary.

To state a CFAA claim, a plaintiff also must establish that a defendant accessed a protected computer "without authorization" or "exceeded authorized access."[80] At least in the 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.[81]

Authorization similarly may be difficult to show in some

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).

[79]*See, e.g.*, *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 please 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.").

[80]18 U.S.C.A. § 1030(a)(4); *see generally infra* § 44.08[1] (analyzing the CFAA in greater detail).

[81]*See WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831 (2013); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*); *infra* § 44.08[1] (analyzing this issue in greater detail).

data privacy cases where the plaintiff voluntarily downloaded the application that is challenged in the litigation.[82]

In *In re iPhone Application Litigation*,[83] 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.[84]

Claims under the Video Privacy Protection Act may be brought against a "video tape service provider who knowingly discloses, to any person, personally identifiable information" about the consumer.[85] 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 . . . ."[86] The Senate Report accompanying the bill clarifies that "similar audio visual materials" include such things as "laser discs, open -reel movies, or CDI technol-

---

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

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

[84]*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.").

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

[86]*See* 18 U.S.C.A. § 2710(a)(4).

ogy . . .,"[87] which was a technology for delivering movies on CD-like disks. All of these *materials* involve video stored on tangible media. Nevertheless, a magistrate judge allowed one VPPA behavioral advertising putative class action suit to proceed in an unreported opinion against Hulu,[88] while in a separate action against Netflix, where the applicability of the statute was not disputed, the court dismissed plaintiff's claims because any disclosure by Netflix was made to the subscriber herself, not to third parties who she may have allowed to access her account, or, in the alternative, Netflix's conduct in displaying a list of recently viewed videos could not be characterized as a knowing violation in light of Netflix's clear disclosure in its privacy statement that subscribers themselves were responsible for maintaining the confidentiality of their account information and for restricting access to devices through which they accessed their Netflix accounts.[89]

Because alleged cloud-based privacy concerns do not fit well within the confines of anti-hacking statutes or other narrow federal privacy statutes, plaintiffs' lawyers may seek federal jurisdiction under the Class Action Fairness Act (CAFA).[90] 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 million 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.[91]

State law claims may suffer from some of the same defects

---

[87]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.

[88]*In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2012 WL 3282960 (N.D. Cal. Aug. 10, 2012).

[89]*Mollett v. Netflix, Inc.*, No. 5:11-CV-01629-EJD, 2012 WL 3731542 (N.D. Cal. Aug. 17, 2012); *see generally supra* § 26.13[10] (analyzing *Hulu, Netflix* and the VPPA, including more recent case law, in greater detail).

[90]28 U.S.C.A. § 1332(d).

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

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.[92]

Indeed, 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, the California Legal Remedies Act,[93] 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.[94] A CLRA claim therefore may not be maintained

---

[92]*See, e.g.*, *Svenson v. Google Inc.*, __ F. Supp. 2d __, 2014 WL 3962820, at *4-5 (N.D. Cal. Aug 12, 2014) (dismissing plaintiff's breach of contract claim for failing to sufficiently allege damage); *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 Facebook Privacy Litig.*, 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); *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" go assert such a claim).

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

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

where a plaintiff seeks a remedy from a free Internet site or free app where no purchase has been made.[95] 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.[96]

Claims under California's Invasion of Privacy Act[97] or the California Constitution[98] likewise will not be actionable, as under ECPA, if premised on non-content data, as opposed to

---

[95]*See In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 451 (D. Del. 2013) (rejecting the argument that plaintiff's personal information constituted a form of payment to Google; dismissing plaintiffs' claim); *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 Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011) (dismissing with prejudice a CLRA claim based on an alleged privacy violation); *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 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).

[96]*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); *see also In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 450-51 (D. Del. 2013) (rejecting the argument that Google's advertising constituted a "service" and not software; dismissing plaintiffs' claim).

[97]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).

