DEFENDING DATA PRIVACY CLASS ACTION LITIGATION

Excerpted from the 2022 update to Chapter 26 (Data Privacy)
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)
(These excerpts are unrevised page proofs for the current update and may contain errors)

ADVANCED DATA PRIVACY, CYBERSECURITY BREACH AND AI CLASS ACTION LITIGATION DEFENSE STRATEGIES AND COMPLIANCE LESSONS

PRIVACY + SECURITY FORUM
MAY 8-10, 2024

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:	Washington, D.C.:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900	2101 L Street, N.W., Ste. 1000
East Palo Alto, CA 914303	Los Angeles, CA 90067	Washington, D.C. 20037
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575	Direct Dial: (202) 331-3138
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575	Fax: (202) 331-3101

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

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
a 5-volume legal treatise by Ian C. Ballon
www.ianballon.net

GT GreenbergTraurig

Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

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

Ballon@gtlaw.com
LinkedIn, Facebook, Threads, BlueSky: IanBallon

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

Los Angeles
1840 Century Park East
Suite 1900
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Washington, D.C.
2101 L Street, N.W.
Suite 1000
Washington, DC 20037
T 202.331.3138
F 202.331.3101

Ian Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents companies in the defense of data privacy, AdTech, and cybersecurity breach class action suits and IP and technology litigation.

Ian has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2024, 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and has been included on the *Daily Journal's* annual list of the Top 100 Layers in California. In 2024, 2023, 2022, 2021, 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards for winning a series of TCPA cases. In addition, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. He has also been 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 has been recognized as one of the Top 75 intellectual property litigators in California by the *Los Angeles and San Francisco Daily Journal* in every year that the list has been published (2009 through 2024). He was also listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" (2012), was recognized as one of the top 100 lawyers in L.A. by the *Los Angeles Business Journal* and is both a Northern California and Southern California Super Lawyer and by Thomson Reuters as a Stand-Out Lawyer (in 2024) based on client nominations.

Ian is also the author of the leading treatise on internet and mobile law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of data privacy and cybersecurity breach issues, and a novel transactional approach to handling security breaches and trends in data privacy, cybersecurity breach and CCPA class action suits. 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). In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Mr. Ballon previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 3

THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

- Registered users should be given notice when they first log-on after a new policy has been posted
- Problems may arise if later practices are inconsistent with commitments made at the time information was collected.

Internal Implementation

- Have adequate internal record-keeping procedures been established to ensure that adequate documentation exists of the particular version of the policy in effect on a given date, in the event of litigation or a regulatory action?
- Have adequate internal (and possibly external) compliance procedures been put in place to ensure that employees are educated about the company's obligations under the policy and assure that the policy in fact is followed?
- Have adequate contract administration procedures been adopted to ensure that third-party contracts comply with California and other state laws (if personally identifying information is to be transferred to third parties)?[46]
- Have adequate procedures been put in place to conduct periodic privacy and security audits to ensure the continued accuracy of the policy (and make appropriate adjustments or revisions over time)?
- What internal mechanisms have been put in place to ensure that the policy is revised as practices change? Will the Legal Department receive notice when new marketing, business practices or technologies are implemented?

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

[46] *See supra* § 26.13[6].

resulted 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. Subsequent disclosures about Cambridge Analytica and others also focused Congressional attention on internet and mobile businesses and their data collection practices. With the advent of the pandemic in 2020-2021, and its impact on brick and mortar businesses, even more attention has been focused by plaintiffs' lawyers on Internet and mobile businesses. All of these developments, in turn, have created greater press attention and consumer awareness of privacy issues.

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

---

[Section 26.15]

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

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-

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

senger data.[3]

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

---

plaintiffs to amend their complaint to assert a Wiretap Act claim); *see also In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (following *Toys R Us* in permitting plaintiffs to aggregate their individual damages under the CFAA to reach the $5,000 threshold).

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

[4]*See, e.g., In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015) (affirming dismissal of plaintiffs' federal Wiretap Act, Stored Communications Act, and Computer Fraud and Abuse Act claims and claims for violation of the California Invasion of Privacy Act (CIPA), California's Consumers Legal Remedies Act (CLRA), the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200), and the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502), but holding that plaintiffs stated claims under the California Constitution and California tort law), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608-09 (9th Cir. 2020) (affirming dismissal of plaintiffs' Stored Communications Act claim because the copy of the URL shown in a user's toolbar was wholly separate from the GET requests that Facebook allegedly duplicated and forwarded to its servers—and was made available solely for the user's convenience—and therefore not stored "incident to transmission" and not

In 2010, for example, a number of suits were brought alleging that flash cookies[5] were being used to "re-spawn" data

---

in *electronic storage*, while reversing dismissal of Wiretap Act, CIPA and other claims), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (affirming in part, reversing in part dismissal of claims arising out of the alleged transmission of personal information about users from a social network to third party advertisers); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal Apr. 1, 2015) (dismissing claims under the Stored Communications Act over alleged sharing of users' personal information with app vendors, but allowing breach of contract, breach of the implied duty of good faith and fair dealing and unfair competition claims to proceed); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962 (N.D. Cal. 2015) (granting in part, denying in part, defendants' motion to dismiss relating to the transfer of data from user's mobile address books to defendants when users selected the "Find Friends" feature to connect with friends on social networks); *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836 (N.D. Cal. 2014) (denying defendant's motion to dismiss ECPA and CIPA claims, but dismissing plaintiffs' UCL claim); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' CLRA and intrusion upon seclusion claims against Google for allegedly disclosing user data to third parties, but allowing claims for breach of contract and fraudulent business practices under the UCL to proceed); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014) (dismissing all of plaintiffs' claims against all defendants with leave to amend, with the exception of the claim for common law intrusion upon seclusion; plaintiffs alleged that the defendant's apps had been surreptitiously accessing and disseminating contact information stored by customers on Apple devices); *Yunker v. Pandora Media, Inc.*, No. 11–CV–03113 JSW, 2014 WL 988833 (N.D. Cal. Mar. 10, 2014) (dismissing with prejudice plaintiff's privacy claim under the California Constitution but denying defendant's motion to dismiss plaintiff's breach of contract claim premised on Pandora's alleged breach of its privacy policy and plaintiffs' UCL claims); *Del Vecchio v. Amazon.com, Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit for Computer Fraud and Abuse Act and state unfair competition, unjust enrichment and trespass claims based on the alleged use of browser and flash cookies); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) (dismissing for lack of Article III standing, with leave to amend, a putative class action suit against Apple and various application providers alleging misuse of personal information without consent); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice all claims against the advertising defendants and CFAA and most other claims against the remaining defendant in a suit alleging the use of flash cookies and browser sniffing); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) (dismissing with leave to amend a putative class action suit brought over the alleged use of flash cookies to store a user's browsing history).

[5]In contrast to browser cookies, flash cookies may be used in conjunc-

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 Adtech practices, among other types of cases, generally involve, at most, theoretical violations where no economic 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-

---

tion with flash media players to record information such as a user's volume preference, as a persistent identifier or for other purposes. *See supra* § 26.03.

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

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

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

Plaintiffs' counsel typically try to sue under statutes that authorize prevailing parties to recover statutory damages and attorneys' fees, since actual damages typically are *de minimis* or non-existent in most of these cases. Consequently, suits often are brought in federal court under federal statutes that provide for statutory damages or attorneys' fee awards (or both), where it also may be easier for plaintiffs' class action lawyers to justify larger settlements based on nation-wide classes.[9] Putative data privacy class action suits have been brought under the Electronic Communications Privacy Act (ECPA),[10] which in Title I (also known as the Wiretap Act) proscribes the intentional *interception* of electronic communications and in Title II (also known as the Stored Communications Act) prohibits unauthorized, intentional *access* to stored information. Plaintiffs also have sued under the Computer Fraud and Abuse Act,[11] which like ECPA, is largely an anti-hacking statute. Suits also have been brought under the Video Privacy Protection Act.[12] Claims additionally potentially may be asserted under state

---

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

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

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

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

law for breach of contract based on alleged breach of privacy policies and terms of use, under state computer crime statutes, for common law privacy claims or for unfair competition, where plaintiffs assert supplemental jurisdiction or jurisdiction under the Class Action Fairness Act (CAFA)[13] as the basis for federal subject matter jurisdiction. In the absence of injury or damage, however, many of these cases may not survive in federal court because injury typically is required to establish standing and is an element of many potential claims.

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

To have standing to sue in federal court under Article III

---

[13]28 U.S.C.A. § 1332(d).

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

[15]Some BIPA cases have addressed standing in this context, where the case had been removed from state court by the defendant, and once in federal court the defendant moved to dismiss for lack of statutory standing (so that the case would be dismissed) but did not want to argue, based on the same facts, that the court lacked Article III jurisdiction, in which case the suit would have been remanded back to state court. The plaintiff, in turn, may not want to argue that there was Article III standing, because the plaintiff would have preferred to have the case remanded to state court, and instead argued that the burden of establishing Article III standing was on the defendant when the case had been removed to federal court by the defendant. As observed by one court,

> Procedurally, Howe finds himself in an awkward position. To succeed in his lawsuit, he must establish that he is a "person aggrieved" who has statutory standing to assert a cause of action under BIPA. However, if he has a cognizable injury under BIPA, then it follows that he also has constitutional standing and must proceed in a disfavored forum. Therefore, in an effort to achieve remand without fatally undermining his claims, Howe declines to take a position on constitutional standing and argues that it is Defendants' burden to establish such standing. . . .
>
> To avoid remand, Defendants find themselves having to establish that Howe has suffered a sufficient injury for purposes of Article III standing even as their motion to dismiss vigorously contests the adequacy of his injury for purposes of statutory standing. Yet it is possible for Defendants to thread this needle. Constitutional standing and statutory standing are distinct inquiries. . . . And a plaintiff may well have Article III standing to maintain an action, but nonetheless lack statutory standing because the statute under which he or she

is suing does not supply a cause of action to individuals in the plaintiff's position. *See Thompson v. N. Am. Stainless, LP*, 562 U.S. 170, 178 (2011).

Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541, at *3-4 (N.D. Ill. May 31, 2018) (citations omitted) (remanding the case back to state court); *see also Thornley v. Clearview AI, Inc.*, 984 F.3d 1241, 1242, 1244 (7th Cir. 2021) (observing, in affirming remand of plaintiffs' BIPA claim for lack of Article III standing, that "Oddly, Thornley insists that she lacks standing, and it is the defendant, Clearview AI, Inc., that is championing her right to sue in federal court. That peculiar line-up exists for reasons that only a civil procedure buff could love: the case started out in an Illinois state court, but Clearview removed it to federal court. Thornley wants to return to state court to litigate the BIPA claims, but Clearview prefers a federal forum. . . . Ordinarily, it is the plaintiff who bears the burden of demonstrating that the district court has subject-matter jurisdiction over her case and that it falls within 'the Judicial Power' conferred in Article III. But more generally, the party that wants the federal forum is the one that has the burden of establishing the court's authority to hear the case."); *id.* at 1249 (Hamilton, J. concurring) (observing, in concurring with Judge Wood's opinion affirming remand, for lack of standing, that "our decision has been determined by the choices that these plaintiffs have made to narrow both their claims and the scope of their proposed class. Judge Wood's opinion recognizes that other plaintiffs might well establish standing for other alleged violations of Section 15(c)."); *Hazlitt v. Apple Inc.*, 543 F. Supp. 3d 643, 2021 WL 2414669, at *4-6 (N.D. Ill. 2021) (holding that Apple, in opposing plaintiffs' motion to remand, met their burden to establish standing over plaintiffs' section 15(a) claim but not with respect to their 15(c) claim); *Goings v. UGN, Inc.,* No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018) (following *Howe* in remanding plaintiff's suit alleging BIPA violations and common law negligence back to state court for lack of Article III standing, where plaintiff was aware that he was providing his biometric data to defendants and did not claim that defendants further disclosed it, and where, as in *Howe,* the defendant challenged only statutory standing to preserve its ability to stay in federal court but those arguments "cast doubt" on the basis for Article III standing); *Roberts v. Dart Container Corp.,* No. 17 C 9295, 2018 WL 3015793, at *1 (N.D. Ill. Mar. 12, 2018) (remanding to state court plaintiff's BIPA claim where the defendant had removed plaintiff's case to federal court and then promptly filed a Rule 12(b)(1) motion to dismiss for lack of standing; "To say that the current state of affairs regarding the issues at hand is a legal and logical mire would be an understatement. . . . Because the parties are in "agreement" that subject-matter jurisdiction is lacking, the Court remands the case . . . ."); *Barnes v. ARYZTA, LLC,* 288 F. Supp. 3d 834, 836-39 (N.D. Ill. 2017) (remanding plaintiff's BIPA suit to state court where the defendant failed to meet its burden of establishing Article III standing in a case it removed to federal court; "On the one hand, Plaintiff seeks remand to the state court and therefore does not want to argue to this Court it has sustained a concrete injury-in-fact because then it would be conceding subject matter jurisdiction in federal court. Defendant, on the other hand, would like to argue that Plaintiff has not sustained an Article III injury but has withdrawn any argument to that effect in a ploy to avoid being forced out of federal court. The difference between the two

of the U.S. Constitution, a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision.[16] In data privacy cases, which frequently involve alleged technical violations with no resulting economic harm, standing determinations frequently turn on whether a plaintiff has suffered an "injury in fact," which must be (a) "concrete and particularized" and (b) "actual or imminent, not conjectural or hypothetical."[17] To establish injury in fact, "allegations of possible future injury are not sufficient."[18] Where standing is based on the risk of a future injury, the threatened injury must be "certainly impending . . . ."[19] Moreover, while the material risk of future harm may satisfy the concrete-harm requirement in

---

parties is that Plaintiff does not have to take a position on the standing issue while Defendant does, because Defendant bears the burden of establishing jurisdiction in this Court."); *see generally supra* § 26.13[12][A] (analyzing BIPA).

[16]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021); *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

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

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

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

[19]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409-10 (2013);

connection with a claim for injunctive relief if the risk of harm is sufficiently imminent and substantial, the mere risk of future harm, without more, is insufficient to establish concrete harm to justify standing in a suit for damages (unless the exposure to the risk of future harm itself causes a *separate* concrete harm).[1]

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 by a favorable decision."[20] In short, standing depends on a showing of injury in fact, causation and redressability.[21] Where standing cannot be established, a putative class action suit will be dismissed.

Prior to certification of any putative class, standing must be established based on the named plaintiffs that actually filed suit, not unnamed putative class members.[22]

A number data of privacy putative class action suits and

---

see generally infra § 27.07 (analyzing *Clapper* in connection with security breach putative class action suits).

[1] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210-11 (2021); *see generally infra* § 27.07[2][B] (analyzing *Ramirez*).

[20] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal citations and quotations omitted); *see also Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.' "; *quoting Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149-50 (2010)); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180–81 (2000) (applying the same standard as *Lujan*); *see also Thole v. U. S. Bank N.A.*, 140 S. Ct. 1615, 1618 (2020) ("To establish standing under Article III of the Constitution, a plaintiff must demonstrate (1) that he or she suffered an injury in fact that is concrete, particularized, and actual or imminent, (2) that the injury was caused by the defendant, and (3) that the injury would likely be redressed by the requested judicial relief.").

[21] *Katz v. Pershing, LLC*, 672 F.3d 64, 71–72 (1st Cir. 2012) (explaining *Lujan*). Nominal damages may satisfy the requirement for redressability. *See Uzuegbunam v. Preczewski*, 141 S. Ct. 792, 797-802 (2021) (holding that "a request for nominal damages satisfies the redressability element of standing where a plaintiff's claim is based on a completed violation of a legal right.").

[22] *See, e.g.*, *Simon v. Eastern Kentucky Welfare Rights Org.*, 426 U.S.

claims have been dismissed for lack of standing. In many cases—particularly those involving alleged user tracking and behavioral advertising and AdTech practices[23] the fail-

---

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)); *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).

In *TransUnion LLC v. Ramirez,* 141 S. Ct. 2190 (2021), the Supreme Court held that, where a class has been certified, "[e]very class member must have Article III standing in order to recover individual damages." *Id.* at 2208. The Court declined to address whether every class member must demonstrate standing before a court certifies a class (*id.* n.4), but plainly the prosepect that, as in *Ramirez*—where the majority of the class was determined to lack standing following trial on the merits—potential standing issues have implications for typicality, adequacy of representation, predominance. manageability, and the definition of a proposed class, among other issues that courts must grapple with under Rule 23 in ruling on motions for class certification. Since standing may be raised at any time during the litigation, and must exist at all times, and for all claims and for each form of relief sought (*id.* at 2207-08; *Uzuegbunam v. Preczewski,* 141 S. Ct. 792, 796 (2021)), standing may play an even greater role in class certification decisions than it did prior to *Ramirez*. *See generally infra* § 27.07[2][B] (analyzing *Ramirez* in greater detail and in connection with cybersecurity breach putative class action suits).

[23]*See, e.g.*, *Revitch v. New Moosejaw, LLC*, Case No. 18-cv-06827-VC, 2021 WL 2371974 (N.D. Cal. June 10, 2021) (dismissing claims against NavisStone over the alleged use of replay software to track user activity, for lack of Article III standing; "For NaviStone's code to track a user's clickstream data, it must place a cookie on that user's web browser. That cookie is both essential to tracking data and an artifact of the code's operation: if the cookie is not on the user's browser, the code did not run. The only possible caveat is that the cookie might have been deleted after the fact, but Revitch has not produced any evidence that that happened and has stated that he has not deleted any cookies from his browser."); *Bernardino v. Barnes & Noble Booksellers, Inc.*, 17-CV-04570 (LAK) (KHP), 2017 WL 3727230, at *5-6 (S.D.N.Y. Aug. 11, 2017) (recommending that plaintiff's motion for a preliminary injunction under the Video Privacy Protection Act be denied for lack of Article III standing); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *8-16 (N.D. Cal. Dec. 21,

2016) (granting summary judgment in favor of Google on plaintiff's individual claims for breach of contract, breach of the duty of good faith and fair dealing and unfair competition under California law, for lack of standing, based on evidence presented by the parties); *In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *3-6 (N.D. Cal. Mar. 26, 2013) (rejecting diminution in the value of plaintiffs' PII, diminished battery capacity, overpayment or costs incurred as grounds to show injury-in-fact to sustain Article III standing, but holding plaintiffs had standing to assert a claim under the California Constitution and for statutory violations); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (granting defendant's motion to dismiss claims for fraudulent misrepresentation, negligent misrepresentation, public disclosure of private facts, actual and constructive fraud, breach of contract and unjust enrichment, for lack of standing, with leave to amend, in a putative class action suit based on the defendant's alleged practice of including the search terms employed by a user in the URL for the search results page displayed in response to a search query, allegedly causing that information to be visible to advertisers in the referer header when a user clicks on an advertiser's link from the results page, but denying the motion with respect to plaintiffs' Stored Communications Act claim); *Low v. LinkedIn Corp.,* No. 11-cv-01468-LHK, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011) (granting defendant's motion to dismiss, for lack of standing, with leave to amend, a putative privacy class action suit based on alleged privacy violations stemming from the alleged disclosure of personally identifiable browsing history to third party advertising and marketing companies where plaintiff was unable to articulate what information of his, aside from his user identification number, had actually been transmitted to third parties, or how disclosure of his anonymous user ID could be linked to his personal identity); *Cohen v. Facebook, Inc.*, No. C 10-5282 RS, 2011 WL 5117164 (N.D. Cal. Oct. 27, 2011) (dismissing with prejudice plaintiffs' statutory right of publicity claims over the use of the names and likenesses of non-celebrity private individuals without compensation or consent in connection with Facebook's "Friend Finder" tool, for failing to allege injury sufficient to support standing, where plaintiffs could not allege that their names and likenesses had any general commercial value and did not allege that they suffered any distress, hurt feelings, or other emotional harm); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) (dismissing for lack of Article III standing, with leave to amend, a putative class action suit against Apple and various application providers 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). *But see In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597-601

ure to provide notice[24] or other alleged privacy violations[25]—

(9th Cir. 2020) (holding that plaintiffs had Article III standing to assert claims for invasion of privacy, intrusion upon seclusion, breach of contract, breach of implied contract, breach of the covenant of good faith and fair dealing, as well under the Wiretap Act and CIPA because they adequately alleged privacy harms, and for common law trespass, fraud, statutory larceny, and violations of the CDAFA, in a suit alleging that an app provider accessed user browsing history from third party apps, when they were logged out of the app, prior to 2011), *cert. denied*, 141 S. Ct. 1684 (2021).

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

[25]*See, e.g.*, *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 681-83 (N.D. Cal. 2021) (dismissing claims alleging that Apple disclosed private information without consent in violation of various privacy laws, based on a newspaper article in the *Guardian*, which did not plausibly suggest that *all* Apple devices were subject to accidental triggers and review by third party contractors and where plaintiffs alleged no facts to suggest that their own private communications were intercepted by accidental triggers; "Plaintiffs' claims of statutory privacy harm rest on an attenuated chain of possibilities that (1) their iPhones were accidentally triggered at some point, (2) the accidental triggers occurred in a context where Plaintiffs had a reasonable expectation of privacy, and (3) (for some claims) Plaintiffs' communications were part of the "small portion" of recordings sent to third party contractors. Absent factual allegations regarding the rate of accidental triggers on devices that Plaintiffs actually own, as well as their *particular* use of those devices in contexts where they had a reasonable expectation of privacy, the injury remains too speculative for Article III standing."); *McCollough v. Smarte Carte, Inc.*, Case No. 16 C 03777, 2016 WL 4077108, at *3-5 (N.D. Ill. Aug. 1, 2016) (dismissing plaintiff's putative Illinois Biometric Information Privacy Act class action suit for lack of Article III and statutory standing where the plaintiff alleged that Smarte Carte retained her fingerprint biometric information without written consent, where Smarte Carte used a person's fingerprints to allow them to access a rented locker, because '[e]ven without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, the Court finds it difficult to imagine, without more, how this retention could work a concrete harm" and she could not establish that she was "aggrieved by" the alleged violation, to establish statutory standing); *Frezza v. Google Inc.,* No. 5:12-cv-00237, 2013 WL 1736788 (N.D. Cal. Apr. 22, 2013) (dismissing claims for breach of contract and breach of implied contract over Google's alleged failure to implement Data Security Standards (DSS) rules in connection with promotions for Google Tags; distinguishing cases where courts found standing involving the disclosure of personal information, as opposed to mere retention of data, as in *Frezza*);

there simply has been no injury from the complained of activity. This may be especially true where the information at issue is publicly available.[1] Needless to say courts have been finding standing in many cases (as discussed later in this section).

Even in security breach cases, standing may be an issue if there has been no allegation of injury (although there presently is a split of authority over whether the mere apprehension of future injury (such as the risk of future identity theft) is sufficiently concrete and particularized to establish standing in a case where there has been a security breach but no actual identity theft or other adverse use of the information—some courts have held that it is not,[26] while others will

---

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)).