[98]*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).

the contents of communications.[99]

Similarly, California's notoriously-broad unfair competition statute requires a showing of actual injury. That statute—California Business and Professions Code section 17200[100]—allows claims to be based on violations of statutes that do not expressly create independent causes of action.[101] 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.' "[102] 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 such unfair competition."[103] Hence, a plaintiff generally may not maintain suit for privacy violations where the plaintiff

---

[99]*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); *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 *17 (D.N.J. July 2, 2014) (dismissing with prejudice plaintiffs' CIPA claim because allegations that Google placed cookies to intercept data could not state a claim where the alleged interception did not involve the contents of any communication); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 444-45 (D. Del. 2013) (dismissing Wiretap and CIPA claims because plaintiffs' allegations did not demonstrate that Google intercepted any contents or meaning).

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

[101]*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].

[102]*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)).

[103]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

obtained access to the defendant's service free of charge[104] unless the claim may be premised on the value of a product purchased in conjunction with obtaining free services.[105] 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.[106]

---

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).

[104]*See 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 Facebook Privacy Litig.*, 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, holding that "[b]ecause Plaintiffs allege that they received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim."); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' CFAA 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).

[105]*See Svenson v. Google Inc.*, __ F. Supp. 2d __, 2014 WL 3962820, at *10 (N.D. Cal. Aug 12, 2014) (dismissing plaintiff's breach of contract claim, noting that "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."); *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 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).

[106]*See, e.g.*, *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,

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.[107] False advertising claims under California law[108] likewise will be dismissed where a plaintiff cannot show that it has suffered injury in fact and lost money or property.[109] Similarly, a claim under

---

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").

[107]*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).

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

[109]*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

California's Computer Crime law[110] is only actionable where a plaintiff can show "damage or loss."[111]

Common law privacy claims may be difficult to assert in data privacy cases absent an ability to characterize the alleged intrusion as highly offensive to a reasonable person,[112] as opposed to merely *de minimis*.

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."[113]

---

met the threshold requirement of showing a loss of money or property, where neither could allege reliance on the allegedly false advertisements or misrepresentations).

[110]Cal. Penal Code § 502.

[111]Cal. Penal Code § 502(e); *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); *see generally infra* § 44.09 (analyzing section 502).

[112]*See In re Nickelodeon Consumer Privacy Litigation*, Case No. 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 *18-19 (D.N.J. July 2, 2014) (dismissing plaintiffs' invasion of privacy claim under New Jersey law where the plaintiffs had not demonstrated why Google's "collection and monetization of online information," including the use of cookies to acquire or intercept IP addresses and URLs, would be "highly offensive" to a reasonable person).

[113]*In re SAIC Corp.*, __ F. Supp. 2d __, 2014 WL 1858458, at *9 (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., 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

Some claims also suffer because of efforts to shoehorn novel privacy theories into existing unfair competition, statutory or common law remedies. For example, in *Steinberg v. CVS Caremark Corp.*,[114] 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[115] places no restrictions on the use of information once de-identified.[116] Plaintiffs' unfair competition and unjust enrichment claims were dismissed based on the lack of any value to the information, among other grounds.[117]

A claim for common law trespass generally requires a showing of substantial impairment, not merely unauthorized access.[118] For this reason, plaintiffs in putative behavioral advertising privacy class action suits may have difficulty stating a claim even where unauthorized access is alleged.[119]

Where a plaintiff cannot state a claim under ECPA

---

be "actually viewed."); *Harper v. 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).

[114]*Steinberg v. CVS Caremark Corp.*, Civil Action No. 11-2428, 2012 WL 507807 (E.D. Pa. Feb. 16, 2012).

[115]45 C.F.R. §§ 160.103, 164.502(d)(1) to 164.502(d)(2); *supra* § 26.11.

[116]*See Steinberg v. CVS Caremark Corp.,* Civil Action No. 11-2428, 2012 WL 507807, at *6–7 (E.D. Pa. Feb. 16, 2012).

[117]*See Steinberg v. CVS Caremark Corp.,* Civil Action No. 11-2428, 2012 WL 507807, at *8–9 (E.D. Pa. Feb. 16, 2012).

[118]*See, e.g.*, *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).

[119]*See, e.g.*, *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

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 privacy premised on the same unauthorized access.[120] Privacy

---

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.").

[120]*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

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[121] or unique mobile device identifier numbers, personal data and geolocation information.[122]

A plaintiff may be unable to state a claim for common law claim for unjust enrichment, 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 permits the collection, use or dissemination of personal information.[123] A

---

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).

[121]*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.").

[122]*See 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).

[123]*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

state law conversion claim may suffer the same defect.[124] 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.[125]

Although not analyzed to date in a data privacy case,

---

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").

[124]*See, e.g.*, *In re Sony Gaming Networks and Customer Data Security Breach Litigation,* Civil Case Nos. 11CV2119, 11CV2120, 2012 WL 4849054, at *23 (S.D. Cal. Oct. 11, 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).

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

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).[126]

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[127] or zip code data[128] or the sale of de-identified personal information.[129]

Under California law, it is no longer clear that a separate claim may even be asserted for unjust enrichment, which

---

[126]*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).

[127]*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. 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).

[128]*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).

[129]*See Steinberg v. CVS Caremark Corp.,* Civil Action No. 11-2428, 2012 WL 507807, at *9 (E.D. Pa. Feb. 16, 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).

since 2011 courts have characterized as a request for restitution, not a separate cause of action under California law.[130] Other states, such as New Jersey, similarly to do not recognize unjust enrichment as a separate cause of action.[131]

California likewise does not recognize a separate cause of action for restitution, which is a remedy that a plaintiff may elect, not a claim.[132]

Even negligence claims may be difficult to sustain in the absence of economic injury.[133] Negligence generally requires 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).[134] To state a claim, a plaintiff in a data privacy case generally must show an "appreciable, nonspeculative, present

---

[130]*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., 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 a claim for unjust enrichment, finding there is no longer any such cognizable claim under California law).

[131]*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).

[132]*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).

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

[134]*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).

injury."[135] Further, in most states, purely economic losses generally are not recoverable as tort damages.[136] A negligence claim also may 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.[137]

---

[135]*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).

[136]*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 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) (dismissing plaintiffs' negligence and negligence *per se* claims under the economic loss rule in a security breach putative class action suit).

[137]*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

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 therefore unascertainable,[138] or involve numerous individualized inquiries 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.*,[139] 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.[140]

---

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).

[138] *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).

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

[140] *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).

Similarly, in *In re Google Inc. Gmail Litigation*,[141] 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 provided consent.

On the other hand, in *Harris v. comScore,*[142] 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.

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 defendant 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.[143] 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 standing to sue for a privacy policy violation.[144]

Likewise, where there is a security breach and resulting

---

[141]*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).

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

[143]*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).

[144]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.*, *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).

harm, a plaintiff may be able to state a claim.[145]

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.[146] The Act provides for statutory damages in cases where violations may be shown.

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.[147] The exemption, however, does not apply, among other things,

---

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).

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

[146]*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).

[147]*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).

to the federal Electronic Communications Privacy Act[148] "or any similar State law."[149]

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.[150] While certification of a liability 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.[151]

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 an Internet 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.*

---

[148]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]).

[149]47 U.S.C.A. § 230(e)(4).

[150]*See, e.g.*, *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); *Kim v. Space Pencil, Inc.*, No. C 11-03796 LB (N.D. Cal. Nov. 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).

[151]*See supra* § 25.07[2].