[1] *See, e.g.*, *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *4-5 (N.D. Cal. Mar. 1, 2021) (dismissing plaintiffs' putative California right of publicity class action claim, arising out of defendant's use of high school yearbook photos and related information in its subscription database, for lack of Article III standing, because (1) "the information in the Yearbook database is not private: it is public yearbook information distributed to classmates (and ultimately to Ancestry). Ancestry's using the public profiles to solicit paying subscribers—standing alone—does not establish injury." (2) plaintiffs did not have a commercial interest in their public profiles that precluded Ancestry's use of the profiles for commercial gain; and (3) Cal. Civ. Code § 3344 requires a showing of injury, not mere use and distribution, as alleged).

[26] *See, e.g.*, *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295, 299-305 (2d Cir. 2021) (affirming dismissal for lack of Article III standing in a case where the defendant accidently sent an email to all of its approximately 65 employees attaching a spreadsheet containing sensitive PII (including Social Security numbers, homes addresses, birth dates, phone numbers, educational degrees, and dates of hire) of approximately 130 then-current and former employees, where plaintiffs failed to allege that their PII was subject to a targeted data breach or allege any facts suggesting that their PII (or that of any others) was misused, and hence failed to allege that they were at a substantial risk of future identity theft

or fraud sufficient to establish Article III standing); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017) (affirming that the plaintiff lacked standing to sue for breach of implied contract and under N.Y. Gen. Bus. L. § 349 where she alleged that she made purchases via a credit card at a Michaels store prior to Michaels' security breach and that thereafter fraudulent charges were attempted, but she did not allege that any fraudulent charges were actually incurred by her, and she did not allege with any specificity that she spent time or money monitoring her credit); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011) (affirming dismissal for lack of standing and failure to state a claim, noting that particularly "[i]n data breach cases where no misuse is alleged, . . . there has been no injury," and that "[a]ny damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker."), *cert. denied*, 566 U.S. 989 (2012); *Hutton v. National Board of Examiners in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018) (finding standing where plaintiffs had had Chase Amazon Visa credit card accounts opened in their names, but reaffirming the principles that "incurring costs for mitigating measures to safeguard against future identity theft may not constitute an injury-in-fact when that injury is speculative . . . ."); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (holding that patients at a Veterans Affairs hospital who sued alleging that their personal information had been compromised as a result of two data security breaches did not have standing because an enhanced risk of future identity theft was too speculative to cause injury in fact and the allegations were insufficient to establish a substantial risk of harm); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763 (8th Cir. 2017) (affirming dismissal of the claims of 15 of the 16 plaintiffs but holding that the one plaintiff who alleged he had suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract and unjust enrichment, among other claims); *Tsao v. Captiva MVP Restaurant Partners, LLC*, 986 F.3d 1332, 1340-45 (11th Cir. 2021) (affirming dismissal of plaintiff's breach of implied contract, negligence, unjust enrichment, unfair competition and related claims, arising out of the data breach of a restaurant's point of sale system, which allegedly exposed plaintiff's (and other customers') credit card and other financial information, and as a result of which plaintiff alleged three types of injuries suffered in his efforts to mitigate the perceived risk of future identity theft: lost cash back or reward points (due to lost use from canceling and waiting for reissued credit cards), lost time spent addressing the problems caused by the cyber-attack, and restricted card access resulting from his credit card cancellations); *Antman v. Uber Technologies, Inc.*, Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *In re Science Applications International Corp. (SAIC) Backup Tape Data that Theft Litigation*, 45 F.

find standing[27]).

Supp. 2d 14, (D.D.C. 2014) (granting in part and denying in part defendant's motion to dismiss plaintiffs' claims arising out of a government data breach; holding, (1) the risk of identity theft alone was insufficient to constitute "injury in fact" for purposes of standing; (2) invasion of privacy alone was insufficient to constitute "injury in fact" for purposes of standing; (3) allegations that victims lost personal and medical information was too speculative to constitute "injury in fact" for purposes of standing; (4) mere allegations that unauthorized charges were made to victims' credit cards or debit cards following theft of data failed to show causation; (5) plaintiffs' claim that victims received a number of unsolicited calls from telemarketers and scam artists following data breach did not suffice to show causation, as required for standing; but (6) allegations that a victim received letters in the mail from credit card companies thanking him for applying for a loan were sufficient to demonstrate causation; and (7) allegations that a victim received unsolicited telephone calls on her unlisted number from insurance companies and others targeted at her specific, undisclosed medical condition were sufficient to demonstrate causation); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092-95 (N.D. Cal. 2013) (dismissing plaintiffs' putative class action suit arising out of a hacker gaining access to their LinkedIn passwords and email addresses, for lack of Article III standing, where plaintiffs alleged no injury or damage); *see generally infra* § 27.07 (analyzing standing in putative data security breach class action suits).

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

Where standing has been found in putative data privacy class action suits, it has been because a plaintiff can allege entitlement to monetary damages[28] or the alleged breach of a

---

(9th Cir. 2018) (holding that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court, relying on the fact that other parties had alleged financial harm from the same security breach, which the court found evidenced the risk to these plaintiffs, who did not allege similar harm but alleged the threat of future harm, and because, after the breach, Zappos provided routine post-breach precautionary advice about changing passwords, which the panel considered to be an acknowledgement by Zappos that the information taken gave the hackers the means to commit financial fraud or identity theft), *cert. denied*, 139 S. Ct. 1373 (2019); *In re U.S. Office of Personnel Management Data Security Breach Litig.*, 928 F.3d 42, 54-61 (D.C. Cir. 2019) (following *Attias* in finding standing in a multi-month cyberattack involving the theft of the personnel records of 21.5 million government employees, over the objection of the dissent that with the passage of time it was not plausible that this attack was undertaken to commit identity theft, and more plausibly involved foreign espionage); *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (following the Seventh Circuit's decision in *Remijas v. Neiman Marcus Group, LLC*, in holding that plaintiffs, whose information had been exposed but who were not victims of identity theft, had plausibly alleged a heightened risk of future injury to establish standing because it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the intent and ability to use the data for ill."), *cert. denied*, 138 S. Ct. 981 (2018); *see generally infra* § 27.07[2] (analyzing standing in putative data security breach class action suits).

The standard for establishing standing in a putative class action premised on the threat of future injury was tightened by the U.S. Supreme Court in in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021), in which the Supreme Court held that a material risk of future harm can satisfy the concrete-harm requirement in the context of a claim for injunctive relief to prevent harm from occurring, if the harm is sufficiently imminent and substantial, but the mere risk of future harm cannot qualify as a concrete harm in a suit for damages (at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm). *Id.* at 1010-12; *infra* § 27.07[2][B] (analyzing the case and its impact on standing in putative data breach class action suits).

[28]*See, e.g.*, *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1208-11 (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);

privacy policy,[29] or, where sensitive personal data has been compromised, based on the risk of future identity theft, where this theory has been applied.[30] Less commonly, Article III standing also may be established based on invasion of a

---

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). *But see Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *4-5 (N.D. Cal. Mar. 1, 2021) (dismissing plaintiffs' California right of publicity claim, arising out of defendant's use of high school yearbook photos and related information in its subscription database, for lack of Article III standing, because (1) "the information in the Yearbook database is not private: it is public yearbook information distributed to classmates (and ultimately to Ancestry). Ancestry's using the public profiles to solicit paying subscribers—standing alone—does not establish injury." (2) plaintiffs did not have a commercial interest in their public profiles that precluded Ancestry's use of the profiles for commercial gain; and (3) section 3344 requires a showing of injury, not mere use and distribution, as alleged).

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

[30] *See, e.g.*, *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (security breach where some members of the putative class had already been the victims of identity theft); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (suit for negligence and breach of contract by employees who had had their personal information, including names, addresses, and social security numbers, compromised as a result of the theft of a company laptop); *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (granting in part and denying in part defendants' motion to dismiss plaintiffs' allegations that defendants failed to provide reasonable network security, including utilizing industry-standard encryption, to safeguard plaintiffs' personal and financial information stored on defendants' network; finding that plaintiffs had sufficiently established Article III standing by plausibly alleging a "credible threat" of impending harm based on the disclosure of their personal information following the intrusion); *see generally infra* § 27.07 (analyzing standing in data security putative class action cases and citing a broader range of opinions). As noted earlier in this section, there is a significant split of authority on how courts view standing in security breach cases where information has been exposed but the only harm is apprehension of future identity theft. *See generally infra* § 27.07[2].

constitutional right.[31]

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

---

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

[32]*See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) (holding, after earlier dismissing plaintiffs' original complaint for lack of standing, that plaintiffs had standing to assert Stored Communications Act and California Constitutional Right of Privacy claims, as alleged in their amended complaint, but dismissing those claims with prejudice for failure to state a claim); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1053–55 (N.D. Cal. 2012) (holding that plaintiffs established injury in fact for purposes of Article III standing by alleging a violation of their statutory rights under the Wiretap Act); *In re Hulu Privacy Litig.,* No. C 11-03764 LB, 2012 WL 2119193, at *8 (N.D. Cal. June 11, 2012) (holding that plaintiffs "establish[ed] an injury (and standing) by alleging a violation of [the Video Privacy Protection Act]"); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (denying defendant's motion with respect to plaintiffs' Stored Communications Act claim, finding a violation of statutory rights to be a concrete injury, while dismissing claims for fraudulent misrepresentation, negligent misrepresentation, public disclosure of private facts, actual and constructive fraud, breach of contract and unjust enrichment in a putative class action suit, for lack of standing, with leave to amend, based on the defendant's alleged practice of including the search terms employed by a user in the URL for the search results page displayed in response to a search query, allegedly causing that information to be visible to advertisers in the referer header when a user clicks on an advertiser's link from the results page); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) (granting in part defendant's motion to dismiss but finding Article III standing in a case where the plaintiffs alleged that a social network transferred data to advertisers without their consent because the Wiretap Act creates a private right of action for any person whose electronic communication is "intercepted, disclosed, or intentionally used," and does not require any further injury), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims).

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

require a showing of damage or injury, in light of a circuit split that ultimately was resolved by the U.S. Supreme Court in 2016[34] and which was further clarified in 2021,[1] but which prior to 2016 had made federal courts in California favored venues for data privacy cases because of the Ninth Circuit's liberal view of standing (and the perception that California law and juries tend to favor plaintiffs, which remains one of the reasons why so many putative data privacy class action suits are brought in federal courts in California).[35]

(N.D. Cal. Jan. 27, 2014) (denying the defendant's motion to certify the opinion for interlocutory appeal).

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

[1]*See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

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

In *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed*, 567 U.S. 756 (2012), the Ninth Circuit had held that a plaintiff had standing to sue a title insurer under the anti-kickback provisions of Real Estate Settlement Procedures Act, 12 U.S.C.A. § 2607, regardless of whether she was overcharged for settlement services, because the statute did not limit liability to instances in which a plaintiff was overcharged. Another Ninth Circuit panel (without citing Edwards) subsequently held that a plaintiff had standing, at least for purposes of a motion to dismiss at the outset of the case, to allege Title I and Title II ECPA claims for Wiretap and Stored Communications Act violations, among others, based on the defendants' alleged telephone surveillance, even though the court acknowledged that the plaintiff ultimately might be unable to prove that she in fact had been subject to illegal surveillance, at which point the court, on a more developed record, might conclude that plaintiff lacked standing. *See Jewel v. National Security Agency*, 673 F.3d 902, 908–911 (9th Cir. 2011); *see also Robins v. Spokeo, Inc.*, 742 F.3d 409, 412-14 (9th Cir. 2014) (holding, in a case in which the plaintiff alleged that the defendant's website published inaccurate information about him, that because the plaintiff had stated a claim for a willful violation of the Fair Credit Reporting Act, for which actual harm need not be shown, the plaintiff had established Article III standing, where injury was premised on the alleged violation of plaintiff's statutory rights), *vacated and remanded*, 136 S. Ct. 1540 (2016); *In re Google, Inc. Privacy Policy Litigation*, Case No. C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec 3, 2013) (following *Edwards* in holding that plaintiffs had established Article III injury under the Wiretap Act and the Stored Communications Act by al-

leging unauthorized access and wrongful disclosure of communications, including disclosure to third parties, in addition to the interception of communications); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (following *Edwards* in denying defendant's motion with respect to plaintiffs' Stored Communications Act claim).

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

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

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

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

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

For an injury to be *particularized,* it "must affect the plaintiff in a personal and individual way."[42] Justice Alito explained that "[p]articularization is necessary to establish

---

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

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

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

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

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

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

[41]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). Justice Alito explained that while Article III standing is determined by a three part test, *Spokeo* turned largely on the first factor. To establish standing, a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.,* 528 U.S. 167, 180-81 (2000).

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

injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.' "[43]

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

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

---

v. Defenders of Wildlife, 504 U.S. 555, 560 n.1 (1992).

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

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

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

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

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

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

[49]One district court held that a state legislature could create rights sufficient to confer Article III standing "[i]n the absence of governing U.S. Supreme Court precedent . . . . " *Matera v. Google, Inc.*, Case No. 15-CV-04062-LHK, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016) (denying defendant's motion to dismiss plaintiff's California Invasion of Privacy Act claim for lack of standing). This analysis, however, is plainly wrong given that Justice Alito expressly identified the role of *Congress*, not state legislatures, in elevating claims. Moreover, state legislatures have no legal authority to confer subject matter jurisdiction over state claims on federal

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

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

Spokeo was a compromise 6-2 opinion that likely would have been decided differently had conservative Justice Scalia, who participated in oral argument for the case, not

---

courts. *See, e.g., Hollingsworth v. Perry*, 570 U.S. 693, 695-96 (2013) ("[S]tanding in federal court is a question of federal law, not state law. And no matter its reasons, the fact that a State thinks a private party should have standing to seek relief for a generalized grievance cannot override our settled law to the contrary."); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017) (citing *Spokeo* and *Hollingsworth* in finding no standing to sue under various state statutes).

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

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

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

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

[54]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016). On remand, the Ninth Circuit concluded that Robins had standing under the Supreme Court's test. *See Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017).

passed away before the opinion issued.[55]

Spokeo was reaffirmed and tightened in *TransUnion LLC v. Ramirez*,[1] in which the Supreme Court, with three new conservative justices appointed by former President Trump who were not members of the Court that decided *Spokeo*, clarified that "*Spokeo* is not an open-ended invitation for federal courts to loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts."[2]

In *Ramirez*, the trial court had certified a class of 8,185 individuals who had OFAC alerts in their credit files. TransUnion offered customers an optional OFAC Name Screen Alert service, which identified individuals whose names were included on a list maintained by the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) of suspected terrorists, drug traffickers and other serious criminals. Plaintiffs had alleged that TransUnion violated the Fair Credit Reporting Act by failing to use reasonable procedures to ensure the accuracy of their credit files. The Supreme Court, however, held that only 1,853 class members, including Ramirez, who had had OFAC alerts in their files communicated to third parties, had standing, because they had suffered a harm with a "close relationship" to the harm associated with the tort of defamation. By contrast, the remaining 6,332 class members whose files also contained misleading OFAC alerts did not have standing because their information was never communicated to a third party and "the mere existence of inaccurate information in a database is insufficient [absent dissemination] to confer Article III standing."[3] The Court also held that formatting errors in notices sent to all class members about the incorrect OFAC

---

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

[1] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

[2] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021).

[3] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2209 (2021). Justice Kavanaugh—analogizing the case to a suit for defamation for purposes of evaluating whether plaintiffs had suffered a concrete injury—explained that publication was essential to liability in a suit for defamation and that there was no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounted to a concrete injury. *Id.* Justice Kavanaugh wrote that "where allegedly inaccurate or misleading information sits in a company database, the plaintiffs' harm is roughly the same, legally speaking, as if someone wrote a defamatory let-

alerts did not justify standing because plaintiffs did not demonstrate that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts under *Spokeo*.[4]

In so ruling, Justice Kavanaugh, writing for the 6-3 majority, reiterated the principle from *Spokeo* that a concrete harm may be based on tangible harm and, in some circumstances, intangible. "[T]raditional tangible harms, such as physical harms and monetary harms . . . ," Justice Kavanaugh explained, readily qualify as concrete injuries under Article III. "Chief among the[] ["[v]arious intangible harms [that] can also be concrete"] are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts . . . [such as], for example, reputational harms, disclosure of private information, and intrusion upon seclusion.[5]. . . And those traditional harms

---

ter and then stored it in her desk drawer. A letter that is not sent does not harm anyone, no matter how insulting the letter is." *Id.* at 2210. The Court reiterated that "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.*

[4]*See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2213-14 (2021). Plaintiffs had argued that TransUnion breached its obligation to provide them their complete credit files upon request because it had sent copies that omitted the OFAC information and then sent a second mailing about OFAC which they argued should have included another summary of rights notice. The Supreme Court, however, held that these were bare procedural violations under *Spokeo,* writing that plaintiffs had

> not demonstrated that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts. *See Spokeo*, 578 U. S., at 341. In fact, they do not demonstrate that they suffered any harm at all from the formatting violations. The plaintiffs presented no evidence that, other than Ramirez, "a single other class member so much as *opened* the dual mailings," "nor that they were confused, distressed, or relied on the information in any way." . . . The plaintiffs put forth no evidence, moreover, that the plaintiffs would have tried to correct their credit files—and thereby prevented dissemination of a misleading report—had they been sent the information in the proper format.

TransUnion LLC v. Ramirez, 141 S. Ct. at 2213. The Court likewise rejected the argument that TransUnion's formatting violations created a risk of future harm. *See id*. at 2212. The Court also rejected the argument of the United States, as *amicus curiae*, that the plaintiffs suffered a concrete "informational injury" because "plaintiffs did not allege that they failed to receive any required information. They argued only that they received it *in the wrong format*." *Id.* at 2214 (emphasis in original).

[5]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021), *citing*

may also include harms specified by the Constitution itself."[6]

Justice Kavanaugh also reiterated that, as *Spokeo* made clear, Congress's views may be "instructive."[7] Quoting a Sixth Circuit opinion, however, he cautioned that

> even though "Congress may 'elevate' harms that 'exist' in the real world before Congress recognized them to actionable legal status, it may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." . . . Congress's creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III any more than, for example, Congress's enactment of a law regulating speech relieves courts of their responsibility to independently decide whether the law violates the First Amendment. . . .
>
> For standing purposes, therefore, an important difference exists between (i) a plaintiff 's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff 's suffering concrete harm because of the defendant's violation of federal law. Congress may enact legal prohibitions and obligations. And Congress may create causes of action for plaintiffs to sue defendants who violate those legal prohibitions or obligations. But under Article III, an injury in law is not an injury in fact. Only those plaintiffs who have been concretely harmed by a defendant's statutory violation may sue that private defendant over that violation in federal court. As then-Judge Barrett succinctly summarized, "Article III grants federal courts the power to redress harms that defendants cause plaintiffs, not a freewheeling power to hold

---

Spokeo, Inc. v. Robins, 578 U.S. 330, 340–41 (2016), *Meese v. Keene*, 481 U.S. 465, 473 (1987) (reputational harms), *Davis v. Federal Election Commission*, 554 U.S. 724, 733 (2008) (disclosure of private information), and *Gadelhak v. AT&T Services, Inc*., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (intrusion upon seclusion); *see generally supra* § 27.07[2] (analyzing standing in cybersecurity breach putative class action suits); *infra* § 29.16[6] (analyzing standing in texting and other TCPA cases and discussing *Gadelhak v. AT&T*).

[6]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021), *citing Spokeo, Inc. v. Robins,* 578 U.S. 330, 340 (2016) (citing *Pleasant Grove City v. Summum*, 555 U.S. 460 (2009) (abridgment of free speech), and *Church of Lukumi Babalu Aye, Inc. v. Hialeah*, 508 U.S. 520 (1993) (infringement of free exercise)).

[7]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021), *quoting Spokeo, Inc. v. Robins,* 578 U.S. 330, 341 (2016).

defendants accountable for legal infractions." *Casillas*, 926 F.3d at 332.[8]

Spokeo and *Ramirez* are relevant to data privacy cases

---

[8] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2205 (2021), *quoting Hagy v. Demers & Adams*, 882 F.3d 616, 622 (6th Cir. 2018) (Sutton, J.) (citing *Spokeo, Inc. v. Robins,* 578 U.S. 330, 341 (2016)). Quoting D.C. Circuit Judge Katsas, sitting by designation on an Eleventh Circuit panel, Justice Kavanaugh reiterated that "[a]s Judge Katsas has rightly stated, 'we cannot treat an injury as "concrete" for Article III purposes based only on Congress's say-so.' " *TransUnion,* 141 S. Ct. at 2205, *quoting Trichell v. Midland Credit Management, Inc*., 964 F.3d 990, 999 n.2 (11th Cir. 2020). Justice Kavanaugh elaborated:

> To appreciate how the Article III "concrete harm" principle operates in practice, consider two different hypothetical plaintiffs. Suppose first that a Maine citizen's land is polluted by a nearby factory. She sues the company, alleging that it violated a federal environmental law and damaged her property. Suppose also that a second plaintiff in Hawaii files a federal lawsuit alleging that the same company in Maine violated that same environmental law by polluting land in Maine. The violation did not personally harm the plaintiff in Hawaii.
>
> Even if Congress affords both hypothetical plaintiffs a cause of action (with statutory damages available) to sue over the defendant's legal violation, Article III standing doctrine sharply distinguishes between those two scenarios. The first lawsuit may of course proceed in federal court because the plaintiff has suffered concrete harm to her property. But the second lawsuit may not proceed because that plaintiff has not suffered any physical, monetary, or cognizable intangible harm traditionally recognized as providing a basis for a lawsuit in American courts. An uninjured plaintiff who sues in those circumstances is, by definition, not seeking to remedy any harm to herself but instead is merely seeking to ensure a defendant's "compliance with regulatory law" (and, of course, to obtain some money via the statutory damages). *Spokeo*, 578 U. S., at 345 (THOMAS, J., concurring) (internal quotation marks omitted); *see Steel Co*., 523 U.S., at 106–107. Those are not grounds for Article III standing.
>
> As those examples illustrate, if the law of Article III did not require plaintiffs to demonstrate a "concrete harm," Congress could authorize virtually any citizen to bring a statutory damages suit against virtually any defendant who violated virtually any federal law. Such an expansive understanding of Article III would flout constitutional text, history, and precedent. In our view, the public interest that private entities comply with the law cannot "be converted into an individual right by a statute that denominates it as such, and that permits all citizens (or, for that matter, a subclass of citizens who suffer no distinctive concrete harm) to sue." *Lujan*, 504 U.S., at 576–577.

TransUnion, 141 S. Ct. at 2205-06 (footnotes omitted). With respect to the requirement that an injury be both concrete *and* particularized, Justice Kavanaugh observed that

> if there were no concrete-harm requirement, the requirement of a particularized injury would do little or nothing to constrain Congress from freely creating causes of action for vast classes of unharmed plaintiffs to sue any defendants who violate any federal law. (Congress might, for example, provide that everyone has an individual right to clean air and can sue any defendant who violates any air-pollution law.) That is one reason why the Court has been careful to emphasize that concreteness and particularization are separate requirements.

Id. at 2206 n.2.

premised on intangible harm and violations of federal statutes. The result of *Spokeo* and *Ramirez* is that merely stating a claim under a federal statute may not be sufficient to establish standing, nor will mere procedural violations of a statute.[56] Data privacy claims have been deemed to involve

---

[56]*See, e.g.*, *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12, 15-17 (2d Cir. 2017) (holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have Article III standing to sue for alleged violations of the Illinois Biometric Information Privacy Act, which was intended to protect against potential misuse of biometric data, because plaintiffs' alleged failure to comply with provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information amounted to merely "procedural violations" under *Spokeo*, where no reasonable player would have concluded that the MyPlayer feature was conducting anything other than a face scan where plaintiffs had to place their faces within 6-12 inches of the camera, slowly turn their heads to the left and right, and continue to do this for approximately 15 minutes, belying any claim of lack of consent; plaintiffs could not allege any material risk of misuse of biometric data for failing to provide notice of the duration for which the data would be held; and plaintiffs failed to show a risk of real harm from the alleged unencrypted transmission of their face scans); *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910-12 (7th Cir. 2017) (holding that the plaintiff lacked standing to sue for Time Warner's alleged retention of his personally identifiable information in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e), because he did not allege that "any of the personal information that he supplied to the company . . . . had been leaked or caused financial or other injury to him or had even been at risk of being leaked."; Although the Act created a right of privacy, and "[v]iolations of rights of privacy are actionable," because plaintiff did not allege that "Time Warner had released, or allowed anyone to disseminate, any of the plaintiff's personal information in the company's possession," the statutory violation alone could not confer standing); *Braitberg v. Charter Communications, Inc.,* 836 F.3d 925, 929-31 (8th Cir. 2016) (dismissing for lack of standing, as a case involving a mere procedural violation under *Spokeo,* plaintiff's putative class action suit alleging that his former cable television provider retained his personally identifiable information in violation of the Cable Communications Policy Act because "Braitberg alleges only that Charter violated a duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it. He does not allege that Charter has disclosed the information to a third party, that any outside party has accessed the data, or that Charter has used the information in any way during the disputed period. He identifies no material risk of harm from the retention; a speculative or hypothetical risk is insufficient. Although there is a common law tradition of lawsuits for invasion of privacy, the retention of information lawfully obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts."); *Hancock v. Urban Outfitters, Inc.,* 830 F.3d 511 (D.C. Cir. 2016) (affirming dismissal of plaintiff's claim under the D.C.'s Use of

merely "bare procedural" violations (and therefore insufficient to establish injury in fact under *Spokeo*) in cases brought under the Fair and Accurate Credit Transactions Act (FACTA),[57] the Fair Credit Reporting Act,[58] and other

---

Consumer Identification Information Act, D.C. Code §§ 47–3151 *et seq*., which provides that "no person shall, as a condition of accepting a credit card as payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form, . . ." for lack of standing, because "[t]he Supreme Court's decision in *Spokeo* . . . closes the door on Hancock and White's claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury.").

[57]5 U.S.C. § 1681c(g)). FACTA seeks to reduce the risk of identity theft by, among other things, prohibiting merchants from including more than the last five digits of a customer's credit card number on a printed receipt. *See* 15 U.S.C. § 1681c(g)(1); *see generally supra* § 26.12[8]. Courts have found standing to be lacking in FACTA cases involving bare procedural violations. *See, e.g., Katz v. Donna Karan, LLC,* 872 F.3d 114 (2d Cir. 2017) (affirming dismissal for lack of standing plaintiff's FACTA claim alleging that he twice purchased items at the defendants' stores, and on both occasions received a printed receipt that identified not only the last four digits of his credit card number but also the first six digits, because plaintiff could not meet his affirmative burden to establish subject matter jurisdiction by a preponderance of the evidence); *Crupar–Weinmann v. Paris Baguette America, Inc*., 861 F.3d 76, 81 (2d Cir. 2017) (affirming the lower court's holding that a procedural violation of FACTA—the printing of the plaintiff's credit card expiration date on her receipt—presented no material risk of harm to the underlying interest Congress sought to protect (identity theft), because Congress itself had clarified that printing the expiration date, without more, did not "increase. . . the risk of material harm of identity theft."); *Kamal v. J. Crew Group, Inc.*, 918 F.3d 102, 112-19 (3d Cir. 2019) (holding that the plaintiff in a FACTA putative class action suit premised on the defendant printing more than the last five digits of a consumer's credit card on a receipt lacked Article III standing for suing over a "bare procedural" violation); *Meyers v. Nicolet Restaurant of De Pere, LLC,* 843 F.3d 724, 726-29 (7th Cir. 2016) (holding that plaintiff lacked standing to sue for a FACTA violation alleging that the defendant failed to provide him with a receipt that truncated the expiration date of his credit card because "without a showing of injury apart from the statutory violation, the failure to truncate a credit card's expiration date is insufficient to confer Article III standing."); *Bassett v. ABM Parking Services, Inc.*, 883 F.3d 776, 779-83 (9th Cir. 2018) (holding that receiving "an overly revealing credit card receipt—unseen by others and unused by identity thieves . . ." constituted a procedural violation of the FCRA that was insufficient to establish Article III standing; "We need not answer whether a tree falling in the forest makes a sound when no one is there to hear it. But when this receipt fell into Bassett's hands in a parking garage and no identity thief was there to snatch it, it did not make an injury."); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 931 (11th Cir. 2020) (en banc) (holding that plaintiff lacked Article III stand-

federal[59] or state[60] privacy statutes. Data privacy cases have

---

ing in a suit alleging that Godiva violated FACTA by printing too many digits on credit card receipts, thereby allegedly exposing customers to an elevated risk of identity theft; rejecting the argument that time spent destroying or safeguarding receipts in an effort to mitigate future harm amounted to anything more than a "hypothetical future harm" under *Clapper*); *see also Daniel v. National Park Service*, 891 F.3d 762, 766-68 (9th Cir. 2018) (distinguishing the Ninth Circuit's opinion in*Bassett*, finding that the plaintiff had alleged a concrete, particularized injury based on identity theft and fraudulent charges that occurred after she received a debit card receipt at Yellowstone National Park that displayed the expiration date of her credit card, but holding that Article III standing was lacking because she had not alleged an injury "fairly traceable" to the violation because her actual debit card number was partially obscured and there were no facts to suggest that the exposure of the expiration date resulted in the identity theft or fraudulent charges).

[58]*SeeTransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) (reversing and remanding judgment following trial in a class action suit where, among other things, the Court held that (1) class members whose credit files contained misleading OFAC alerts that were not communicated to third party creditors did not have standing because "the mere existence of inaccurate information in a database is insufficient [absent dissemination] to confer Article III standing" and (2) formatting errors in notices sent to all class members about the incorrect OFAC alerts did not justify standing because plaintiffs did not demonstrate that the format of TransUnion's mailings caused them a harm with a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts under *Spokeo*); *see also, e.g.*, *Long v. Southeastern Pennsylvania Transportation Authority*, 903 F.3d 312, 320-25 (3d Cir. 2018) (holding that job applicants lacked Article III standing to sue under the Fair Credit Reporting Act over the defendant's failure to provide them with notice of their right to obtain copies of their background checks before denying them employment, because the failure amounted to a bare procedural violation, where the plaintiffs in fact understood their rights); *Groshek v. Time Warner Cable, Inc.*, 865 F.3d 884, 887 (7th Cir. 2017) (finding no standing to bring a Fair Credit Reporting Act claim where defendants disclosed that they would be obtaining consumer reports, but the disclosures were not in the format required by the FCRA); *see generally supra* § 26.12[3] (analyzing the FCRA).

[59]*See, e.g.*, *Markakos v. Medicredit, Inc.*, 997 F.3d 778, 779-82 (7th Cir. 2021) (affirming dismissal of plaintiff's FDCPA claim, alleging violations by sending her letters that stated inconsistent debt amounts and that unclearly identified her creditor, for failing to allege injury-in-fact sufficient to confer Article III standing; "In the last five months, we've held eight times that a breach of the Fair Debt Collection Practices Act ('FDCPA') does not, by itself, cause an injury in fact. We now repeat that refrain once more."); *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910-12 (7th Cir. 2017) (holding that the plaintiff lacked standing to sue for Time Warner's alleged retention of his personally identifiable information in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e),

been dismissed for lack of Article III standing on other

---

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

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

grounds[61] as well.

499, 510-21 (S.D.N.Y. 2017); *NEI Contracting & Engineering, Inc.*, 926 F.3d 528, 532-33 (9th Cir. 2019) (affirming decertification of a class, following the determination that the named plaintiff lacked Article III standing, in a suit brought under the California Invasion of Privacy Act, alleging that the defendant violated CIPA by recording customer orders without consent); *Heeger v. Facebook, Inc*., 509 F. Supp. 3d 1182, 1187-91 (N.D. Cal. 2020) (dismissing plaintiffs' claims in *Heeger* for violations of the California constitution and CIPA and for intrusion upon seclusion, for lack of Article III standing because they did not plausibly allege any privacy injuries where they did not allege more than the collection of IP addresses associated with mobile devices, "and there is no legally protected privacy interest in IP addresses."; "The *Heeger* FAC now reads like a book report that simply summarizes third-party news stories about Facebook's ostensible capacity to 'discern precise locations' from user data. . . . Few facts are alleged without the caveat of 'on information or belief,' or without hedging on whether Facebook actually does what Heeger accuses, or simply has the ability to do it. . . . These allegations. . . did little more than parrot internet musings about things Facebook may or may not be doing, and which plaintiffs may or may not have experienced themselves. When these fillers are stripped away, all that the Heeger FAC alleges is that Facebook collected plaintiffs' IP addresses.").

Standing to assert state law claims presumably should be more limited—since Congress, which does not enact state laws, by definition could not elevate a state law claim to one justifying standing (although courts often treat state statutory claims as though they were federal claims in applying *Spokeo* and its progeny).

[61] *See, e.g., Salcedo v. Hanna*, 936 F.3d 1162, 1166-73 (11th Cir. 2019) (finding no standing in a Telephone Consumer Protection Act texting case where the plaintiff received only a single text message, holding that Congress, in enacting the TCPA, was concerned about junk faxes, which "has little application to the instantaneous receipt of a text message[,]" and that the intangible harm experienced from receipt of an unwanted text message bears little relation to the harm experienced from intrusion upon seclusion, trespass or nuisance (which requires intrusion on real property), or conversion or trespass to chattels ("although Salcedo's allegations here bear a passing resemblance to this kind of historical harm, they differ so significantly in degree as to undermine his position. History shows that Salcedo's allegation is precisely the kind of fleeting infraction upon personal property that tort law has resisted addressing.")); *Cordoba v. DirecTV, LLC*, 942 F.3d 1259 (11th Cir. 2019) (holding that plaintiffs whose phone numbers were not on the National Do Not Call Registry and never asked Telcel not to call them again lacked Article III standing for unwanted calls received from Telcel, under the TCPA, because the receipt of a call was not traceable to Telcel's alleged failure to comply with regulations requiring it to maintain an internal do-not-call list); *McCollough v. Smarte Carte, Inc.,* Case No. 16 C 03777, 2016 WL 4077108, at *3-5 (N.D. Ill. Aug. 1, 2016) (dismissing plaintiff's putative Illinois Biometric Information Privacy Act class action suit for lack of Article III and statutory standing where the plaintiff alleged that Smarte Carte retained her fingerprint biometric information without written consent, where Smarte

On the other hand, *Spokeo*'s directive to look to either Congress or whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts has been construed in some cases to provide a basis for standing because of the nature of privacy rights at common law[62] and/or because of federal statutory claims deemed by some courts to be analogous to common law invasion of privacy, including suits brought under the Electronic Communications Privacy Act,[9] Video Privacy Protection Act,[63]

Carte used a person's fingerprints to allow them to access a rented locker, because '[e]ven without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, the Court finds it difficult to imagine, without more, how this retention could work a concrete harm" and she could not establish that she was "aggrieved by" the alleged violation, to establish statutory standing); *see generally infra* § 29.16 (analyzing the TCPA and case law construing it).

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

[9]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litig.,* 827 F.3d 262, 272–74 (3d Cir. 2016) ((holding that plaintiffs had Article III standing to pursue ECPA Title II (Stored Communications Act) and other claims), *cert. denied,* 137 S. Ct. 624 (2017); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 597-99 (9th Cir. 2020) (ECPA Title I (Wiretap Act) and II (Stored Communications Act), *cert. denied,* 141 S. Ct. 1684 (2021); *Campbell v. Facebook, Inc*., 951 F.3d 1106, 1117-20 (9th Cir. 2020) (Title I - Wiretap Act, 18 U.S.C.A. § 2511(1)(a)); *In re Google Referrer Header Privacy Litigation,* 465 F. Supp. 3d 999, 1006-10 (N.D. Cal. 2020) (18 U.S.C.A. § 2702); *In re Google LLC Street View Electronic Communications Litigation*, __ F. Supp. 3d __, 2020 WL 1288377, at *2-4 (N.D. Cal. 2020) (ECPA (Wiretap Act)).

[63]*See, e.g., In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 272-74 (3d Cir. 2016) (holding, without much analysis, that plaintiffs had Article III standing to pursue Stored Communications Act, Video Privacy Protection Act, California Invasion of Privacy Act, New Jersey computer crime and common law privacy claims), *cert. denied,* 137 S. Ct. 624 (2017);

Telephone Consumer Protection Act,[64] and the Fair Credit

Eichenberger v. ESPN, Inc., 876 F.3d 979, 982-84 (9th Cir. 2017) (affirming dismissal on the merits, but first holding that the plaintiff had standing to sue for the alleged disclosure of personally identifiable information under the Video Privacy Protection Act, which the Ninth Circuit panel deemed an alleged violation of "a substantive provision that protects concrete interest."); *Perry v. CNN,* 854 F.3d 1336, 1339-41 (11th Cir. 2017) (holding that a user of the CNN mobile app had standing to sue under the Video Privacy Protection Act, where he alleged no injury other than the statutory violation, because (1) "[t]he structure and purpose of the VPPA supports the conclusion that it provides actionable rights" in prohibiting the wrongful disclosure of personal information, and (2) a VPPA claim has a close relationship to a common law right of privacy, which is a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts, where "[t]he intrusion itself makes the defendant subject to liability, even though there is no publication or other use . . . "; citing Restatement of Torts § 652B cmt. B); *In re Vizio, Inc. Consumer Privacy Litig.,* 238 F. Supp. 3d 1204, 1215-17 (C.D. Cal. 2017) (holding that plaintiffs had standing to sue under the VPPA and Wiretap Act in a putative database privacy class action suit involving data allegedly collected by a smart television manufacturer and others, based on the close relationship of these claims to common law invasion of privacy and because of Congress's judgment in enacting the VPPA); *Yershov v. Gannett Satellite Information Network, Inc.*, 204 F. Supp. 3d 353, 358-64 (D. Mass. 2016) (denying defendant's motion to dismiss for lack of Article III standing); *see generally supra* § 26.13[10] (analyzing the VPPA in greater detail).

[64]*See, e.g.*, *Melito v. Experian Marketing Solutions, Inc.*, 923 F.3d 85, 88, 92-95 (2d Cir. 2019) (holding that "Plaintiffs' receipt of the unsolicited text messages, sans any other injury, is sufficient to demonstrate injury-in-fact."; " 'nuisance and privacy invasion' were the harms Congress identified when enacting the TCPA. Pub. L. No. 102-243, §§ 5, 12. And text messages, while different in some respects from the receipt of calls or faxes specifically mentioned in the TCPA, present the same 'nuisance and privacy invasion' envisioned by Congress when it enacted the TCPA."); *Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 652-54 (4th Cir. 2019) (holding that the plaintiff, in a suit brought over telemarketer calls to a number on the national Do-Not-Call registry under 47 U.S.C.A. § 227(c)(5) had standing; "Since that harm is both particular to each person and imposes a concrete burden on his privacy, it is sufficient to confer standing."); *Van Patten v. Vertical Fitness Group, LLC*, 847 F.3d 1037, 1042-43 (9th Cir. 2017) (holding that the plaintiff had alleged sufficient harm to establish Article III standing in a TCPA case because (1) "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states" and (2) Congress, in enacting the statute, established "the substantive right to be free from certain types of phone calls and text messages absent consumer consent."); *see also Golan v. FreeEats.com, Inc.*, 930 F.3d 950, 957-59 (8th Cir. 2019) (affirming standing where the plaintiff received two answering machine messages from the defendant, by analogy to common law nuisance). *But see Salcedo v. Hanna*, 936 F.3d 1162, 1166-73 (11th Cir. 2019) (disagreeing with *Van Pat-*

Reporting Act,[65] including an FCRA claim premised on a security breach,[66] as well as under the California Invasion of Privacy Act (CIPA)[10] and California Confidentiality of Medi-

---

ten, finding that Congress was concerned about junk faxes, which "has little application to the instantaneous receipt of a text message[,]" and that the intangible harm experienced from receipt of an unwanted text message bears little relation to the harm experienced from intrusion upon seclusion ("We do not see this type of objectively intense interference where the alleged harm is isolated, momentary, and ephemeral."), trespass or nuisance (which requires intrusion on real property), or conversion or trespass to chattels ("although Salcedo's allegations here bear a passing resemblance to this kind of historical harm, they differ so significantly in degree as to undermine his position. History shows that Salcedo's allegation is precisely the kind of fleeting infraction upon personal property that tort law has resisted addressing.")); *Cordoba v. DirecTV, LLC*, 942 F.3d 1259 (11th Cir. 2019) (holding that plaintiffs whose phone numbers were not on the National Do Not Call Registry and never asked Telcel not to call them again lacked Article III standing for unwanted calls received from Telcel, under the TCPA, because the receipt of a call was not traceable to Telcel's alleged failure to comply with regulations requiring it to maintain an internal do-not-call list); *see generally infra* § 29.16 (analyzing the TCPA and case law construing it).

[65]*See, e.g.*, *Nayab v. Capital One Bank (USA), N.A.*, 942 F.3d 480 (9th Cir. 2019) (holding that a consumer suffers a concrete injury in fact, as required to have standing to pursue a FCRA claim, when a third party obtains her credit report for a purpose not authorized by the FCRA, regardless whether the report is published or otherwise used by that third party); *Syed v. M-I, LLC*, 853 F.3d 492, 499-500 (9th Cir. 2017) (holding that the plaintiff had standing where the defendant disclosed that it would be obtaining consumer reports, but disclosed this information in a different format than what was required by FCRA, where the plaintiff alleged that he failed to understand the disclosure); *see generally supra* § 26.12[3] (analyzing the FCRA).

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

[10]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litig.,* 827 F.3d 262, 272–74 (3d Cir. 2016), *cert. denied,* 137 S. Ct. 624 (2017); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 597-99 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1684 (2021); *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117-20 (9th Cir. 2020).

cal Information Act (CMIA).[11]

Spokeo's impact on putative security breach and TCPA class action suits is addressed in sections 27.07[2] and 29.16,

---

[11]*See, e.g.*, *Stasi v. Inmediata Health Group Corp*., No. 19-CV-2353 JM (LL), 2020 WL 6799437, at *2-6 (S.D. Cal. Nov. 19, 2020) (holding that plaintiffs had established Article III and statutory standing to sue under the CMIA, Cal. Civ. Code §§ 56-56.265, in a putative data breach case brought by patients against a medical billing provider).

The CMIA prohibits the unauthorized "disclosure" of medical information, the negligent maintenance of medical information, and the negligent "release" of medical information, and provides for a private cause of action. Cal. Civ. Code §§ 56.10(a), 56.101(a), 56.36(b). The statute also provides for nominal damages without having to show the plaintiff "suffered or was threatened with actual damages." *Id.* § 56.36(b)(1). The CMIA applies to health care providers, service plans, and contractors. *Id.* § 56.10(a). *Medical information,* within the meaning of the CMIA, means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." *Id.* § 56.05(j). *Individually identifiable,* in turn, "means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." *Id.*; *see also Wilson v. Rater8, LLC,* Case No.: 20-cv-1515-DMS-LL, 2021 WL 4865930, at *4-5 (S.D. Cal. Oct. 18, 2021) (dismissing plaintiff's claim that defendants disclosed plaintiff's name, cellular telephone number, "treating physician names, medical treatment appointment information, and medical treatment discharge dates and times" to Rater8 because while some of this information was "individually identifiable," none of it constituted "medical information" within the meaning of the statute, which is defined in section 56.05(j) as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or *treatment*" (emphasis added), but plaintiff alleged the records at issue involved a doctor's appointment pursuant to a demand by an insurance carrier in connection with an automobile accident; "Describing an examination as treatment does not make it so."); *In re Blackbaud, Inc., Customer Data Breach Litig*., Case No. 3:20-mn-02972-JMC, 2021 WL 3568394, at *6-8 (D.S.C. Aug. 12, 2021) (granting in part, denying in part, defendant's motion to dismiss plaintiffs' CMIA claim in a case arising out of a ransomware attack); *Eisenhower Medical Center v. Superior Court*, 226 Cal. App. 4th 430, 434-35, 172 Cal. Rptr. 3d 165 (4th Dist. 2014) (holding that CMIA must be *substantive*; "It is clear from the plain meaning of the statute that medical information cannot mean just any patient-related information held by a health care provider, but must . . . include 'a patient's medical history, mental or physical condition, or treatment.' ").

respectively. *Ramirez* is analyzed in greater detail in section 27.07[2][B].

While many privacy cases involve merely intangible harm, injury in fact in security breach and other cases alternatively may be based on the threat of future harm. The cases most directly relevant to future harm is *Clapper v. Amnesty International USA*,[67] in which the Court made clear that "allegations of possible future injury are not sufficient"[68] and *TransUnion LLC v. Ramirez*,[12] in which the 6-3 majority characterized the holding in *Clapper* as relevant to suits for injunctive relief, not damages. To justify standing based on future harm under *Clapper*, a threatened injury must be "certainly impending" to constitute injury in fact.[69] In *Ramirez,* Justice Kavanaugh, writing for the majority, explained that "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial."[13] However, "a plaintiff 's standing to seek injunctive relief does not necessarily mean that the plaintiff has standing to seek retrospective damages."[14] The Court held that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm—at least unless the exposure to the risk of future harm itself causes a *separate* concrete harm."[15]

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

A number of data privacy suits have been brought under

---

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

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

[12]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

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

[13]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210 (2021), *citing Clapper v. Amnesty Int'l USA,* 568 U.S. 398, 414 n.5 (2013); and *Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983).

[14]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210 (2021).