Concepcion[152] 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.[153]

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 plaintiffs' counsel from even moving for class certification.[154] Judges, however, closely scrutinize unilateral contracts with consumers and will not enforce arbitration provisions if assent to the proposed agreement has been obtained[155] 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.[156]

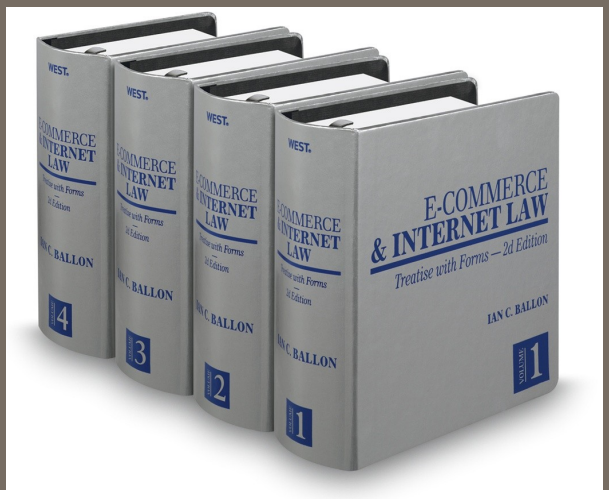
The law governing arbitration agreements and class action waivers in unilateral contracts is analyzed in section 22.05[2][M] and chapter 56. How to draft an arbitration provision to maximize its enforceability is separately considered in section 22.05[2][M][vi].

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.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS,2D 2015

Ian C. Ballon

The most comprehensive authority available on digital media, the cloud, mobile, social media Internet and e-commerce law



THOMSON REUTERS™

TAKE YOUR INTERNET AND MOBILE PRACTICE TO THE NEXT LEVEL

E-Commerce & Internet Law is a comprehensive, authoritative work covering business-to-business and business-to-customer issues, regulatory issues, and emerging trends. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to more than 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 four sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Privacy, Security 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
- Liability of Internet and Mobile Sites and Services (Including Social Networks and Blogs)
- Civil Jurisdiction and Litigation

Questions to Answer as Internet law moves to mobile devices, social media and the cloud:

- Does content syndication to mobile providers take a service provider outside the DMCA?
- How does text marketing differ from email marketing?
- Privacy issues when dealing with users who are subject to COPPA or teenagers not subject to COPPA but subject to heightened concern
- Facebook and Twitter contacts as the basis for personal jurisdiction
- How to obtain substitute service over a foreign defendant in an Internet dispute

Key Features of E-Commerce & Internet Law

- The only treatise to comprehensively and exhaustively cover the liability of Internet and mobile service providers, cloud storage providers, bloggers, and owners and operators of social networks and other Web 2.0 applications
- Substantial caselaw coverage on Terms of Use and Internet contracts to help you draft better agreements, with sample forms and provisions
- Latest caselaw and analysis on sponsored links, key word sales, and liability for search engine optimization practices
- Includes coverage on enforcing judgments against domain names and the extent to which even unrelated claims against foreign defendants could be satisfied in U.S. courts
- Rethinking consumer criticism, gripe site, blog, and fan site law in light of new Lanham Act and CDA caselaw (including a checklist for evaluating potential claims and their viability)
- Comprehensive analysis of state law security breach notification statutes, together with practical tips on how to prepare for and respond to security breaches
- Extensive data on the prices paid for domain names and how to value them
- How to draft Privacy Policies, Terms of Use, and other documents and conduct website and privacy audits
- Practical tips, checklists, forms, and helpful information that goes well beyond what is usually included in a legal treatise
- Glossary terms drawn from the latest caselaw (helpful for briefs and contract definitions)
- Practical strategies for effectively documenting Internet transactions, drafting forms, and devising winning litigation strategies
- Exhaustive DMCA guidelines, CDA analysis, and strategies for managing user content
- Most thorough and clear cut analysis of Internet jurisdiction available anywhere
- Clear, concise, comprehensive and practical analysis

SUMMARY OF CONTENTS

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

Chapter 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. Using the Internet in Your Legal Practice: Online Resources and Strategies

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Database Protection and Screen Scraping
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names
8. Internet Patents

Volume 2

Chapter 10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Protection and Misappropriation

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: UCITA, the UETA, Federal Legislation and the EU Distance Sales Directive
16. Internet Licenses: Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements
24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

Part IV. Privacy, Security and Internet Advertising

25. Introduction to Consumer Protection in Cyber space
26. Data Privacy

Volume 3

Chapter 27. Internet, Network and Data Security
28. Advertising in Cyberspace
29. Spamming, Email Marketing and the Law of Unsolicited Commercial Email
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. Taxation of Electronic Commerce
34. Antitrust Restrictions on the Conduct of Electronic Commerce
35. State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression In Cyberspace