[15]*TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210-11 (2021) (emphasis in original); *see generally infra* § 27.07[2][B] (analyzing *Ramirez* in greater depth).

the Electronic Communications Privacy 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.[70]

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

To the extent claims are based on *disclosure* under either Title I or II, as opposed to interception (under Title I) or access (under Title II), civil claims may only be based on the *contents* of a communication. Personal data such as a person's name, email address, home address, phone number or other details that could identify a person, however, are treated as non-content data, not the *contents* of a communication, which is defined under ECPA as "information concerning the substance, purport, or meaning of that communication."[71] On this basis alone, most claims premised

---

[70] *See infra* §§ 44.06, 44.07.

[71] 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

on disclosure will not be actionable under either Title I or Title II[72] (subject to narrow exceptions, such as where a URL, which generally is considered non-content data, reveals the substance of a communication[73]).

---

data collected by the telephone company about the source, destination, duration, and time of a call."), *cert. denied*, 559 U.S. 987 (2010); *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding, in a copyright infringement suit, that YouTube was prevented by the Stored Communications Act from disclosing the content of videos marked by users as private, but ordering "production of specified non-content data about such videos" because "the ECPA does not bar disclosure of non-content data about the private videos (e.g., the number of times each video has been viewed on YouTube.com or made accessible on a third-party website through an 'embedded' link to the video)."); *see generally infra* § 50.06[4] (analyzing contents and non-contents under ECPA in greater detail and discussing additional cases).

[72]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 935-36 (N.D. Cal. 2015) (dismissing plaintiffs' Wiretap Act claim because the data allegedly transmitted through cookies about the browsing history of logged-out users was not the contents of a communication), *rev'd on other grounds*, 956 F.3d 589, 607-08 (9th Cir. 2020) (holding that Facebook was not exempt from liability as a matter of law under the Wiretap Act as a party to the communication, without opining on whether plaintiffs adequately pleaded other requisite elements of the statute, which were not raised in the appeal), *cert. denied*, 141 S. Ct. 1684 (2021); *Svenson v. Google Inc.*, No. 13–cv–04080–BLF, 2015 WL 1503429, at *7-8 (N.D. Cal. Apr. 1, 2015) (applying *Zynga* in dismissing without leave to amend plaintiff's SCA claim premised on the alleged disclosure of credit card information (but not numbers), purchase authorization data, addresses, zip codes, names, phone numbers, and email addresses, in connection with the use of Google Wallet); *In re: Carrier IQ, Inc. Consumer Litig.*, 78 F. Supp. 3d 1051, 1083-84 (N.D. Cal. 2015) (dismissing Wiretap Act claim for alleged interception of user names or passwords by the Carrier IQ Software in a putative consumer class action suit); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (dismissing plaintiff's claim because geolocation data was not the contents of a communication and holding that "personally identifiable information that is automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication is not covered by the Wiretap Act."); *see generally infra* § 50.06[4][B].

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

For similar reasons, claims based on non-content data also may fail to state claims under the California constitutional right to privacy or California's Invasion of Privacy Act, Cal. Penal Code § 631(a).[74]

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)). Merely alleging that non-content data was the substance of a communication, however, does not make it so. *See generally infra* § 50.06[4].

[74]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (dismissing plaintiff's CIPA claim where he did not plead facts to show how Facebook used a "machine, instrument or contrivance" to obtain the contents of communications and did not adequately allege that Facebook acquired the contents of a communication), *rev'd on other grounds*, 956 F.3d 589, 607-08 (9th Cir. 2020) (holding that Facebook was not exempt from liability as a matter of law under the Wiretap Act as a party to the communication, without opining on whether plaintiffs adequately pleaded other requisite elements of the statute, which were not raised in the appeal), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1037-42 (N.D. Cal. 2014) (dismissing with leave to amend plaintiff's claim for a violation of California's constitutional right to privacy where plaintiffs alleged that Yahoo's alleged scanning, storage and disclosure of email content violated their right to privacy).

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

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

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.

Data privacy and related AdTech and behavioral advertising claims premised on unauthorized *interception*[75] under Title I (or state statutory equivalents[16]) have failed where there has been consent or no interception[76] (or, at least, no

---

ment of state laws on the same subject.' " *Id., quoting Rice v. Santa Fe Elevator Corp*., 331 U.S. 218, 230 (1947).

[75]*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).

[16]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *2-5 (N.D. Cal. July 28, 2021) (dismissing wiretap claims under California, Florida, and Washington state law (Cal. Penal Code §§ 631(a), 635; Fla. Stat. Ann. § 934.03(2)(d) (permitting interception of a communication "when all of the parties to the communication have given prior consent"); Wash. Rev. Code Ann. §§ 9.73.030(1) (a)-(b) (permitting interception with "the consent of all the participants")), where plaintiffs provided consent by assenting to Instacart's Privacy Policy, which set forth, among other things, that Instacart could share information payment processor partners and third parties); *Javier v. Assurance IQ, LLC*, Case No. 4:20-cv-02860-JSW, 2021 WL 940319, at *2-4 (N.D. Cal. Mar. 9, 2021) (dismissing plaintiff's claim under the California Invasion of Privacy Act (CIPA), Cal. Penal Code § 631, where the plaintiff had given click-through assent to Assurance's Privacy Policy, which made clear that Assurance tracked activity on its website and stated that it may use third party vendors to do so).

[76]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274-76 (3d Cir. 2016) (affirming dismissal of plaintiffs' Wiretap claim, holding that "Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications."), *cert. denied,* 137 S. Ct. 624 (2017); *Rodriguez v. Google LLC*, Case No. 20-cv-04688-RS, 2021 WL 2026726, at *6 (N.D. Cal. May 21, 2021) (dismissing plaintiffs' claim for violating section 2511(1)(a) "[b]ecause Google's alleged interceptions occurred with the consent of app developers . . ." and

"the consent of one party is a complete defense to a Wiretap Act claim"; quoting an earlier case); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 626 (N.D. Cal. 2021) (dismissing plaintiffs' Wiretap Act claim, in a suit alleging that Google collected user data from users of the Chrome browser who chose not to sync their browsers with their Google accounts, because "[t]he Wiretap Act and the SCA prohibit 'the person or entity providing [the ECS]' from divulging the contents of any communication to any person or entity, but Plaintiffs do not allege that Google divulged the contents of any communication to a third party. Rather, Plaintiffs allege that Google divulged information to itself. . . . Accordingly, Plaintiffs' unauthorized disclosure claims under the Wiretap Act and the SCA fail."); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' claims under the Wiretap Act, Stored Communications Act, and Cal. Penal Code § 631(a) (CIPA) where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in the terms of the defendant's Privacy Policy); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953, 955 (N.D. Cal. 2017) (dismissing plaintiff's putative class claims under the Wiretap Act, based on consent provided pursuant to Facebook's Data Policy and Cookie Policy; *citing Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014) ("He who consents to an act is not wronged by it." (quoting Cal. Civ. Code § 3515)) and 18 U.S.C.A. § 2511(2)(d)), *aff'd*, 745 F. App'x 8, 9 (9th Cir. 2018) ("A reasonable person viewing those disclosures would understand that Facebook maintains the practices of (a) collecting its users' data from third-party sites and (b) later using the data for advertising purposes. Knowing authorization of the practice constitutes Plaintiffs' consent."); *In re Vizio, Inc. Consumer Privacy Litig.,* 238 F. Supp. 3d 1204, 1226-28 (C.D. Cal. 2017) (dismissing plaintiffs' Wiretap Act and companion California Invasion of Privacy Act claims with leave to amend where plaintiffs had "not articulated with sufficient clarity when Vizio supposedly intercepted their communications."); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1022-31 (N.D. Cal. 2014) (holding, in a putative Stored Communications Act class action suit, that the plaintiffs consented to email scanning); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1063 (N.D. Cal. 2014) (dismissing plaintiffs' Wiretap Act claim based on Path's mobile app's alleged copying and transmission of electronic address books; "Although Path allegedly transmitted the Class Members' Contact Address Books from the Class Members' mobile devices to Path's servers, Path did not 'intercept' a 'communication' to do so."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *7–8 (N.D. Cal. Mar. 26, 2013) (holding, in a behavioral advertising case, that the plaintiff failed to state a Wiretap Act claim in part where (1) he alleged that he provided his personal information directly to Pandora and that Pandora "intercepted" the information from him, rather than alleging that the defendant used a device to intercept a communication from the plaintiff to a third party, and (2) the communication was directed to Pandora, within the meaning of 18 U.S.C.A. § 2511(3)(A)); *Hernandez v. Path, Inc.*, No. 12-cv-01515-YGR, 2012 WL 5194120, at *3 (N.D. Cal. Oct. 19, 2012) (dismissing plaintiff's claim on the same grounds as in *Opperman*, cited above); *Marsh v. Zazoom Solutions, LLC,* No. C–11–05226–YGR, 2012 WL 952226, at * 17 (N.D. Cal. Mar. 20, 2012) (dismissing plaintiff's Wiretap Act claim in a case

involving payday loans, where the plaintiff did not allege that any defendant "acquired the information by capturing the transmission of information that was otherwise in the process of being communicated to another party," or that any defendant used a "device" to intercept the communication); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712–13 (N.D. Cal. 2011) (dismissing plaintiffs' Title I claim where the communication either was directed from the user to the defendant (in which case the service was the addressee or intended recipient and therefore could disclose the communication to advertisers as long as it had its own lawful consent) or was sent from the user to an advertiser (in which case the advertiser was the addressee or intended recipient), but in either case was not actionable), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim and reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their ECPA claims); *Crowley v. Cybersource*, 166 F. Supp. 2d 1263, 1268-69 (N.D. Cal. 2001) (dismissing an interception claim premised on Amazon.com's alleged disclosure to co-defendant, Cybersource, where the plaintiff's email was sent directly to Amazon.com and was not acquired through use of a device).

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

In *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607-08 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1684 (2021), the Ninth Circuit held that although the Wiretap Act does not define the term *party,* "entities that surreptitiously duplicate transmissions between two parties are not parties to the communication within the meaning of the Act." *Id.* at 607. In that case, the panel held that GET requests allegedly sent to Facebook from websites with Facebook plug-ins were not sent to a party. The panel explained:

> When an individual internet user visits a web page, his or her browser sends a message called a "GET request" to the web page's server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referer header containing the personally-identifiable URL information. Typically, this communication occurs only between the user's web browser and the third-party website. On websites with Facebook plug-ins, however, Facebook's code directs the user's browser to copy the referer header from the GET request and then send a separate but identical GET request and its associated referer header to Facebook's server. It

interception by the defendant).[77] Collecting user data such as a customer's requested URL, the referer URL[78] (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

---

is through this duplication and collection of GET requests that Facebook compiles users' browsing histories.

Id.

In so holding the Ninth Circuit disagreed with the Third Circuit's holding and analysis in *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 140-43 (3d Cir. 2015), *cert. denied,* 137 S. Ct. 36 (2016), which held that defendants were the intended recipients of duplicate GET requests, and thus were parties to the communication, where third party websites duplicated user GET requests and sent them to defendants.

In *Facebook, Inc. Internet Tracking Litigation*, the Ninth Circuit emphasized, however, that the "party exception must be considered in the technical context of th[e] case." 956 F.3d at 607; *see also, e.g.*, *Saleh v. Nike, Inc.*, __ F. Supp. 3d __, 2021 WL 4437734, at *9-11 (C.D. Cal. Sept. 27, 2021) (dismissing plaintiff's CIPA section 631(a) claim for direct liability (but not aiding), alleging use of FullStory session replay software, and distinguishing *Facebook Internet Tracking,* because "[w]hereas in *In re Facebook* the plaintiffs alleged Facebook recorded communications between the plaintiffs and third parties to which Facebook was *not* a party, here, Plaintiff alleges Nike and FullStory recorded Plaintiff's communications with Nike. . . . Thus, to the extent Plaintiff alleges Nike recorded its own communications with Plaintiff, the court finds the § 631 exemption applies."); *Yoon v. Lululemon USA, Inc.*, __ F. Supp. 3d __, 2021 WL 3615907, at *6 (C.D. Cal. July 15, 2021) (denying in part Lululemon's motion to dismiss plaintiff's CIPA 631(a)(iv) claim for aiding in wiretapping, premised on Lululemon's use of Quantum Metric session replay software on its website).

[77]*See, e.g.*, *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 685 (N.D. Cal. 2021) (dismissing plaintiffs' claim for failing to allege that their own communications were intercepted or disclosed, as opposed to those potentially of others, in a putative data privacy suit alleging that Apple disclosed private information without consent in violation of various privacy laws, based on a newspaper article in the *Guardian*); *Kirch v. Embarq Management Co.,* No. 10-2047-JAR, 2011 WL 3651359, at *7-9 (D. Kan. Aug. 19, 2011) (granting summary judgment for the defendant on plaintiff's claim in a putative class action suit where the court found that a third party, rather the defendant, intercepted the plaintiff's communications), *aff'd*, 702 F.3d 1245, 1246–47 (10th Cir. 2012) (holding that section 2520 does not impose civil liability on aiders or abettors), *cert. denied*, 569 U.S. 1013 (2013).

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

was collected in the ordinary course of business.[79]

The Stored Communications Act, which is Title II of ECPA, prohibits both unauthorized access (or exceeding authorized access) that alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in section 2701,[80] subject to exceptions for access by the person or entity providing a wire or electronic communications service[81] and by a user of that service with respect to a communication of or intended for that user;[82] and knowingly divulging the contents of a communication while in electronic storage in section 2702,[83] subject to exceptions including to an addressee or intended recipient of such communication,[84] where authorized[85] and with lawful consent.[86] Adtech, behavioral advertising and other data privacy 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

---

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

[80]18 U.S.C.A. § 2701(a). Authorization may be given for a limited purpose. In *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 838 (8th Cir. 2015), for example, the Eighth Circuit stated in *dicta* that where a defendant gave his ex-girlfriend his Gmail user name and password so that she could send his resume to a prospective employer, and only for that purpose, subsequent access to the account would be deemed unauthorized under the SCA.

[81]18 U.S.C.A. § 2701(c)(1).

[82]18 U.S.C.A. § 2701(c)(2).

[83]18 U.S.C.A. § 2702(a).

[84]18 U.S.C.A. § 2702(b)(1).

[85]18 U.S.C.A. § 2702(b)(2).

[86]18 U.S.C.A. § 2702(b)(3).

storage by that service."[87] However, a provider of an electronic communication service may divulge the contents of a communication to an addressee or intended recipient of such communication.[88] 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.[89] Allegations that an ECS provider accessed information for its own purposes likewise will fail.[17]

---

[87]18 U.S.C.A. § 2702(a)(1).

[88]18 U.S.C.A. § 2702(b)(1).

[89]18 U.S.C.A. § 2702(b)(3).

[17]*See, e.g.*, *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 625-28 (N.D. Cal. 2021) (dismissing plaintiffs' Stored Communications Act claim, in a suit alleging that Google collected user data from users of the Chrome browser who chose not to sync their browser histories with their Google accounts, because "[t]he Wiretap Act and the SCA prohibit 'the person or entity providing [the ECS]' from divulging the contents of any communication to any person or entity, but Plaintiffs do not allege that Google divulged the contents of any communication to a third party. Rather, Plaintiffs allege that Google divulged information to itself. . . . Accordingly, Plaintiffs' unauthorized disclosure claims under the Wiretap Act and the SCA fail."; "the SCA provides an exception from liability for 'conduct authorized . . . by the person or entity providing' the alleged ECS. 18 U.S.C. § 2701(c)(1). . . . Google is the entity providing the ECS because Google provides the Chrome browser, which is a Google service. . . . Google was the entity allegedly collecting Plaintiffs' data. Accordingly, Google, the entity providing the ECS, authorized the alleged collection of data. Because the alleged misconduct was authorized by the entity providing the ECS, Google is not subject to liability under the SCA's unauthorized access provision."); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 822 (N.D. Cal. 2020) (dismissing plaintiffs' SCA claim for unauthorized disclosure, premised on the allegation that Google Assistant disclosed audio or transcripts to Google. because the plaintiffs did not allege that Google had divulged the information to a third party, and "[Google's] own use of Plaintiffs' data for advertising purposes does not constitute an unlawful 'disclosure.' "); *Heeger v. Facebook, Inc*., Case No. 18-cv-06399-JD, 2019 WL 7282477, at *3 (N.D. Cal. Dec. 27, 2019) (dismissing plaintiffs' claim because "he alleges only that Facebook collected users' location 'data,' and not the contents of communications, even assuming Facebook "divulged" that data to third parties."); *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1026-27 (N.D. Cal. 2014) ("The SCA grants immunity to 18 U.S.C. § 2701(a) claims to electronic communication service providers . . . for accessing content on their own servers."); *In re Google, Inc. Privacy Policy Litig*., No. C-12-01382-PSG, 2013 WL 6248499, at *12 (N.D. Cal. Dec. 3, 2013) ("Whatever the propriety of Google's actions, it plainly authorized actions that it took itself.").

Because section 7201 addresses a knowing disclosure, it may not provide the basis for a claim based on a security breach, where the defendant-company typically is a victim that did not know about the incursion.[90] In *In re Facebook, Inc. Internet Tracking Litig.*,[18] the Ninth Circuit affirmed dismissal of plaintiffs' section 2701(a) claim where the information allegedly accessed (GET requests allegedly showing URLs accessed by users on third party websites) was not in electronic storage.

In *In re Facebook Privacy Litigation*,[91] the court dismissed plaintiffs' Title II claim alleging that by clicking on a banner advertisement, users unknowingly were transmitting information to advertisers, because the communication at issue either was sent to Facebook or to third party advertisers. As explained by the court:

> Under either interpretation, Plaintiffs fail to state a claim under the Stored Communications Act. If the communications were sent to Defendant, then Defendant was their "addressee or intended recipient," and thus was permitted to divulge the communications to advertisers so long as it had its own "lawful consent" to do so. 18 U.S.C. § 2702(b)(3). In the alternative, if the communications were sent to advertisers, then the advertisers were their addressees or intended recipients, and Defendant was permitted to divulge the communications to them. *Id.* § 2702(b)(1).[92]

Plaintiffs' Title I claim against Facebook likewise suffered from a similar defect in that case. The court ruled that a

---

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

[18] *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608-09 (9th Cir. 2020) (affirming dismissal of plaintiffs' SCA claim because the copy of the URL shown in a user's toolbar was wholly separate from the GET requests that Facebook allegedly duplicated and forwarded to its servers—and was made available solely for the user's convenience—and therefore not stored "incident to transmission" and not in *electronic storage*), *cert. denied,* 141 S. Ct. 1684 (2021).

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

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

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.[93]

In *Low v. LinkedIn Corp.*,[94] 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).[95] In so holding, the court explained that LinkedIn IDs were numbers generated by LinkedIn, not user data sent by users for offsite storage and processing. URL addresses of viewed pages similarly were not sent to LinkedIn by plaintiffs for storage or processing.[96]

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. As articulated by the Ninth

---

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

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

[95]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).

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

Circuit, a plaintiff must show that a defendant "(1) gained unauthorized access to a 'facility' where it (2) accessed an electronic communication in 'electronic storage.' "[19]

Section 2701 requires a showing that a defendant accessed without authorization "a facility through which an electronic communication service is provided."[97] "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, . . ."[98] 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.[99] As explained by one judge, "courts have distinguished facilities that *provide* an electronic communication service—

---

[19]*In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 608 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1684 (2021).

[97]18 U.S.C.A. § 2701(a)(1). A *facility,* according to the Eleventh Circuit, includes "the physical means or equipment for doing something." *Brown Jordan Int'l, Inc. v. Carmicle,* 846 F.3d 1167, 1177 n.4 (11th Cir. 2017) (quoting Oxford English Dictionary Online). As explained by the Third Circuit, " 'facility' is a term of art denoting where network service providers store private communications." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 147 (3d Cir. 2015), *cert. denied,* 137 S. Ct. 36 (2016); *see also Decoursey v. Sherwin-Williams Co.*, No. 19-02198-DDC-GEB, 2020 WL 1812266, at *6 (D. Kan. Apr. 9, 2020) (holding that Facebook's server qualified as a facility under the SCA); *see generally infra* § 44.08[1] (analyzing *facility* in greater detail).

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

[99]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 146-48 (3d Cir. 2015) (holding that a user's web browser could not constitute a facility), *cert. denied,* 137 S. Ct. 36 (2016); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 627-28 (N.D. Cal. 2021) (dismissing plaintiffs' Stored Communications Act claim, in a suit alleging that Google collected user data from users of the Chrome browser who chose not to sync their browser information with their Google accounts, because "plaintiffs' personal computing devices are not facilities"; "The SCA does not provide a statutory definition of facility. . . . However, the SCA specifies that a facility must be one "through which an [ECS] is provided." 18 U.S.C. § 2701(a)(1). Based on this language, several 'courts in this Circuit and others have interpreted 'facility' to exclude users' personal devices.' ") (quoting *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 820-21); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 820-22 (N.D. Cal. 2020) (rejecting the argument that plaintiffs' devices' RAM could constitute the facility from which their communications were accessed "while they were temporarily stored" there); *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017)

such as an email provider's servers or an ISP—from those that merely *enable* the electronic communication service—such as a user's personal computer or phone."[20]

Similarly, claims premised on information stored on user devices will be difficult to maintain because the data at issue may not deemed to be in *electronic storage*. In addition to showing that a defendant intentionally accessed a facility through which an electronic communication service is provided without authorization (or exceeded authorized access), to state a claim under the Stored Communications Act a plaintiff also must show that the defendant, through this unauthorized access, "thereby obtains, alters, or prevents authorized access to a wire or electronic communication

---

(dismissing plaintiff's amended SCA claim because, among other things, personal computers are not "facilities" under the SCA), *aff'd on other grounds,* 956 F.3d 589, 608-09 (9th Cir. 2020) (affirming dismissal of plaintiffs' SCA claim because the copy of the URL shown in a user's toolbar was wholly separate from the GET requests that Facebook allegedly duplicated and forwarded to its servers—and was made available solely for the user's convenience—and therefore not stored "incident to transmission" and not in *electronic storage*), *cert. denied,* 141 S. Ct. 1684 (2021); *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.

[20]*Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 686 (N.D. Cal. 2021) (emphasis in the original) (holding that Siri was not a facility and therefore dismissing plaintiffs' claim under section 2701(a)(1); "First, Siri is software and not a 'facility' under any common sense of the term. Second, Plaintiffs do not allege that Siri provides an 'electronic communication service'—they allege that it enables 'a variety of tasks,' such as setting alarms and responding to questions. . . . Third, the statute exempts from liability 'conduct authorized [ ] by the person or entity providing a wire or electronic communication service.' 18 U.S.C. § 2701(c). Apple is the service provider here and presumably authorized its own conduct.").

while it is in electronic storage . . . ."[100] *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."[101] Where the information accessed is stored on a user's device (or in a cookie file[102] or a browser's toolbar and browsing history,[103] or on a universally unique device identifier (UUID)[104] used in connection with advertising or email stored on a user's own

---

[100]18 U.S.C.A. § 2701(a).

[101]18 U.S.C.A. § 2510(17).

[102]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal. 2015) (dismissing plaintiffs' SCA claim because "Plaintiff's theory . . . —that Facebook accesses personal information through persistent cookies permanently residing in users' personal web browsers—cannot be reconciled with the temporary nature of storage contemplated by the statutory definition."), *aff'd on other grounds*, 956 F.3d 589, 608-09 (9th Cir. 2020) (affirming dismissal of plaintiffs' SCA claim because the copy of the URL shown in a user's toolbar was wholly separate from the GET requests that Facebook allegedly duplicated and forwarded to its servers—and was made available solely for the user's convenience—and therefore not stored "incident to transmission" and not in *electronic storage*; "Plaintiffs' interpretation of the SCA would stretch its application beyond its limits."), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 447 (D. Del. 2013) (explaining, in connection with dismissing plaintiff's SCA claim, that "[t]here seems to be a consensus that '[t]he cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and, hence, [the SCA's] protection"), *aff'd in relevant part on other grounds*, 806 F.3d 125, 146-48 (3d Cir. 2015) (affirming dismissal of plaintiffs' SCA claim because a user's web browser could not constitute a facility), *cert. denied*, 137 S. Ct. 36 (2016); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512–13 (S.D.N.Y. 2001); *In re Toys R Us, Inc. Privacy Litig.,* No. 00-CV-2746, 2001 WL 34517252, at *4 (N.D. Cal. Oct. 9, 2001).

[103]*See In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017) (dismissing plaintiff's amended SCA claim because, among other things, the tool bar and browser history are "stored locally on the user's personal computer for the user's convenience."), *aff'd*, 956 F.3d 589, 608-09 (9th Cir. 2020) (affirming dismissal of plaintiffs' SCA claim because the copy of the URL shown in a user's toolbar was wholly separate from the GET requests that Facebook allegedly duplicated and forwarded to its servers—and was made available solely for the user's convenience—and therefore not stored "incident to transmission" and not in *electronic storage*), *cert. denied*, 141 S. Ct. 1684 (2021).

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

computer[105] or a Blackberry mobile device[106]), the information is not in *electronic storage*[107] as defined in the Act.[108]

As explained by one court, "[t]itle II deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers."[109] In other

---

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

[106]*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.").

[107]Under the statute, 'electronic storage' means (1) 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,' or (2) 'any storage of such communication by an electronic communication service for purposes of backup protection of such communication.' " *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 839 (8th Cir. 2015), *quoting* 18 U.S.C.A. § 2510(17). In *Anzaldua*, the court held that a draft email was not in *electronic storage*; "because the email had not been sent, its storage on the Gmail server was not 'temporary, intermediate,' and 'incidental to the electronic transmission thereof.' " 793 F.3d at 840, *quoting* 18 U.S.C.A. § 2510(17). Likewise, the sent version of the same email was not stored for backup purposes; Gmail stores sent messages as a matter of course, not as a duplicate backup. 793 F.3d at 840-42 (noting disagreement among various courts about what constitutes backup). As the Eighth Circuit explained, the SCA "is not a catch-all statute designated to protect the privacy of stored Internet communications; instead, it is narrowly tailored to provide a set of Fourth-Amendment-like protections for computer networks." *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 839 (8th Cir. 2015), *quoting* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004).

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

[109]*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).

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."[110] 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."[111] 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).[112] For purposes of ECPA, consumers or other *end users* are not the

---

[110]18 U.S.C.A. § 2701(c)(2).

[111]18 U.S.C.A. § 2510(13).

[112]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274-76 (3d Cir. 2016) (affirming dismissal of plaintiffs' Wiretap claim, holding that "Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications."), *cert. denied*, 137 S. Ct. 624 (2017); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1060 (N.D. Cal. 2012) (holding that "because the 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). *But see In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607-08 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1684 (2021) (disagreeing with the Third Circuit, holding that "entities that surreptitiously duplicate transmissions between two parties are not parties to the communication within the meaning of the Act."); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 623-24 (N.D. Cal. 2021) (holding that Google could not meet its burden of establishing implied consent that "websites consented to, or even knew about," the alleged interception of a subset of communications with users

users referenced by the statute.[113] In the nomenclature of the statute, end users, or consumers, are referred to as *customer* or *subscribers*.[114]

Pursuant to section 2511(2)(d), a website operator also may be deemed an intended recipient of communications, such as data included in website cookies[115] or otherwise on a user's hard drive.[116]

---

who used Chrome without the sync feature, at the outset of the case on a motion to dismiss where plaintiff's allegations are presumed accurate, based solely on the terms of the privacy policy applicable to Chrome).

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

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

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

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

[115]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 140-45 (3d Cir. 2015) (affirming dismissal of plaintiffs' Wiretap Act claim where plaintiffs alleged that "defendants acquired the plaintiffs' internet history information when, in the course of requesting webpage advertising content at the direction of the visited website, the plaintiffs' browsers sent that information directly to the defendants' servers. Because the defendants were the intended recipients of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to the defendants' servers— . . . § 2511(2)(d) means the defendants have done nothing unlawful under the Wiretap Act."), *cert. denied*, 137 S. Ct. 36 (2016).

[116]*See, e.g.*, *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389,

In addition, mistaken disclosures are not actionable under the Stored Communications Act. In *Long v. Insight Communications of Central Ohio, LLC*,[117] the defendant had mistakenly provided the wrong subscriber information in response to a subpoena in a child pornography investigation. The Bureau of Criminal Investigation traced several hundred files containing child pornography to a particular IP address. Investigators requested a grand jury subpoena requiring Time Warner Cable to provide subscriber information linked to the IP address. TWC complied, but mistakenly disclosed subscriber information tied to a different IP address. The person wrongly misidentified and his family sued under the SCA (and for state law claims). In dismissing plaintiffs' putative class action suit, the Sixth Circuit held that the requirements that SCA violations be undertaken *knowingly* and *intentionally* were not met when the defendant did not realize that it was providing the wrong subscriber information in response to the subpoena. The Sixth Circuit held that to impose liability under section 2707(a), there must be "a showing that the provider knew not only that it was divulging information (i.e., that the act of disclosure was not inadvertent), but also what information was being divulged (i.e., the facts that made the disclosure unauthorized)."[118]

Further, even when a Stored Communications Act claim can be stated, at least two circuits have held that a plaintiff may not recover statutory damages under the SCA unless he or she has incurred actual damages.[119]

In addition to user authorization, both Title I and Title II

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

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

[118]*Long v. Insight Communications of Central Ohio, LLC*, 804 F.3d 791, 797 (6th Cir. 2015). The Sixth Circuit also affirmed the district court's rulings that, on the same facts, the defendant did not commit intentional disclosure of private information under Ohio law, intentional infliction of emotional distress or breach of contract.

[119]*See Van Alstyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199, 208

of ECPA create express exceptions where consent has been obtained from customers or subscribers.[120] 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.[121]

Courts have entered judgment for the defendant or dismissed putative privacy class action suits where consent was inferred from TOU or a Privacy Policy (under both ECPA[122] and equivalent state laws[21]).

In contrast to Title II, Title I addresses communications in

(4th Cir. 2009); *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 965 (11th Cir. 2016).

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

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

[122]*See, e.g.*, *Williams v. Affinion Group, LLC*, 889 F.3d 116, 120-23 (2d Cir. 2018) (affirming summary judgment for defendants on the ECPA claims of former participants in an online membership program, in a putative class action suit, finding consent under section 2511(2)(d) based on their acceptance of website Terms & Conditions); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' claims under the Wiretap Act, Stored Communications Act, and Cal. Penal Code § 631(a) where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in the terms of the defendant's Privacy Policy); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953, 955 (N.D. Cal. 2017) (dismissing putative class claims under the Wiretap Act, California Constitution, California Information Privacy Act, and for California common law invasion of privacy, for allegedly sharing sensitive medical information, based on consent provided pursuant to Facebook's Data Policy and Cookie Policy), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("He who consents to an act is not wronged by it." (quoting Cal. Civ. Code § 3515)); *Cain v. Redbox Automated Retail, LLC*, 136 F. Supp. 3d 824 (E.D. Mich. 2015) (granting summary judgment in favor of Redbox on plaintiffs' Michigan Video Rental Privacy Act, breach of contract and unjust enrichment claims in a putative class action suit where the plaintiffs provided written permission to Redbox to allow it to disclose information as set forth in its Privacy Policy); *Garcia v. Enterprise Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing plaintiff's California Invasion of Privacy Act claim with leave to amend where the

defendant—app provider's Terms of Use and Privacy Policy provided consent for the alleged disclosures); *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1027-31 (N.D. Cal. 2014) (granting defendant's motion to dismiss with prejudice plaintiffs' Wiretap Act claim based on the allegation that Yahoo scanned and analyzed emails to provide personal product features and targeted advertising, detect spam and abuse, create user profiles, and share information with third parties, and stored email messages for future use based on explicit consent set forth in the Yahoo Global Communications Additional Terms of Service for Yahoo Mail and Yahoo Messenger agreement); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1211-14 (N.D. Cal. 2014) (dismissing Wiretap Act and SCA claims because plaintiffs consented to LinkedIn's collection of email addresses from users' contact lists through LinkedIn's disclosure statements); *Del Vecchio v. Amazon.com, Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (dismissing, with leave to amend, a trespass and CFAA claim based on the alleged use of browser and flash cookies where, among other things, the potential use of browser and flash cookies was disclosed to users in the defendant's "Conditions of Use and Privacy Notice"); *Kirch v. Embarq Management Co.,* No. 10-2047-JAR, 2011 WL 3651359, at *7–9 (D. Kan. Aug. 19, 2011) (holding, in granting summary judgment for the defendant, that the plaintiffs consented to the use by third parties of their de-identified web-browsing behavior when they accessed the Internet under the terms of Embarq's Privacy Policy, which was incorporated by reference into its Activation Agreement, and which provided that de-identified information could be shared with third parties and that the Agreement could be modified; and because the Policy was amended in advance of the NebuAd test to expressly disclose the use and allow users to opt out by clicking on a hypertext link), *aff'd on other grounds*, 702 F.3d 1245 (10th Cir. 2012), *cert. denied*, 569 U.S. 1013 (2013); *Deering v. CenturyTel, Inc.*, No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011) (dismissing plaintiff's ECPA claim based on the terms of defendant's privacy policy and an email sent to subscribers advising them that the Policy had been updated, in a putative class action suit over sharing of cookie and web beacon data); *Berry v. Webloyalty.com, Inc.*, No. 10-CV-1358-H CAB, 2011 WL 1375665, at *8 (S.D. Cal. Apr. 11, 2011) (in dismissing an ECPA claim over the "Shopper Discounts and Rewards" program, "[t]he Court conclude[d] that Plaintiff Berry's entry of his email address twice and clicking on 'YES' constitute[d] authorization given the several disclosures made on the enrollment page"), v*acated and remanded for lack of standing*, 517 F. App'x 581 (9th Cir. 2013); *Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13, 2010) (dismissing plaintiff's ECPA claim where the defendant-ISP provided notice to consumers in its Privacy Notice and Subscriber Agreement that their electronic transmissions might be monitored and would in fact be transferred to third parties, and also provided specific notice via a link on its website of its use of the NebuAd Appliance to transfer data to NebuAd and of subscribers' right to opt out of the data transfer (via a link in that notice)), *vacated on other grounds*, 722 F.3d 1151 (9th Cir. 2013) (holding that the lower court erred in declining to compel arbitration); *supra* § 26.14[2] (analyzing these cases). *But see Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 685 (N.D. Cal. 2021) (deny-

transit (or temporary, intermediate storage). In *In re iPhone Application Litigation*,[123] the court held that geolocation data stored for up to a one-year time period did not amount to "temporary, intermediate storage . . . incidental to the electronic transmission . . ." of an electronic

---

ing defendant's motion to dismiss plaintiff's Wiretap Act claim based on consent, holding that a provision in Apple's Software License Agreement stating that Siri's operation may not be "error free" was a "general disclaimer . . . nowhere near specific and unambiguous enough to represent that Siri may activate by accident."); *In re Google Inc. Gmail Litig.,* Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *12-15 (N.D. Cal. Sept. 26, 2013) (denying Google's motion to dismiss based on the court's finding that it did not have express or implied consent within the meaning of 18 U.S.C.A. § 2511(2)(d) to intercept incoming email to create profiles to send targeted advertising to recipients based on its Terms of Service and Privacy Policy); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1076–77 (N.D. Cal. 2012) (denying plaintiffs' motion to dismiss claims in a putative class action suit where the court found some ambiguity in the defendant's Terms and Conditions); *In re Vistaprint Corp. Marketing & Sales Practices Litig.*, MDL No. 4:08-md-1994, 2009 WL 2884727, at *9 (S.D. Tex. Aug. 31, 2009) (dismissing ECPA claim where plaintiffs, "by clicking Yes in the designated spaces on the webpages, authorized VistaPrint to transfer that information" to the "VistaPrint Rewards" program).

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

[21]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *2-5 (N.D. Cal. July 28, 2021) (dismissing wiretap claims under California, Florida, and Washington state law (Cal. Penal Code §§ 631(a), 635; Fla. Stat. Ann. § 934.03(2)(d) (permitting interception of a communication "when all of the parties to the communication have given prior consent"); Wash. Rev. Code Ann. §§ 9.73.030(1) (a)-(b) (permitting interception with "the consent of all the participants")), where plaintiffs provided consent by assenting to Instacart's Privacy Policy, which set forth, among other things, that Instacart could share information payment processor partners and third parties); *Javier v. Assurance IQ, LLC*, Case No. 4:20-cv-02860-JSW, 2021 WL 940319, at *2-4 (N.D. Cal. Mar. 9, 2021) (dismissing plaintiff's claims under the California Invasion of Privacy Act (CIPA) and California Constitution, where the plaintiff had given click-through assent to Assurance's Privacy Policy, which made clear that Assurance tracked activity on its website and stated that it may use third party vendors to do so).

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

communication.[124]

Title I claims also may fail where they are brought over information that is "readily accessible to the general public,"[125] such as material posted on a website[126] 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."[127]

Given the number of parties involved in online and mobile advertising, some suits have sought to hold defendants liable for third party practices. Where direct liability cannot be established under ECPA, however, civil claims may not be maintained based on aider and abettor, conspiracy or secondary liability.[128]

---

[124]18 U.S.C.A. § 2510(17).

[125]*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 . . . .").

[126]*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).

[127]*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).

[128]*See, e.g.*, *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 168–69 (5th Cir. 2000), *cert. denied*, 532 U.S. 1051 (2001); *Doe v. GTE Corp.*, 347 F.3d 655, 658 (7th Cir. 2003) ("[N]othing in the statute condemns assistants, as opposed to those who directly perpetrate the act."); *Reynolds v. Spears*, 93 F.3d 428, 432–33 (8th Cir. 1996); *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1005-06 (9th Cir. 2006) (affirming dismissal of plaintiff's Stored Communications Act claim and rejecting the argument that "a person or entity who aids and abets or who enters into a conspiracy is someone or something that is 'engaged' in a violation."); *Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1246-47 (10th Cir. 2012) (holding that section 2520

To state a civil claim for a violation of the Computer Fraud and Abuse Act (CFAA), a plaintiff must allege at least a $5000 loss,[129] which is a threshold that bars many consumer data privacy claims—especially those based on behavioral advertising where there is no economic loss or (injury) or merely *de minimis* damage. The $5,000 threshold requirement alone has proven to be an insurmountable bar in many data privacy cases.[130] Courts also have been reluctant to

---

"does not impose civil liability on aiders or abettors."), *cert. denied*, 569 U.S. 1013 (2013); *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1007 (N.D. Cal. 2017) (holding that the plaintiff could not assert claims based on secondary liability; "Plaintiff has grouped the Defendants together and appears to argue she can establish liability by showing concerted action. However, in order to state a claim, Plaintiff must be able to allege that each Defendant engaged in conduct that directly violates the Wiretap Act."); *In re: Carrier IQ, Inc. Consumer Litig.*, 78 F. Supp. 3d 1051, 1089-90 (N.D. Cal. 2015) (dismissing plaintiffs' Wiretap Act claim where plaintiffs did not allege that the device manufacturers acquired the contents of any of plaintiffs' communications because "there is simply no secondary liability (such as aiding and abetting) under the ECPA"); *Byrd v. Aaron's, Inc.*, 14 F. Supp. 3d 667, 675 (W.D. Pa. 2014) (dismissing plaintiff's claim of conspiracy to commit ECPA violations because "secondary liability no longer exists under the current statutory structure of the ECPA."); *Shefts v. Petrakis*, 954 F. Supp. 2d 769, 774-76 (C.D. Ill. 2013) (granting summary judgment because "Defendant Morgan cannot be held liable under the ECPA under 'procurement,' 'agency,' 'conspiracy,' or any other 'secondary' theories of liability . . . ."); *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 891 F. Supp. 2d 13, 23–24 (D.D.C. 2012) (holding that there is no cause of action under ECPA for secondary 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].

[129]18 U.S.C.A. §§ 1030(c)(4)(A)(i), 1030(g). A civil CFAA claim where a $5,000 loss need not be shown may be made on limited grounds generally not applicable to data privacy cases. *See id.; infra* § 44.08[1] (analyzing the statutory provisions in greater detail).

[130]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 148-49 (3d Cir. 2015) (affirming dismissal of plaintiffs' CFAA claim for failure to allege the threshold loss of $5,000 required to state a civil claim under the CFAA, where they could not allege any viable lost marketing opportunity for their data), *cert. denied*, 137 S. Ct. 36 (2016); *Andrews v. Sirius XM Radio Inc*., 932 F.3d 1253, 1262-63 (9th Cir. 2019) (denying leave to amend for plaintiff to add a CFAA claim as futile, where he alleged that he was denied the profits he might have received from commodifying his personal information (which Sirius XM allegedly obtained through unlawful means), because the concept of *loss* under the CFAA is narrow and "refers *only* to losses that occurred 'because of interruption of service.' 18 U.S.C. § 1030(e)(11) . . . ;" The CFAA is an anti-

hacking statute, not a misappropriation statute, and "[t]he statute's 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself."); *Cottle v. Plaid Inc*., Case No. 20-cv-03056-DMR, 2021 WL 1721177, at *15-16 (N.D. Cal. Apr. 30, 2021) (dismissing plaintiffs' claim, which alleged at least $5,000 in lost value of indemnification rights, as based on speculative allegations of loss, and rejecting arguments that the monetary threshold could be met by allegations of loss of the right to control his own data, loss of the value of his data, or loss of the right to protection of the data); *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 634 (N.D. Cal. 2021) (dismissing plaintiffs' CFAA claim, in a suit alleging that Google collected user data from people using the Chrome browser who chose not to sync their browser histories with their Google accounts, where plaintiffs did not allege $5,000 in loss caused by the alleged violation); *Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *8-9 (S.D.N.Y. Aug. 17, 2016) (dismissing plaintiffs' CFAA claim in a suit based on alleged use of tracking cookies), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017); *In re Google Android Consumer Privacy Litig.*, No. 11–MD–02264 JSW, 2014 WL 988889, at *4 (N.D. Cal. Mar. 10, 2014) (dismissing plaintiff's amended CFAA claim without leave to amend based on plaintiffs' inability to allege $5,000 in damages based on diminished battery life and data plan use); *In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *7 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's CFAA claim in a suit brought over the alleged sharing of information between the Android Market and advertisers, with leave to amend); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *10 (N.D. Cal. Mar. 26, 2013) (dismissing with leave to amend plaintiff's CFAA claim in a behavioral advertising putative class action suit where the plaintiff alleged diminished memory storage but did not allege $5,000 in damages); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066–67 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' CFAA claim premised on the cost of memory space on class members' iPhones as a result of storing allegedly unauthorized geolocation data); *Del Vecchio v. Amazon.com, Inc.*, No. C11–366RSL, 2012 WL 1997697 (W.D. Wash. Jun. 1, 2012) (dismissing with prejudice plaintiff's CFAA claim for failure to allege $5,000 in damages); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *4 (W.D. Wash. Dec. 1, 2011) (dismissing, with leave to amend, a CFAA claim based on the alleged use of browser and flash cookies for failure to allege $5,000 in damages or any injury, and questioning in *dicta* whether plaintiffs, in an amended complaint, could allege unauthorized access under the CFAA where the use of browser and flash cookies was disclosed to users in the defendant's "Conditions of Use and Privacy Notice"); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice a CFAA claim alleging general impairment to the value of plaintiff's computer in a putative behavioral advertising class action suit); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011); *Czech v. Wall Street on Demand, Inc.*, 674 F. Supp. 2d 1102 (D. Minn. 2009) (dismissing a class action based on allegedly unauthorized text messages sent to plaintiffs' phones where

treat the disclosure of personal information as having economic value,[131] at least in the absence of any evidence to the

---

plaintiffs merely alleged in conclusory fashion that the unwanted text messages depleted RAM and ROM, causing phone functions to slow down and lock up, caused phones to shut down, reboot or reformat their memory, interfered with bandwidth and hard drive capacity); *Fink v. Time Warner Cable,* No. 08 Civ. 9628 (LTS) (KNF), 2009 WL 2207920, at *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because the plaintiff merely alleged damage by "impairing the integrity or availability of data and information," which was "insufficiently factual to frame plausibly the damage element of Plaintiff's CFAA claim"); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *see generally supra* § 5.06 (CFAA case law on database law and screen scraping); *infra* § 44.08 (analyzing the CFAA and case law construing it in greater detail).

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

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

Id. at 149.

[131] *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 148-49 (3d Cir. 2015) (affirming dismissal of plaintiffs' CFAA claim for failure to allege the threshold loss of $5,000 required to state a civil claim under the CFAA, where they could not allege any viable lost marketing opportunity for their data), *cert. denied*, 137 S. Ct. 36 (2016); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1068 (N.D. Cal. 2012); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *3 (W.D. Wash. Dec. 1, 2011) (dismissing plaintiff's CFAA claim, with leave to amend, noting that "[w]hile it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this

contrary.

To state a CFAA claim, a plaintiff also must establish that a defendant accessed a protected computer "without authorization" or "exceeded authorized access."[132] CFAA violations premised on exceeding use (rather than access) restrictions, such as use restrictions found in a Privacy Policy, Terms of Use or company policy, are no longer viable where access otherwise was permitted.[133] As explained by the Second Circuit, a person exceeds authorized access "only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access."[134] A person cannot exceed authorized access, within the meaning of the CFAA, by accessing a computer "with an improper purpose . . . . to obtain or alter information that he is otherwise authorized to access . . . . "[135]

Authorization similarly may be difficult to show in some

---

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.").

[132]18 U.S.C.A. § 1030(a)(4); *see generally infra* § 44.08[1] (analyzing the CFAA in greater detail).