Volume 4

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

Chapter 40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Soft ware and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email
46. Identity Theft
47. Civil Remedies for Unlawful Seizures

Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Website Owner and Service Provider Liability for User Generated Content and User Misconduct
50. Strategies for Managing Third-Party Liability Risks
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

Part X. Civil Jurisdiction and Litigation

52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation
58. Email and other Electronic Communications in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client

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

NEW IN THE 2015 EDITION

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Mr. Ballon, who is admitted to practice in California, the District of Columbia and Maryland and in the U.S. District Court for the District of Colorado, represents companies in copyright, trademark, trade secret, right of publicity, privacy and security and other Internet-related cases and in defense of data privacy, security, TCPA, advertising and Internet and mobile class action suits.

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 Daily Journal as one of the Top 75 Intellectual Property litigators and Top 100 lawyers in California.

Mr. Ballon 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 was recognized by the Los Angeles and San Francisco Daily Journal in 2009 for obtaining the third largest plaintiff's verdict in California in 2008 in MySpace, Inc. v. Wallace, which was one of several cases in which he served as lead counsel that created important precedents on the applicability of the CAN-SPAM Act, California's anti-phishing statute and other laws to social networks.

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. certification from the International Association of Privacy Professionals.

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 Google+, Twitter and LinkedIn (@IanBallon).

Contributing authors: Ed Chansky, Emilio Varanini , Tucker McCrady, Parry Aftab and Josh Raskin

- Exhaustive coverage of the latest law and trends in data privacy, data security, TCPA and CAN-SPAM Act litigation (including class action litigation) – the most comprehensive available anywhere!
- The U.S. Supreme Court's decision in *Aereo* and its impact on public performance and direct liability case law (and the continuing validity of *Cartoon Network* in light of *Aereo*)
- New standards for false advertising law based on the U.S. Supreme Court's 2014 opinions
- Patent law in light of *Alice* and other new U.S. Supreme Court opinions (updated by Joshua Raskin)
- Exhaustive circuit-by-circuit, claim-by-claim and fact pattern analysis of the CDA, 47 U.S.C. § 203(c) – the most comprehensive available anywhere!
- Understanding the TCPA, how it differs from the CAN-SPAM Act and whether and to what extent FCC rules and guidelines impact laws and litigation governing text marketing.
- The interplay between the DMCA, the CDA and other safe harbors, defenses and exemptions available to cloud service providers, operators of social networks, mobile providers, app developers and app store hosts, service providers and employer-owned computer networks.
- The parameters of federal preemption of right of publicity and other IP claims under the Telecommunications Act.
- The latest analysis on the interplay between Internet, cloud and mobile business and antitrust law (updated by Emilio Varanini)
- New sections addressing the common law copyright issues for sound recordings in digital media and California's law prohibiting sites and services from restricting user criticism
- Updated analysis of state security breach laws in the 48 states that have them and in D.C., Puerto Rico and Guam – analyzed holistically the way a practitioner would, rather than merely by chart or graph.
- Music licensing (updated by Tucker McCrady)
- Latest law and practice on how to draft, enforce and litigate Terms of Use agreements and privacy policies for websites and mobile devices
- Complete analysis of security breach case law, statutes and trends
- Mobile, Internet and social media contests and promotions (updated by Ed Chansky)
- Latest law on sponsored links, database protection, screen scraping and search engine optimization
- Complete, updated catalogue of state statutes governing state security breach notification laws, email marketing and online dating
- Latest case law on subpoenaing data from internet, mobile and social network sites and what is permissible under ECPA and state statutory and common law privacy laws
- Hundreds of new and recent cases and FTC data privacy, security and COPPA enforcement actions and settlements
- The most comprehensive authority available on the law of digital media, the cloud, mobile and social media law as well as e-Commerce and internet law.