[133]*See Van Buren v. United States*, 141 S. Ct. 1648, 1662 (2021) (resolving a circuit split, holding that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him."); *see also U.S. v. Valle*, 807 F.3d 508, 524–28 (2d Cir. 2015); *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 203-06 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); Royal Truck & *Trailer Sales & Service, Inc. v. Kraft*, 974 F.3d 756, 759-63 (6th Cir. 2020); *U.S. v. Nosal*, 676 F.3d 854, 856-63 (9th Cir. 2012) (*en banc*); *supra* § 5.06 (analyzing the CFAA in connection with Terms of Service restrictions); *infra* § 44.08[1] (analyzing this issue in greater detail).

In *Van Buren*, the Supreme Court declined to address whether access restrictions must be based on "technological (or 'code-based') limitations" to be actionable, or whether they also could be "contained in contracts or policies." *Van Buren v. United States*, 141 S. Ct. 1648, 1659 n.8 (2021).

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

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

data privacy cases where the plaintiff voluntarily downloaded the application that is challenged in the litigation.[136]

In *In re iPhone Application Litigation*,[137] 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.[138]

Numerous putative class action suits have been filed under the Video Privacy Protection Act, which may be brought against a "video tape service provider who knowingly discloses, to any person, personally identifiable information" about the consumer.[139] 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 . . . ."[140] The Senate Report accompanying the bill clarifies that "similar audio visual materials" include such things as "laser discs, open -reel movies, or CDI technol-

---

[136]*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.

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

[138]*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.").

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

[140]*See* 18 U.S.C.A. § 2710(a)(4).

ogy . . . ,"[141] which was a technology for delivering movies on CD-like disks. All of these *materials* involve video stored on tangible media. Nevertheless, this argument about the inapplicability of the VPPA to online video players has not yet been addressed by any court.[142]

As analyzed more extensively in section 26.13[10], a VPPA suit will be unsuccessful where a plaintiff cannot establish a *knowing* disclosure,[143] if the information disclosed does not qualify as PII under the VPPA's statutory definition,[144] or

---

[141]S. Rep. No. 100-599, 100th Cong. 2d Sess. 9, 12 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 3435-9 to 3435-10; *see generally supra* § 26.13[10] (expanding on this argument).

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

[143]*See, e.g.*, *Bernardino v. Barnes & Noble Booksellers, Inc.*, 17-CV-04570 (LAK) (KHP), 2017 WL 3727230, at *9 (S.D.N.Y. Aug. 11, 2017) (recommending that plaintiff's motion for a preliminary injunction be denied, in part, because the plaintiff had not demonstrated the likelihood of "proving that Barnes & Noble 'knowingly' made a disclosure of PII"), *report and recommendation adopted*, 2017 WL 3726050 (S.D.N.Y. Aug. 28, 2017); *In re: Hulu Privacy Litig.*, 86 F. Supp. 3d 1090 (N.D. Cal. 2015) (granting summary judgment for Hulu because there was no evidence of knowledge); *see generally supra* § 26.13[10] (analyzing the VPPA in greater detail).

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

because a cause of action under the VPPA may only be maintained for knowing disclosures, not the failure to delete information within the statutorily prescribed time limit[145] or for the receipt (rather than disclosure) of PII.[146] Several suits also have been dismissed because users of free mobile apps or website video players may not qualify as *consumers* eligible to sue under the statute (although there is a split of authority between the First and Eleventh Circuits on this point).[147]

Claims under the Driver's Privacy Protection Act,[148] which was modeled in part on the VPPA, may not be viable unless the plaintiff's personal information was disclosed by a state

---

5023535, at *3 (N.D. Ga. Oct. 8, 2014) (dismissing plaintiff's Video Privacy Protection Act claim because an Android ID is not "personally identifiable information"), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015). *But see Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016) (holding that a user's GPS coordinates and the Android ID of a user's smart phone plausibly constituted PII under the VPPA); *see generally supra* § 26.13[10] (analyzing these cases).

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

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

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

[148]18 U.S.C.A. §§ 2721 to 2725; *supra* § 26.13[11] (analyzing the DPPA).

DMV, not a third party.[149]

Class action lawyers also have tried to frame claims under federal statutes that do not allow for a private right of action by individuals, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[22] and the Children's Online Privacy Protection Act (COPPA).[23] Courts, however, generally have rejected disguised HIPAA claims framed in terms of breach of contract,[24] as well as under other theories

---

[149]*See Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1259-62 (9th Cir. 2019) (affirming dismissal of plaintiff's putative class action suit, where Sirius XM allegedly obtained plaintiff's name and telephone number (which constitute PII under the statute) for an impermissible use under the DPPA, but obtained it from a third party (the car dealership that sold him a pre-owned vehicle that came equipped with Sirius XM radio), not a state DMV).

To state a civil claim, a plaintiff must show that a defendant (1) knowingly obtained, disclosed, or used his or her personal information, (2) from a motor vehicle record, (3) for a purpose not permitted under the statute. *See* 18 U.S.C.A. § 2724(a); *Taylor v. Acxiom Corp.*, 612 F.3d 325, 335 (5th Cir. 2010); *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1259 (9th Cir. 2019); *Chevaldina v. Katz*, 787 F. App'x 651 (11th Cir. 2019), *citing Thomas v. George, Hartz, Lundeen, Fulmer, Johnstone, King, and Stevens, P.A.*, 525 F.3d 1107, 1112 (11th Cir. 2008). The plaintiff has the burden of proving that the purpose for the defendant's use was impermissible. *Thomas*, 525 F.3d at 1112.

[22]The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub.L. No. 104–191, 110 Stat.1936 (1996) (codified primarily in Titles 18, 26 and 42 of the United States Code); *see generally supra* § 26.11. HIPAA generally provides for confidentiality of medical records. 42 U.S.C. §§ 1320d–1 to d–7. HIPAA does not afford a private right of action, either express or implied. *See, e.g.*, *Meadows v. United Services, Inc.*, 963 F.3d 240, 244 (2d Cir. 2020); *Acara v. Banks*, 470 F.3d 569, 570–72 (5th Cir. 2006); *Faber v. Ciox Health, LLC*, 944 F.3d 593, 596–97 (6th Cir. 2019); *Stewart v. Parkview Hospital*, 940 F.3d 1013, 1015 (7th Cir. 2019); *Carpenter v. Phillips*, 419 F. App'x 658, 659 (7th Cir. 2011); *Dodd v. Jones*, 623 F.3d 563, 569 (8th Cir. 2010); *Seaton v. Mayberg*, 610 F.3d 530, 533 (9th Cir. 2010), *cert. denied*, 562 U.S. 1222 (2011); *Freier v. Colorado*, 804 F. App'x 890, 891-92 (10th Cir. 2020) (holding that amendments to HIPAA did not authorize a private cause of action); *Wilkerson v. Shinseki*, 606 F.3d 1256, 1267 n.4 (10th Cir. 2010).

[23]15 U.S.C.A. §§ 6501 to 6506; 16 C.F.R. §§ 312.1 to 312.13; *see generally supra* § 26.13[2].

[24]*See, e.g.*, *Brush v. Miami Beach Healthcare Group Ltd.*, 238 F. Supp. 3d 1359, 1367-69 (S.D. Fla. 2017) (dismissing breach of express and implied contract claims; "Because the Defendants are required by law to adhere to HIPAA without receiving any consideration from the Plaintiff or any other patient, these provisions cannot create contractual obligations. . . . Plaintiff cannot mask a HIPAA claim as a breach of

of recovery.[25] State law claims premised on HIPAA violations likewise may fail,[26] but have been attempted in a number of cases.

Because alleged AdTech, cloud-based, social media, web and mobile data privacy claims often do not fit neatly within the confines of federal anti-hacking statutes or other federal criminal or narrow privacy laws, plaintiffs' lawyers may seek federal jurisdiction under the Class Action Fairness Act (CAFA).[150] 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 al-

---

contract claim. . . . Plaintiff [likewise] cannot create a private right of action for violations of HIPAA by recasting her claims as common law, implied contract claims."); *Cairel v. Jessamine County Fiscal Court*, No. 5:15-CV-186-JMH, 2015 WL 8967884, at *4 (E.D. Ky. Dec. 15, 2015) ("Plaintiff attempts to circumvent the fact that no private right of action exists under HIPAA by characterizing her claim thereunder as one for breach of contract. Regardless of whether the contract included a HIPAA provision, there simply is no private right of action for violations of HIPAA, at the state or federal level."); *Sheldon v. Kettering Health Network,* 40 N.E.3d 661, 674 (Ohio Ct. App. 2015) ("[T]o the extent that HIPAA universally has been held not to authorize a private right of action, to permit HIPAA regulations to define per se the duty and liability for breach is no less than a private action to enforce HIPAA, which is precluded."). *But see Dinerstein v. Google, LLC,* 484 F. Supp. 3d 561, 582-84 (N.D. Ill. 2020) (disagreeing with other courts, holding a breach of contract claim not preempted by HIPAA; "HIPAA regulations specifically provide that "more stringent" state rules are not preempted, 45 C.F.R. § 160.203(b), and "more stringent" is defined to include a state law that "provides *584 greater privacy protection for the individual who is the subject of the individually identifiable health information," § 160.202. A contract claim incorporating HIPAA is such a "more stringent" measure and is thus not preempted by the federal statute.").

[25]*See, e.g.*, *Adams v. Eureka Fire Protection District*, 352 F. App'x 137, 139 (8th Cir.2009) (holding that "[s]ince HIPAA does not create a private right, it cannot be privately enforced either via § 1983 or through an implied right of action.").

[26]*See, e.g.*, *Faber v. Ciox Health, LLC*, 944 F.3d 593, 596–602 (6th Cir. 2019) (affirming dismissal of plaintiff's putative class action claims for causes of action based on negligence, negligence *per se*, unjust enrichment, and breach of implied-in-law contract; "All of Plaintiffs' common-law claims suffer from the same fundamental defect: Tennessee common law is no substitute for the private right of action that Congress refused to create in HIPAA. That unavoidable conclusion has consequences. Here, it means that Plaintiffs cannot prove every element of their claims.").

[150]28 U.S.C.A. § 1332(d).

leges 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.[151]

State law claims that are popular with plaintiff's counsel typically are ones asserted under statutes that afford the potential to recover statutory damages, such as the California Consumer Privacy Act (CCPA)[27] (and, as of January 1, 2023, the California Privacy Rights Act (CPRA)),[28] or allow recovery of fees, such as the Illinois Biometric Privacy Act,[29] which authorizes both statutory damages and fees.

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

---

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

[27] *See* Cal. Civ. Code § 1798.150; *see generally supra* § 26.13A[14] (analyzing the statute and potential claims). Despite its name, the CCPA only allows a private cause of action for certain security breaches—not violations of the privacy law undertakings it mandates, which are enforced exclusively through administrative process. *See generally supra* § 26.13A. To state a CCPA claim in state or federal court (and potentially seek class certification) a plaintiff must allege and prove that (1) the plaintiff is a resident of California, (2) the defendant is a *business* (as defined in the statute) subject to the CCPA, (3) the incident occurred on or after January 1, 2020 and (4) resulted in the unauthorized access and exfiltration, theft, or disclosure of specific *personal information* (defined more narrowly than under the CCPA generally), (5) the personal information was unencrypted or unredacted at the time when exfiltrated, stolen, or disclosed, (6) the exfiltration, theft, or disclosure resulted from a business's failure to implement reasonable security measures, and (7) the plaintiff is not subject to a binding and enforceable arbitration agreement. *Supra* § 26.13A[14] (laying out and explaining these elements). To recover statutory damages, a plaintiff must further show that it provided notice and an opportunity to cure, and that the business did not do so (as discussed later in this section). Cal. Civ. Code § 1798.150(a)(1); *see generally supra* § 26.13A[14]..

[28] Cal. Civ. Code § 1798.150(a)(1) (effective Jan. 1, 2023).

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

injury and damage[152] (although in a small number of courts plaintiffs theoretically may be able to plead diminishment of the market value of personal information[153]). In general,

---

[152]*See, e.g.*, *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561, 591-92 (N.D. Ill. 2020) (dismissing plaintiff's breach of contract claim, in a putative data privacy class action suit brought against a research hospital whose electronic health records had been disclosed for research purposes to create predictive health models, for inadequately alleging money damages by claiming that he "overpaid" for services provided because of the value of his information; "He asserts that he is entitled to 'restitution on the basis that he did not receive the full benefits of his payments to the University.' . . . At most, this allegation suggests that some indeterminate amount of the price he paid for his treatments represents the cost of the University's privacy practices. This court agrees with others that have found such allegations to be insufficient."); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *16 (N.D. Cal Dec. 21, 2016) (granting summary judgment in favor of Google on plaintiff's individual claims for breach of contract and breach of the duty of good faith and fair dealing because the plaintiff could present no evidence of damages from Google's alleged (but disputed) breach of its privacy policy); *Svenson v. Google Inc.*, 65 F. Supp. 2d 717, 724–25 (N.D. Cal. 2014) (dismissing plaintiff's breach of contract claim with leave to amend for failing to sufficiently allege damage where "Plaintiff has not alleged any facts showing that Defendants' business practice—disclosing users' Contact Information to third-party App vendors—changed her economic position at all."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *13 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's breach of privacy policy claim with leave to amend where the plaintiff failed to allege "actual and appreciable damage based on the collection and dissemination of his PII."); *Rudgayzer v. Yahoo! Inc.,* No. 5:12-CV-01399 EJD, 2012 WL 5471149, at *7 (N.D. Cal. Nov. 9, 2012) (dismissing plaintiff's suit alleging breach of contract because his first and last name was disclosed in the "from" line of his Yahoo! email account where "an allegation of the disclosure of personal or private information does not constitute actionable damage for a breach of contract claim."); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1028-29 (N.D. Cal. 2012) (dismissing plaintiffs' contract claim with prejudice because emotional and physical distress damages are not recoverable for breach of contract under California law and because the unauthorized collection of personal information does not create economic loss and plaintiffs did not allege that the collection foreclosed their opportunities to capitalize on the value of their personal information or diminished its value); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' breach of contract claim because California law requires a showing of "appreciable harm and actual damage" to assert such a claim); *Gardner v. Health Net, Inc.*, No. CV 10-2140, 2010 WL 11597979, at *6 (C.D. Cal. Aug. 12, 2010) (dismissing plaintiff's breach of contract claim resulting from a data breach for "fail[ure] to allege any cognizable damages" because "an increased risk of identity theft[] cannot establish" damage that would support a breach of contract claim).

[153]*See In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014)

"[n]ominal damages, speculative harm, or threats of future harm do not suffice to show a legally cognizable injury" for a breach of contract claim.[154] A claim likewise may fail based

---

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

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

[154]*Castillo v. Nationstar Mortg. LLC*, 15-CV-01743, 2016 WL 6873526, at *3 (N.D. Cal. Nov. 22, 2016); *see also Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *9-10 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' breach of contract claim (premised on a company's Terms of Service and Privacy Policy), in a putative cybersecurity breach class action suit, because (1) nominal damages do not suffice to show legally cognizable injury under California law, (2) the alleged lost benefit of the bargain is not sufficient to allege damages because Quora's services were free and plaintiffs could not allege that the services they received were worth less as a result of the alleged breach, and (3) out-of-pocket mitigation expenses associated with the alleged data breach were not legally cognizable where plaintiffs had not suffered from identity theft—and alleged "only that they [we]re at an increased risk of identity theft—and therefore "there [we]re no damages to mitigate."); *In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *12 (N.D. Cal. May 27, 2016) (holding that alleging nominal damages was insufficient to state a claim for breach of contract in a cybersecurity breach case); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009), *aff'd*,

on the language of the Privacy Policy.[155]

An unfair competition claim premised on misrepresentation in a Privacy Policy, Terms of Use agreement or other statement or contract, similarly will fail where a plaintiff cannot allege that he or she actually read the challenged representation[30] or relied upon it.[31]

---

380 F. App'x 689 (9th Cir. 2010) (affirming dismissal of a breach of contract claim in a data breach putative class action suit because nominal damages are not recoverable).

[155]*See, e.g., Carlsen v. GameStop, Inc.*, 833 F.3d 903, 910-12 (8th Cir. 2016) (affirming dismissal of plaintiff's claims for breach of contract and alleged violations of Minnesota's Consumer Fraud Act, where GameStop's Privacy Policy, which was incorporated in its Terms of Service, did not define PII to include plaintiff's Facebook ID and browser history, which were the data elements that plaintiff alleged had been improperly shared); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 832-33 (N.D. Cal. 2020) (dismissing plaintiffs' breach of contract claim where plaintiff's allegations were contradicted by the terms of the Privacy Policy); *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 801-02 (N.D. Cal. 2019) (granting in part and denying in part defendant's motion to dismiss plaintiff's breach of contract claim premised on defendant's privacy policy).

[30]*See, e.g.*, *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *27-28 (N.D. Cal. Aug. 30, 2017) (dismissing plaintiffs' UCL fraud claim in a cybersecurity breach case to the extent based on defendants' alleged misrepresentation that they had "physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you" where plaintiffs had assented to Yahoo's Terms of Use and Privacy Policy but had not alleged they read the actual statement; "plaintiffs in misrepresentation cases must allege that they actually read the challenged representations" in order to state a claim."); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1220 (N.D. Cal. 2014) (dismissing plaintiffs' misrepresentation-based UCL claims where plaintiffs did not allege that they had read any of LinkedIn's alleged misrepresentations; "To make the reliance showing, this Court has consistently held that plaintiffs in misrepresentation cases must allege that they actually read the challenged representations."); *see also, e.g.*, *In re iPhone Application Litig*., 6 F. Supp. 3d 1004, 1018 (N.D. Cal. 2013) (granting summary judgment for the defendant on the issue of standing where none of the plaintiffs presented evidence that he or she even saw, let alone read and relied upon, the alleged misrepresentations contained in Apple's Privacy Policies); *In re LinkedIn User Privacy Litig*., 932 F. Supp. 2d 1089, 1093 (N.D.Cal.2013) (dismissing plaintiffs' claim for lack of standing because "Plaintiffs do not even allege that they actually read the alleged misrepresentation—the Privacy Policy—which would be necessary to support a claim of misrepresentation. . . . Because a causal connection between a defendant's actions and plaintiff's alleged harm is required for standing, Plaintiffs have not established standing based on an alleged misrepresentation.").

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

A claim for implied contract generally will fail where there

---

[31] *See, e.g.*, *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1194 (N.D. Cal. 2020) (dismissing, with leave to amend, claims for intentional misrepresentation and omission, deceit by concealment or omission under Cal. Civ. Code §§ 1709, 1710, and negligent misrepresentation, for lack of reliance, in a putative data privacy class action suit alleging that Facebook tracked plaintiffs' device location and IP address when its Privacy Policy stated that these data elements would be collected "depending on the permissions you've granted.").

[156] *See, e.g.*, *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 611 (9th Cir. 2020) (affirming dismissal of plaintiffs' claim that Facebook's alleged tracking practices violated the implied covenant of good faith and fair dealing because "as pleaded, the allegations did not go beyond the breach of contract theories asserted by Plaintiffs and were thus properly dismissed."), *cert. denied,* 141 S. Ct. 1684 (2021); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's breach of express and implied contract and breach of implied covenant of good faith and fair dealing, based on the disclaimer of warranties provision in Walmart's Terms of Use, in a putative cybersecurity breach class action suit); *Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1194-95 (N.D. Cal. 2020) (dismissing plaintiffs' claim for breach of the implied covenant of good faith and fair dealing for failing to go beyond their breach of contract claim); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *10-11 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' breach of the covenant of good faith and fair dealing claim, in a putative cybersecurity breach class action suit, as barred by the express disclaimer of warranties and limitation of liability provision contained in Quora's Terms of Service); *Svenson v. Google Inc.*, 65 F. Supp. 2d 717, 725-26 (N.D. Cal. 2014) (dismissing plaintiff's breach of the implied duty of good faith and fair dealing claim as duplicative of her breach of contract claim); *see also In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 802-03 (N.D. Cal. 2019) (granting in part and denying in part defendant's motion to dismiss plaintiff's breach of the duty of good faith and fair dealing premised on defendant's privacy policy, where some of the alleged conduct was disclosed in the policy); *Song Fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 885 (N.D. Cal. 2015) (granting Google's motion to dismiss claims for breach of YouTube's Terms of Service and breach of the duty of good faith and fair dealing arising out of plaintiffs' removal of a video where the Terms of Service permitted YouTube to remove the video "and eliminate its view count, likes, and comments"; "if defendants were given the right to do what they did by the express provisions of the contract there can be no breach [of the duty of good faith and fair dealing].").

is an express contract.[157] The same is true for the related claim of breach of confidence.[158] Indeed, where a Terms of Service agreement contains an express warranty disclaimer and limitation of liability provision, all claims for breach of express, implied, and quasi-contract may be dismissed.[159]

A claim for breach of an implied contract also will fail where the plaintiffs can't allege that they read or even saw the purported documents constituting the contract.[32]

Although numerous putative class action suits were

---

[157]*See, e.g.*, *Baer v. Chase*, 392 F.3d 609, 616-17 (3d Cir. 2004) ("There cannot be an implied-in-fact contract if there is an express contract that covers the same subject matter.").

[158]*See, e.g.*, *Berkla v. Corel Corp.*, 302 F.3d 909, 918 (9th Cir. 2002) ("[T]he tort of breach of confidence is grounded on an implied-in-law or quasi-contractual theory . . . . California courts have made clear that these two causes of action are mutually exclusive"); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *8 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' breach of confidence claim premised on Quora's Privacy Policy, in a putative cybersecurity breach class action suit, because a "breach of confidence claim . . . must be based on an implied obligation or contract—not an express contract."). A breach of confidence claim requires a showing that a plaintiff conveyed confidential *and novel* information to a defendant, who then breached that confidence. *Id.* at 917; *see generally supra* § 13.03 (analyzing breach of confidence claims in connection with idea misappropriation).

[159]*See Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's breach of express and implied contract and breach of implied covenant of good faith and fair dealing, based on the disclaimer of warranties provision in Walmart's Terms of Use, in a putative cybersecurity breach class action suit); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *10-11 (N.D. Cal. Dec. 19, 2019) (dismissing claims for breach of implied contract and breach of the covenant of good faith and fair dealing in a putative cybersecurity breach class action suit, as barred by the express disclaimer of warranties and limitation of liability provision contained in Quora's Terms of Service); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037-38 (N.D. Cal. 2019) (dismissing claims for breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, quasi-contract, and breach of confidence in a putative data security breach class action suit, where Facebook's Terms of Service included a limitation-of-liability clause); *see also Adkins v. Facebook, Inc.*, No. C 18-05982 WHA, 2019 WL 3767455 (N.D. Cal. Aug. 9, 2019) (denying in relevant part plaintiff's motion to amend his Complaint, and enforcing contractual waiver provisions in a data breach case over unconscionability objections).

[32]*See, e.g.*, *Krottner v. Starbucks Corp.,* 406 F. App'x 129, 131-32 (9th Cir. 2010) (affirming dismissal of plaintiffs' implied contract claims, in a suit arising out of a security breach caused when a laptop was stolen).

brought against subscription music services and magazine vendors under Michigan's Preservation of Personal Privacy Act (a part of which is also known as Michigan Video Rental Privacy Act), which previously afforded a successful plaintiff up to $5,000 in statutory damages, that statute was amended effective July 31, 2016, to no longer provide a statutory damages remedy.[160] As a consequence, for claims brought on or after July 31, 2016, a plaintiff cannot state a claim if he she

---

[160]*See* Mich. Comp. Laws § 445.1715(2) (limiting claims to "customers . . . . who [have] suffer[ed] actual damages . . . . "); *see generally supra* § 26.13[10] (analyzing the statute and discussing cases construing it). Mich. Comp. Laws Ann. § 445.1712(1) generally provides that, "except otherwise as provided by law, a person, or an employee or agent of the person, engaged in the business of selling at retail, renting, or lending books or other written materials, sound recordings, or video recordings shall not knowingly disclose to any person, other than the customer, a record or information that personally identifies the customer as having purchased, leased, rented, or borrowed those materials from the person engaged in the business." The statute creates an exception for "the disclosure of a record or information that has been aggregated or has been processed in a manner designed to prevent its association with an identifiable customer." *Id.* §§ 445.1712(1), 445.1712(2).

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

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

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

did not suffer actual damages.[161]

A claim under the Illinois Biometric Information Privacy Act (BIPA)[162] likewise may fail where the plaintiff cannot establish that he or she is *aggrieved by* the alleged violation (although the Illinois Supreme Court has established a relatively low bar for statutory standing).[163]

---

maintained by the person that is disclosing the information, and is available to customers or the general public.

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

A customer who "suffers actual damages as a result of a violation" of this PPPA may bring a civil action against the person that violated this act and recover (a) "actual damages, including damages for emotional distress" and (b) reasonable costs and attorneys' fees. *Id.* § 445.1715(2).

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

[162]740 Ill. Comp. Stat. Ann. 14/1 to 14/25; *see generally supra* § 26.13[12] (analyzing the statute).

[163]*See* 740 Ill. Comp. Stat. Ann. 14/20 (authorizing a private right of action for "any person aggrieved by a violation" of BIPA); *Rosenbach v. Six Flags Entertainment Corp.*, 2019 Il. 123186, 129 N.E.3d 1197, 1203-07 (Ill. 2019) (holding that a person need not have sustained actual damage beyond his or her rights under the Act in order to establish statutory standing to sue under it); *see also Dixon v. Washington and Jane Smith Community—Beverly*, Case No. 17 C 8033, 2018 WL 2445292, at *11-12 (N.D. Ill. May 31, 2018) (denying defendant's motion to dismiss for lack of statutory standing as a "person aggrieved" because "Dixon did allege an injury to a privacy right in her complaint—and . . . obtaining or disclosing a person's biometric data without her consent or knowledge constitutes an actual and concrete injury because it infringes on the right to privacy in that data . . . ."); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 510-21 (S.D.N.Y. 2017) (dismissing plaintiff's amended complaint with prejudice, holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have either Article III or statutory standing to sue for alleged violations of BIPA because plaintiffs conceded that they "received advance notice that their faces would be scanned . . . [and] consented to have their faces scanned," and a "more extensive notice and consent could not have altered the standing equation because there has been no material risk of harm to a concrete BIPA interest that more extensive notice and consent would have avoided" where the defendant used the biometric data as intended by the parties), *aff'd on other grounds sub. nom Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017) (affirming dismissal based on lack of Article III standing without reaching the statutory standing issue).

Plaintiffs also have sought to sue online genetic testing companies under state genetic privacy statutes.[164] While a number of states have enacted laws protecting privacy in genetic data, only a limited number provide for a private cause of action.[165]

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

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

[165]*See, e.g.,* Alaska Stat. § 18.13.020 (providing for actual damages plus $5,000 or, if the violation resulted in profit or monetary gain to the violator, $100,000); N.J. Stat. Ann. § 10:5-49(c) (providing for the recovery of actual damages, including damages for economic, bodily, or emotional harm, proximately caused by the disclosure of an individual's genetic in-

California[33] and Florida[34] wiretap statutes have not provided fertile ground for suits brought over the use by websites of replay technology.

State computer crime statutes likewise may not afford relief in a case where there has been no economic harm.[166]

---

formation in violation of New Jersey's Genetic Privacy Act); N.M. Stat. Ann. § 24-21-6 (allowing for recovery of actual damages, damages of up to $5,000 in addition to any economic loss if the violation results from willful or grossly negligent conduct, and reasonable attorneys' fees, among other things); Or. Rev. Stat. Ann. § 192.541 (providing for a range of statutory damages); Utah Code Ann. § 26-45-105 (allowing for injunctive relief and damages, plus statutory and punitive damages against an insurance company or employer who violates the Genetic Testing Privacy Act); *see generally supra* § 26.13[12] (analyzing privacy in biometric and genetic data).

[33]*See, e.g.*, *Saleh v. Nike, Inc.*, ___ F. Supp. 3d ___, 2021 WL 4437734, at *12-14 (C.D. Cal. Sept. 27, 2021) (dismissing plaintiff's CIPA section 635 claim, alleging use of FullStory session replay software, because "[c]ontrary to Plaintiff's argument, § 635 does not prohibit the 'implementation' or 'use' of a wiretapping device; instead, it prohibits the manufacture, assembly, sale, offer for sale, advertisement for sale, possession, transport, import, or furnishment of such device" and ruling, by analogy to ECPA, that a private cause of action may not be premised on mere possession and therefore plaintiff lacked Article III standing); *Graham v. Noom, Inc.*, No. 3:20-cv-6903, 2021 WL 1312765, at *7-8 (N.D. Cal. Apr. 8, 2021) (dismissing plaintiffs' 635(a) CIPA claim because plaintiffs could not allege eavesdropping where FullStory merely provided a cloud-based software tool and acted as "an extension of Noom[,]" and thus there could be no section 635 violation and plaintiffs lacked Article III standing); *see also Yale v. Clicktale, Inc.*, No. 3:20-cv-7575, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (applying *Noom* to reach the same result); *Johnson v. Blue Nile, Inc.*, No. 3:20-cv-8183, 2021 WL 1312771, at *3 (N.D. Cal. Apr. 8, 2021) (applying *Noom* to reach the same result).

[34]*See Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860, at *2 (Fla. Cir. June 11, 2021) (holding that sections 934.03(1)(a) and 934.03(1)(d) of the Florida Security of Communications Act's purpose was "to address eavesdropping and illegal recordings regarding the substance of communications or personal and business records . . . and not to address the use by a website operator of analytics software to monitor visitors' interactions with that website operator's own website. . . . [T]he FSCA does not cover Plaintiff's claims seeking to penalize Spirit's use of session replay software on its Website.").

[166]*See, e.g., In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 277-78 (3d Cir. 2016) (affirming the district court's dismissal with prejudice of plaintiffs' claims under the New Jersey Computer Related Offenses Act (CROA), N.J. Stat. Ann. § 2A:38A–3, an anti-hacking statute, because plaintiffs could not "allege that they had been 'damaged in business or property,' as the plain text of the New Jersey Act requires" and because the appellate panel was not willing to "credit their theory of damage—

Even specialized statutes intended to make it easy for plaintiff's counsel to bring consumer class action cases may not be well suited to data privacy suits based on behavioral advertising or other perceived privacy violations where there is no quantifiable harm or only *de minimis* damage. For example, California's Consumers Legal Remedies Act (CLRA),[167] 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.[168] A CLRA claim therefore may not be maintained where a plaintiff seeks a remedy from a free Internet site or free app where no purchase has been made,[169] although a

---

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

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

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

[169]*See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152-53 (3d Cir. 2015) (affirming dismissal of plaintiffs' CLRA claim and rejecting the argument that Google's alleged access to personal information stored in cookies constituted a forced "sale" of trackable internet history information as a form of payment to Google), *cert. denied,* 137 S. Ct. 36 (2016); *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *32-33 (N.D. Cal. Aug. 30, 2017) (dismissing plaintiffs' CLRA claim because "[t]he mere fact that Yahoo gained some profit from Plaintiffs' use of Yahoo's free email services does not by itself show that Plaintiffs 'purchased' those services from Defendants. . . . Plaintiffs cite no legal authority—and the Court is not aware of any legal authority—to support Plaintiffs' theory that the mere transfer of PII renders Plaintiffs' use of a free service a 'purchase' or 'lease' of that service. . . . The Court cannot ignore the CLRA's 'strict requirement' of a 'purchase or lease' simply because Plaintiffs believe that the result is unfair in this case."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *12 (N.D. Cal. Mar. 26, 2013)

Ninth Circuit panel, in an unreported decision, allowed a CLRA claim to proceed premised on the lost sales value of personal information.[170] 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.[171] A CLRA claim also may fail where the plaintiffs cannot allege reliance (for example, when a CLRA claim is premised on the breach of a privacy policy).[172]

Claims under the California Invasion of Privacy Act

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

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

[171] *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).

[172] *See In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 982-83 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' CLRA claim, explaining that "[i]f Nisenbaum and the other members of his subclass did not see, read, hear or consider the terms of Google's then-active privacy policy before creating their account, they could not have relied on any representation it contained in making their decisions to purchase Android phones, and without affirmatively alleging reliance on Google's misrepresentations, the CLRA claim cannot survive.").

(CIPA)[173] or the California Constitution[174] (and under Flor-

[173]The California Invasion of Privacy Act (CIPA), Penal Code §§ 630 *et seq.*, affords multiple potential causes of action pursuant to section 637.2(a), including under section 631(a) a claim against anyone

> [1] who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or
>
> [2] who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or
>
> [3] who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above. . . .

Cal. Penal Code § 631(a). "The California Supreme Court has clarified that this lengthy provision contains three operative clauses protecting against 'three distinct and mutually independent patterns of conduct': (i) 'intentional wiretapping,' (ii) 'willfully attempting to learn the contents or meaning of a communication in transit over a wire,' and (iii) 'attempting to use or communicate information obtained as a result of engaging in either of the two previous activities.' " *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 825 (N.D. Cal. 2020), *quoting Tavernetti v. Superior Court*, 22 Cal. 3d 187, 192, 148 Cal. Rptr. 883, 583 P.2d 737 (1978). The third clause covers any attempt to use or communicate information obtained as a result of engaging in either of the two previous activities. *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 827 (dismissing plaintiffs' claim); *Tavernetti*, 22 Cal. 3d at 192.

Although the law is not entirely settled, the better view is that "California's highest court would likely conclude Section 631(a) does not protect oral communications." *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 688 (N.D. Cal. 2021) (explaining that oral communications are expressly covered by section 632).

A claim under subpart (1) will fail where there is no machine, instrument or contrivance. *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (dismissing plaintiff's CIPA claim where he did not plead facts to show how Facebook used a "machine, instrument or contrivance" to obtain the contents of communications and did not adequately allege that Facebook acquired the contents of a communication), *rev'd on other grounds*, 956 F.3d 589, 607-08 (9th Cir. 2020) (holding that Facebook was not exempt from liability as a matter of law under CIPA (or the Wiretap Act) as a party to the communication, without opining on whether plaintiffs adequately pleaded other requisite elements of the statute, which were not raised in the appeal), *cert. denied*, 141 S. Ct. 1684 (2021).

A CIPA wiretap claim is construed coexstensively with a Wiretap Act claim under Title I of ECPA. *See, e.g.*, *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (CIPA analysis "is the same as that

under the federal Wiretap Act"); *see also In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (holding that the federal Wiretap Act does not create liability for interception of "record information regarding the characteristics of the message that is generated in the course of the communication"). By its terms, it also requires tapping into a "telegraph or telephone wire, line, cable, or instrument . . . ." Cal. Penal Code § 631(a); *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 825-26 (N.D. Cal. 2020) (dismissing plaintiffs' claim for failing to make this allegation); *see also Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127-28 (N.D. Cal. 2020) (dismissing plaintiffs' CIPA claim for failing to allege an interception where plaintiffs argued that 2FA prevented a user from accessing his Apple ID or services (such as when the user had lost his trusted device) because "if a user cannot access an Apple service like FaceTime due to 2FA, as Plaintiffs allege, the user cannot create any communication over FaceTime for Apple to 'intercept.' "); *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 938, 953-54 (N.D. Cal. 2014) (dismissing plaintiff's CIPA claim based on allegations that defendants "wrongfully accessed the accounts at issue," because "any subsequent reading or forwarding of those emails by defendants does not constitute an illegal 'interception' "). Further, "[t]he intent requirement of the Wiretap Act requires a defendant to act "purposefully and deliberately and not as a result of accident or mistake." *United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015). "Although no 'evil' motive is required, the defendant must have 'acted consciously and deliberately with the goal of intercepting wire communications.' " *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021) (quoting *Christensen* and holding that "[a]lthough the question is close, the Court finds that Plaintiffs adequately allege intent at this stage. Plaintiffs allege that Apple knows of the accidental Siri triggers and, instead of deleting the resulting messages, sends them to contractors to improve Siri's functioning. . . . To be sure, one of the purposes of the third-party contractor review is to distinguish deliberate from accidental Siri activations (and, presumably, to reduce the latter). . . . It is difficult to see how Apple could intentionally allow accidental Siri triggers to proceed only to use the intercepted information to prevent accidental triggers. Nevertheless, the Court finds that at this stage, Plaintiffs sufficiently allege that Apple fails to take remedial action while knowing of the accidental activations, sufficient to make the conduct 'intentional.' ").

While section 631 prohibits wiretapping, section 632 proscribes eavesdropping and recording. *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 688 (N.D. Cal. 2021). Unlike section 631, section 632 is also limited to *confidential* communications. *Id.* Section 632 authorizes a claim against any "person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication." *Eavesdrop* in this context refers "to a third party secretly listening to a conversation between two other parties." *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 827 (N.D. Cal. 2020) (quoting earlier cases). It "does not require an unauthorized connection to a transmission line, whereas wiretapping does." *Id.* at 826 (quotation omitted). *Confidential*, in turn, means "based on an 'objectively reasonable expectation that the conversation is not being overheard or recorded.' " *Lopez v. Apple, Inc.*,

519 F. Supp. 3d 672, 689 (N.D. Cal. 2021), *quoting Flanagan v. Flanagan*, 27 Cal. 4th 766, 774-76, 117 Cal. Rptr. 2d 574, 41 P.3d 575 (2002).

Courts have rejected claims brought under section 632 where a communication is not confidential or the plaintiff does not have an objectively reasonable expectation of privacy. *See, e.g.*, *Rodriguez v. Google LLC*, Case No. 20-cv-04688-RS, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021) (dismissing plaintiffs' section 632 claim based on the presumption that internet communications do not reasonably give rise to an objectively reasonable expectation that the communication will not be overheard or recorded, where the plaintiffs did not plead "unique, definite circumstances rebutting California's presumption against online confidentiality."); *Lopez v. Apple, Inc*., 519 F. Supp. 3d 672, 689-90 (N.D. Cal. 2021) (dismissing plaintiffs' claim arising out of alleged communications involving Siri because "iPhones are frequently used in public settings, and Plaintiffs have not alleged that they used them in private settings that justify such an expectation. Plaintiffs have therefore not sufficiently alleged confidentiality."); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 827-28 (N.D. Cal. 2020) (dismissing plaintiffs' Complaint for failing to adequately allege that communications were confidential in a putative class action suit alleging that plaintiffs' conversations were wrongfully recorded due to "false accepts" by virtual assistant software and then disclosed to subcontractors; "The California Supreme Court has held that a conversation is 'confidential' under § 632 'if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded.' " *Id.* at 828, *quoting Kearney v. Salomon Smith Barney, Inc*., 39 Cal. 4th 95, 117 n.7, 45 Cal. Rptr. 3d 730, 137 P.3d 914 (2006); *see also Faulkner v. ADT Sec. Services, Inc*., 706 F.3d 1017, 1019 (9th Cir. 2013). Neither party disputes that this standard is the same as the "reasonable expectation of privacy" required under the Wiretap Act, 18 U.S.C. § 2510(2)."); *Revitch v. New Moosejaw, LLC*, Case No. 18-cv-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019) (dismissing plaintiff's 632 claim because "[e]ven if Revitch could plausibly allege that NaviStone's code constitutes an "amplifying or recording device," he cannot allege that his browsing activity and form field entries fall within the scope of confidential communications protected by section 632"); *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1051–52 (N.D. Cal. 2018) (holding that "emails and other electronic messages" were not confidential communications under section 632); *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 848-49 (N.D. Cal. 2014) (dismissing plaintiff's claim based on allegedly scanned Facebook messages); *In re Google Inc. Gmail Litig.*, Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *23 (N.D. Cal. Sept. 26, 2013) (scanned email); *see also People v. Nakai*, 183 Cal. App. 4th 499, 518–19, 107 Cal. Rptr. 3d 402 (2010) (holding that defendant's Yahoo instant messages with a decoy, who was posing as a 12-year-old girl, were not confidential; although the defendant intended for the communication between himself and the recipient to be kept confidential, he could not reasonably expect that the communications would not be recorded where Yahoo's policies "indicated that chat dialogues may be shared for the purpose of investigating or preventing illegal activities[,]" Yahoo "warn[ed] users that chat dialogues can be 'archive[d], print[ed], and save[d,]' " and "[c]omputers that are connected to the internet are capable of instanta-

neously sending writings and photographs to thousands of people.") *But see Brown v. Google LLC*, 525 F. Supp. 3d 1049 1073-74 (N.D. Cal. 2021) (denying defendant's motion to dismiss plaintiffs' CIPA 632 claim alleging that the defendant accessed browsing information from plaintiffs while they were searching in private mode, because plaintiffs "could have had a reasonable expectation that their private browsing communications were not being disseminated" and "Google's policies did not indicate that data would be collected from users in private browsing mode and shared with Google.").

Some plaintiffs have sued Adtech companies for allegedly violating Cal. Penal Code § 635(a), which proscribes the manufacture, assembly, or sale of (or offer to sell, advertise to sell, possess, transport, import, or furnish to another) a device primarily or exclusively designed or intended for eavesdropping upon the communication of another, for providing replay software to website publishers. *See, e.g.*, *Saleh v. Nike, Inc.*, __ F. Supp. 3d __, 2021 WL 4437734, at *12-14 (C.D. Cal. Sept. 27, 2021) (dismissing plaintiff's CIPA section 635 claim, alleging use of FullStory session replay software, because "[c]ontrary to Plaintiff's argument, § 635 does not prohibit the 'implementation' or 'use' of a wiretapping device; instead, it prohibits the manufacture, assembly, sale, offer for sale, advertisement for sale, possession, transport, import, or furnishment of such device" and ruling, by analogy to ECPA, that a private cause of action may not be premised on mere possession and therefore plaintiff lacked Article III standing); *Graham v. Noom, Inc.*, No. 3:20-cv-6903, 2021 WL 1312765, at *7-8 (N.D. Cal. Apr. 8, 2021) (dismissing plaintiffs' 635(a) CIPA claim because plaintiffs could not allege eavesdropping where FullStory merely provided a cloud-based software tool and acted as "an extension of Noom[,]" and thus there could be no section 635 violation and plaintiffs lacked Article III standing); *see also Yale v. Clicktale, Inc.*, No. 3:20-cv-7575, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (applying *Noom* to reach the same result); *Johnson v. Blue Nile, Inc.*, No. 3:20-cv-8183, 2021 WL 1312771, at *3 (N.D. Cal. Apr. 8, 2021) (applying *Noom* to reach the same result).

Section 635 is patterned on 18 U.S.C.A. § 2512, which has been construed as a criminal law provision that does not allow for a private right of action. *See, e.g.*, *DIRECTV, Inc. v. Nicholas*, 403 F.3d 223, 227 (4th Cir. 2005); *Yoon v. Lululemon USA, Inc.*, __ F. Supp. 3d __, 2021 WL 3615907, at *7-8 (C.D. Cal. July 15, 2021) (dismissing plaintiff's claim, holding that there is no private right of action for the violation of section 2512(1); "Section 2512(1) provides for fines or imprisonment; it is therefore a criminal statute. Section 2520(a) provides a civil right of action for persons whose communications are 'intercepted, disclosed, or intentionally used in violation of this chapter.' But the 'manufacturing, assembly, possession, or sale' activities that are criminalized in § 2512(1) are distinct from 'interception, disclosure, or use' activities. Moreover, § 2520(a) allows recovery 'from the person or entity . . . which engaged in that violation . . .'—'that violation' referring to 'interception, disclosure, or use.' The two provisions speak past each other; one criminalizes the manufacturing of wiretap technology, while the other allows for private civil lawsuits stemming from the use of that technology."); *Cohen v. Casper Sleep Inc*., Nos.

17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *5 (S.D.N.Y. July 12, 2018); *In re Lenovo Adware Litig.*, Case No. 15-md-02624, 2016 WL 677245, at *7 (N.D. Cal. Oct. 27, 2016) (collecting authorities); *Potter v. Havlicek*, No. 3:06-CV-211, 2008 WL 2556723, at *4-7 (S.D. Ohio June 23, 2008); *see also DIRECTV Inc. v. Robson*, 420 F.3d 532, 539 & n.31 (5th Cir. 2005) ("§ 2512(1)(b) *does* makes it a crime to 'intentionally . . . possess[ ] . . . any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications[.]' Tellingly, however, the civil cause of action embodied in § 2520 does not cover such possessory violations."); *Luis v. Zang*, 833 F.3d 619, 636 (6th Cir. 2016) (holding, in a suit where the plaintiff alleged that his female friend's husband installed a software program called WebWatcher on her computer, which intercepted Mr. Luis's communications to his female friend and then forwarded them to a server run by the defendant, that although in general "§ 2520 provides a cause of action against only those defendants whose violation of the Wiretap Act consists of an intercept, disclosure, or intentional use of a communication[,]" because the defendant had continuously operated the device that intercepted Mr. Luis's communications, Mr. Luis could assert a section 2512(1) claim through section 2520(a) of the Wiretap Act); *DirecTV, Inc. v. Treworgy*, 373 F.3d 1124, 1127 (11th Cir. 2004) (holding there is no private right of action under section 2520 against a person for possession of a pirate device in violation of section 2512(1)(b)).

At least one court has extended this holding to a claim premised on CIPA section 635. *See Yoon v. Lululemon USA, Inc.*, __ F. Supp. 3d __, 2021 WL 3615907, at *7-8 (C.D. Cal. July 15, 2021) (holding that "the language of the CIPA is far more straightforward than the analogous language of the Wiretap Act: only a person 'who has been injured by a violation of this chapter' may assert a civil claim. Quantum Metric's manufacture, assembly, sale, advertisement, transportation, import, or furnishing of Session Replay did not directly injure Yoon. Rather, Yoon alleges that Lululemon's *use* of Session Replay injured her. For that reason, CIPA § 637.2 does not provide Yoon with a private right of action to enforce CIPA § 635 against Quantum Metric.").

There has also been some litigation under section 637.7, which provides (subject to exceptions when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle, and for "the lawful use of an electronic tracking device by a law enforcement agency") that '[n]o person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.' Cal. Penal Code § 637.7. For purposes of this section, an *electronic tracking device* means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals. *Id.* § 637.7(d). Because this section contemplates use of tracking devices attached to vehicles, claims involving browser or mobile app data have been difficult to assert successfully. *See Heeger v. Facebook, Inc.*, Case No. 18-cv-06399-JD, 2019 WL 7282477, at *3 (N.D. Cal. Dec. 27, 2019) (dismissing plaintiffs' claim because "the plain language of the CIPA does not accommodate technology like a mobile

ida's wiretap statute[35]) will not be actionable, as under

---

app on a digital device, and plaintiff does not persuasively show otherwise."); *In re Google Location History*, 428 F. Supp. 3d 185, 192-96 (N.D. Cal. 2019) (dismissing plaintiffs' CIPA claim under Cal. Penal Code § 637.7, alleging geolocation tracking by various apps, because this section of "CIPA, by its plain terms, is not concerned with data storage but focuses on unconsented data tracking, which is not at issue. . . . [and even] assuming some type of unconsented tracking was occurring, Defendant's services [apps such as Google Maps and Chrome] are not a 'device' within the meaning of Section 637.7(d)."); *see also In re Google Location History*, Case No. 5:18-cv-05062-EJD, 2020 WL 2929629 (N.D. Cal. June 3, 2020) (denying reconsideration).

As with other claims, CIPA cases brought in federal court also may be dismissed if the plaintiffs fail to establish Article III standing. *See, e.g.*, *NEI Contracting & Engineering, Inc*., 926 F.3d 528, 532-33 (9th Cir. 2019) (affirming decertification of a class, following the determination that the named plaintiff lacked Article III standing, in a suit brought under the California Invasion of Privacy Act, alleging that the defendant violated CIPA by recording customer orders without consent); *Heeger v. Facebook, Inc*., 509 F. Supp. 3d 1182, 1187-91 (N.D. Cal. 2020) (dismissing the *Heeger* plaintiffs' claims for intrusion upon seclusion, violation of the California constitution and CIPA for lack of Article III standing because they did not plausibly allege any privacy injuries where they did not allege more than the collection of IP addresses associated with mobile devices, "and there is no legally protected privacy interest in IP addresses.").

[174]*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).

[35]*See, e.g.*, *Goldstein v. Costco Wholesale Corp.*, Case No. 21-CV-80601-RAR, 2021 WL 4134774 (S.D. Fla. Sept. 9, 2021) (dismissing plaintiff's claim under the Florida Security of Communications Act, Fla. Stat. Ann. §§ 934.10(1)(a), 934.10(1)(d), arising out of Costco's use of session replay software on its commercial website, with prejudice, because the alleged interception did not implicate the contents of a communication, and declining to "rewrite Florida's wiretapping law in the face of changing technology. . . . [T]hese actions did not convey the substance of any communication. Rather, this mere tracking of Plaintiff's movements on Defendant's website is the cyber analog to record information Defendant could have obtained through a security camera at a brick-and-mortar store. The FSCA's text itself reinforces that such actions fall outside the statute's purview."); *Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860, at *3 (Fla. Cir. June 11, 2021) (dismissing plaintiff's claim under the Florida Security of Communications Act, over the defendant's use of replay technology, because plaintiff couldn't allege that the contents of electronic communications had been intercepted); *see also, e.g., Goldstein v. Luxottica of America, Inc.*, Case No. 21-80546-CIV-CANNON-Reinhart, 2021 WL 4093295 (S.D. Fla. Aug. 23, 2021) (following *Jacome v. Spirit Airlines* and *Cardoso v. Whirlpool Corp.* in recommending dismissal of plaintiff's Florida Security of Communications Act claim with prejudice, where plaintiff alleged that he visited defendant's website

ECPA, if premised on non-content data, as opposed to the contents of communications.[175] A CIPA claim likewise may

---

(www.ray-ban.com) twice "and that Defendant unlawfully intercepted his electronic communications using 'session replay' technology to track his activities on the website" because "the information Mr. Goldstein alleges the session replay software captured is (1) not 'contents,' (2) not an 'electronic communication,' and (3) not a prohibited 'interception.' "), *report and recommendation adopted,* 2021 WL 4125357 (S.D. Fla. Sept. 9, 2021) (adopting the recommendation and dismissing plaintiff's case with prejudice); *Swiggum v. EAN Services, LLC*, No. 8:21-493, 2021 WL 3022735, at *2 (M.D. Fla. July 16, 2021) (citing *Jacome v. Spirit Airlines* in granting defendant's motion to dismiss, ruling that "the FSCA does not apply to the plaintiff's claims regarding session replay technology software on a commercial website"); *Cardoso v. Whirlpool Corp*., No. 21-60784, 2021 WL 2820822, at *2 (S.D. Fla. July 6, 2021) (following *Jacome v. Spirit Airlines* in dismissing plaintiff's FSCA claim because the FSCA does not apply to session replay technology and the plaintiff did not allege interception of the contents of her communications); *Connor v. Whirlpool Corp*., No. 21-14180, 2021 WL 3076477, at *2 (S.D. Fla. July 6, 2021) (following *Jacome v. Spirit Airlines* in dismissing plaintiff's FSCA claim because the FSCA does not apply to session replay technology and the plaintiff did not allege interception of the contents of her communications). *But see Alhadeff v. Experian Information Solutions, Inc.,* 541 F. Supp. 3d 1041 (C.D. Cal. 2021) (denying defendant's motion to dismiss plaintiff's FSCA claim based on arguments that there was no interception, the data allegedly accessed was not the contents of the communication, and defendant did not use the information, in an early case that does not reference any of the Florida state or federal case law cited in this footnote).

[175]*See, e.g.*, *Yoon v. Lululemon USA, Inc.*, __ F. Supp. 3d __, 2021 WL 3615907, at *5-6 (C.D. Cal. July 15, 2021) (dismissing plaintiff's CIPA 631(a)(ii) claim, premised on Lululemon's use of Quantum Metric session replay software on its website, because Yoon's allegation that Quantum Metric recorded her "keystrokes, mouse clicks, pages viewed, and shipping and billing information . . . [and] the date and time of the visit, the duration of the visit, Plaintiff's IP address, her location at the time of the visit, her browser type, and the operating system on her device" did not involve the contents or meaning of the communication; "CIPA § 631(a)[ii] protects only the internal, user-generated material of a message, not routine identifiers, whether automatically generated or not."); *Graham v. Noom, Inc.*, No. 3:20-cv-6903, 2021 WL 1312765, at *6 (N.D. Cal. Apr. 8, 2021) (dismissing plaintiffs' 631(a) CIPA claim because plaintiffs alleged that what had been accessed was non-content data, rather than the contents of a communication, which is defined the same way under CIPA as under the Wiretap Act); *McCoy v. Alphabet, Inc.*, Case No. 20-cv-05427-SVK, 2021 WL 405816, at *13-14 (N.D. Cal. Feb. 2, 2021) (dismissing plaintiff's CIPA claim because "Plaintiff alleges that Defendant collected data on when and how often an Android Smartphone user opens and runs non-Google apps and the amount of time spent on the apps. . . . This alone is more akin to log in activities, and *In re Zynga* forecloses a CIPA claim predicated on this type of record information."); *Brodsky v. Apple Inc.*, 445 F. Supp.

not be maintained where the defendant itself was a party to the alleged communication.[176] Privacy claims under CIPA

3d 110, 127 (N.D. Cal. 2020) (dismissing plaintiffs' CIPA claim because plaintiffs alleged that Apple intercepted plaintiffs' login activities—requests to access third-party apps or (presumably) user names and passwords, which were record information not the contents of communications); *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); *see also Yale v. Clicktale, Inc.*, No. 3:20-cv-7575, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (applying *Noom* to reach the same result); *Johnson v. Blue Nile, Inc.*, No. 3:20-cv-8183, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021) (applying *Noom* to reach the same result).

[176]*See In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 276 (3d Cir. 2016) (affirming dismissal of CIPA claims where Viacom, as a party to the communications, authorized Google to place cookies on plaintiffs' computers; CIPA "prohibits the interception of wire communications and disclosure of the contents of such intercepted communications," but "does not apply when the alleged interceptor was a party to the communications."); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' CIPA claim because Cal. Penal Code § 631(a), like the Wiretap Act, broadly prohibits the interception of wire communications and disclosure of those intercepted communications—*i.e.*, eavesdropping or the secret monitoring by third parties—and could not be applied to Google's alleged use and disclosure of information stored in cookies because Google was itself a party to those electronic communications), *cert. denied*, 137 S. Ct. 36 (2016); *Graham v. Noom, Inc.*, No. 3:20-cv-6903, 2021 WL 1312765, at *4-6 (N.D. Cal. Apr. 8, 2021) (dismissing plaintiffs' 631(a) CIPA claim because FullStory was a vendor that provided a software service that captured its clients' data, hosted it on FullStory's servers, and allowed its clients to analyze their data; distinguishing *Facebook Tracking* and *Moosejaw* because "as a service provider, FullStory is an extension of Noom. It provides a tool — like the tape recorder in *Rogers* — that allows Noom to record and analyze its own data in aid of Noom's business. . . . It is not a third-party eavesdropper."; "Only a third party can listen to a conversation secretly. *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975). By contrast, a party to a communication can record it (and is not eavesdropping when it does). *Id*. at 897–99;"); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 125-27 (N.D. Cal. 2020) (dismissing plaintiffs' CIPA claim because plaintiffs' "login activities" were communications that plaintiffs themselves sent to Apple's servers); *see also Yale v. Clicktale, Inc.*, No. 3:20-cv-7575, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (applying *Noom* to reach the same result); *Johnson v. Blue Nile, Inc.*, No. 3:20-cv-8183, 2021 WL 1312771, at *2 (N.D. Cal. Apr. 8, 2021) (applying *Noom* to reach the same result). *But see In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 608 (9th Cir. 2020) (disagreeing with the Third Circuit and holding that "simultaneous, unknown duplication and communication of GET requests

and the California Constitution also may not be viable if brought more than a year after they have accrued[36] or where consent has been obtained[177] (or under equivalent wiretap-

---

do not exempt a defendant from liability under the party exception."), *cert. denied,* 141 S. Ct. 1684 (2021); *Revitch v. New Moosejaw, LLC*, Case No. 18-cv-06827-VC, 2019 WL 5485330, at *1-2 (N.D. Cal. Oct. 23, 2019) (denying defendant's motion to dismiss plaintiff's CIPA claim against NaviStone and New Moosejaw based on allegations that Moosejaw embedded NaviStone's analytics software on its website and rejecting theory that Moosejaw could make NaviStone a party to the communication under CIPA).

[36]CIPA claims are subject to a one-year statute of limitations. *E.g., Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 624 (N.D. Cal. 2021); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 134-39 (N.D. Cal. 2020) (dismissing plaintiff's CIPA claim as time barred in a putative data privacy class action suit). Claims under the California Constitution are as well. *E.g., McGowan v. Weinstein,* 505 F. Supp. 3d 1000, 1018-19 (C.D. Cal. 2020) (dismissing (with leave to amend) the claim of actress Rose McGowan, who alleged that various people associated with Harvey Weinstein were vicariously liable for Black Cube's invasion of her right to privacy in her unpublished manuscript, *Brave,* which Black Cube copied from her laptop during a meeting when she left the room briefly to go to the bathroom, where she failed to plead inability to timely discover the facts, which had occurred more than one year prior to her filing suit).

[177]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *2-5 (N.D. Cal. July 28, 2021) (dismissing wiretap claims under California, Florida, and Washington state law (including Cal. Penal Code §§ 631(a), 635), where plaintiffs provided consent by assenting to Instacart's Privacy Policy, which set forth, among other things, that Instacart could share information payment processor partners and third parties); *Javier v. Assurance IQ, LLC*, Case No. 4:20-cv-02860-JSW, 2021 WL 940319, at *2-4 (N.D. Cal. Mar. 9, 2021) (dismissing plaintiff's claims under the California Invasion of Privacy Act (CIPA) and California Constitution, where the plaintiff had given click-through consent to Assurance's Privacy Policy, which made clear that Assurance tracked activity on its website and stated that it may use third party vendors to do so, over the objections that, among other things, consent was obtained after the defendant allegedly began tracking plaintiff's use of the site, and that disclosure that Assurance used TrustedForm JavaScript that can be pasted into a form page to record "keystrokes, mouse clicks, data entry and other electronic communications" appeared under the heading "Web beacons" instead of in the "cookies and tracking technology" section); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888, at *5 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' Cal. Penal Code § 631(a) claim where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in the terms of the defendant's Privacy Policy; "All of the Complaint's statutory claims depend on a lack of consent. *See* 18 U.S.C. § 2511(2)(d) (exempting from the ECPA communications for which 'one of the parties to the communication has given prior consent to such interception'); 18 U.S.C. § 2702(b)(3) (allowing a provider to divulge

information 'with the lawful consent of the originator or an addressee or intended recipient of such communication'); Cal. Penal Code § 631(a) (prohibiting wiretaps 'without the consent of all parties to the communication'); . . ."); *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953, 955 (N.D. Cal. 2017) (dismissing plaintiff's putative class claims under the California Information Privacy Act, based on consent provided pursuant to Facebook's Data Policy and Cookie Policy), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("He who consents to an act is not wronged by it." (quoting Cal. Civ. Code § 3515)); *Garcia v. Enterprise Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing plaintiff's California Invasion of Privacy Act claim with leave to amend where the defendant—app provider's Terms of Use and Privacy Policy provided consent for the alleged disclosures). *But see Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 622-23 (N.D. Cal. 2021) (declining to find consent as a matter of law under CIPA, the Wiretap Act, and various other claims, in ruling on a preliminary motion, where the applicable privacy policy might have led a reasonable user to believe that Google did not collect his or her personal information when the user had not elected to sync data in Chrome).

In *Javier,* the plaintiff alleged that Assurance used TrustedForm, which allegedly was JavaScript code that could be "pasted into a form page to record 'keystrokes, mouse clicks, data entry, and other electronic communications of visitors to websites.' " 2021 WL 940319, at *1. Assurance allegedly used the code to record consent to be contacted by phone, to refute potential claims under the Telephone Consumer Protection Act. *See generally infra* § 29.16. The court rejected plaintiff's argument that the consent was invalid because the website started recording his activities before he was presented with a button to provide click-through assent to Assurance's Privacy Policy. *See* 2021 WL 940319, at *3 (upholding retroactive consent). The court also found that the notice page where consent was provided was "uncluttered, with only a few entry fields followed by the disclosure on a single page; the text placed hyperlinks in a different color to indicate their selectability; and there were no additional features, such as a dark background or additional links having different formatting, that would have obscured the notice." *Id.*; *see generally supra* § 21.03 (analyzing contract formation and assent to Terms of Use).

With respect to the substance of the Privacy Policy disclosure, the court rejected the plaintiff's argument that the Policy did not disclose recording because it placed some disclosures in the "Web beacons" section, instead of the "cookies and tracking technology" section; because the tracking technology section indicated that tracking was performed "to enhance your shopping experience"; because the policy stated Assurance "may" use third party monitors; and because "transfer [ ] of data" did not indicate real time monitoring. *See* 2021 WL 940319, at *4. The court explained:

> These arguments are largely irrelevant. The policy clearly indicates that Assurance tracks activity on its website and may use third party vendors to do so. The policy as a whole is only two pages long, which means that none of the terms are buried or obscured. That the privacy policy also discusses other types of tracking, such as data collection for purposes of personalization, does not detract from its plain disclosures elsewhere. Accordingly, the Court finds that the privacy policy to which Javier agreed disclosed the specific conduct at issue here.

ping laws from other states, under the California Constitution or for common law intrusion upon seclusion where consent was provided[37]) or under the California Constitution or for common law intrusion upon seclusion where an alleged privacy violation is not substantial..[178] Privacy claims

---

Id.

[37]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *2-5 (N.D. Cal. July 28, 2021) (dismissing wiretap claims under California, Florida, and Washington state law (Cal. Penal Code §§ 631(a), 635; the Florida Security of Communications Act, Fla. Stat. Ann. § 934.03(2)(d) (permitting interception of a communication "when all of the parties to the communication have given prior consent"); and Washington's Wiretap Act, Wash. Rev. Code Ann. §§ 9.73.030(1) (a)-(b) (permitting interception with "the consent of all the participants")), where plaintiffs provided consent by assenting to Instacart's Privacy Policy, which set forth, among other things, that Instacart could share information payment processor partners and third parties).

[178]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 294-95 (3d Cir. 2016) (affirming dismissal of plaintiffs' New Jersey intrusion upon seclusion claim against Google for allegedly using tracking cookies to track website activity by children because tracking cookies can serve legitimate commercial purposes and "Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad other websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."), *cert. denied*, 137 S. Ct. 624 (2017); *Saleh v. Nike, Inc.*, ___ F. Supp. 3d ___, 2021 WL 4437734, at *14-15 (C.D. Cal. Sept. 27, 2021) (dismissing plaintiff's claim under the California Constitution, arising out of Nike's alleged use of FullStory session replay software, because plaintiff did not allege that Nike and FullStory "collected intimate or sensitive personally identifiable information or otherwise disregarded Plaintiff's privacy choices while simultaneously holding themselves out as respecting them. . . . The fact that FullStory's software allegedly captured, among other things, '(a) [t]he user's mouse clicks; (b) [t]he user's keystrokes; (c) [t]he user's payment card information, including card number, expiration date, and CCV code; (d) [t]he user's IP address; (e) [t]he user's location at the time of the visit; and (f) [t]he user's browser type and the operating system on their devices,' . . . is insufficient to demonstrate that Defendants' conduct constituted a serious invasion of a protected privacy interest."); *Schmitt v. SN Servicing Corp.*, Case No. 21-cv-03355-WHO, 2021 WL 3493754, at *7 (N.D. Cal. Aug. 9, 2021) (dismissing plaintiff's California invasion of privacy claim in a data breach case, rejecting the argument that the criminal nature of the breach meant the invasion of privacy was substantial); *Yoon v. Lululemon USA, Inc.*, ___ F. Supp. 3d ___, 2021 WL 3615907, at *9 (C.D. Cal. July 15, 2021) (dismissing plaintiff's claim, arising out of Lululemon's use of Quantum Metric session replay software, noting that "courts have been less willing to find that users have a cognizable privacy interest in browsing data collected only while users interact with the website of the defendant company."); *Graham v. Noom, Inc.*, No. 3:20-cv-6903, 2021 WL 1312765, at *8 (N.D. Cal. Apr. 8, 2021) (dismissing

plaintiffs' claim that defendants violated the California Constitution by using replay software to wiretap their use of the Noom website because there was no wiretap and thus plaintiffs did not plausibly plead a legally protected privacy interest); *Yale v. Clicktale, Inc.*, No. 3:20-cv-7575, 2021 WL 1428400, at *3 (N.D. Cal. Apr. 15, 2021) (applying *Noom* to reach the same result); *Lopez v. Apple, Inc*., 519 F. Supp. 3d 672, 690-91 (N.D. Cal. 2021) (dismissing claims for intrusion upon seclusion and privacy under the California Constitution, premised on a newspaper article in the *Guardian,* which reported that some Apple devices had been subject to accidental triggers and review by third party contractors, where plaintiffs had not alleged "specific circumstances to show that Apple intercepted their confidential communications. Nor have they alleged that the scale or pervasiveness of the accidental triggers itself gives rise to a privacy invasion."); *McCoy v. Alphabet, Inc*., Case No. 20-cv-05427-SVK, 2021 WL 405816 (N.D. Cal. Feb. 2, 2021) (dismissing plaintiff's intrusion upon seclusion claim and claim under the California Constitution, in a putative class action suit alleging that Google monitored and collected sensitive personal data when users used non Google apps on Android devices, where "[t[he data alleged to have been collected without Plaintiff's consent, the frequency and duration of use of certain apps, d[id] not rise to the requisite level of an egregious breach of social norms or intrusion in a manner highly offensive to a reasonable person."); *Heeger v. Facebook, Inc*., 509 F. Supp. 3d 1182, 1193-94 (N.D. Cal. 2020) (dismissing claims for intrusion upon seclusion and under the California Constitution where, at most, plaintiffs alleged that Facebook "pinned" plaintiff Lundy down to a city and state while logged into the app; "a generalized location, such as one that locates a user no more precisely than within several city blocks, may not implicate much in the way of privacy concerns."); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 829-31 (N.D. Cal. 2020) (dismissing plaintiffs' California Constitutional invasion of privacy and common law intrusion upon seclusion claims because "Plaintiffs have not alleged sufficient information about the conversations that were allegedly intercepted and recorded to establish that they were had under circumstances that would give rise to a reasonable expectation of privacy."); *Manigault-Johnson v. Google, LLC*, No. 18-cv-1032, 2019 WL 3006646, at *5-6 (D.S.C. Mar. 31, 2019) (following *Nickelodeon* in dismissing plaintiffs' South Carolina intrusion upon seclusion claim, in a putative class action suit alleging that defendants collected certain personal information from children under 13 without giving notice or obtaining advanced, verifiable consent, in violation of COPPA, because the Complaint failed to allege "a substantial and unreasonable intrusion, *i.e*., facts showing that the intrusion occurred in a manner 'highly offensive' to a reasonable person.); *Razuki v. Caliber Home Loans, Inc*., No. 17CV1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. Jun. 8, 2018) (dismissing plaintiff's claim for invasion of privacy under the California Constitution for failing to state a claim, in a security breach case based on the alleged disclosure of personal information because "[l]osing personal data through insufficient security doesn't rise to the level of an egregious breach of social norms underlying the protection of sensitive data like social security numbers . . . . [plaintiff's] allegations don't suggest the type of intentional, egregious privacy invasion contemplated in *Hill*."); *Yunker v. Pandora Media, Inc.*,

also may not be viable where plaintiffs cannot claim that that harms alleged (based on news reports or company admissions) actually impacted them (as opposed to other, unnamed, members of a putative class).[38]

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

"[T]he California Supreme Court has moved toward treating the tort [of intrusion upon seclusion] and constitutional privacy inquiries as functionally identical, although the claims do continue to exist as separate claims with technically distinct elements." *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1033 (N.D. Cal. 2019) (analyzing cases). To state a claim for intrusion upon seclusion under California law, a plaintiff must allege (1) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff had a reasonable expectation of privacy and (2) that intrusion was 'highly offensive' to a reasonable person. To state a claim for invasion of privacy under the California Constitution, a plaintiff must allege (1) a specific, legally protected privacy interest, (2) a reasonable expectation of privacy, and (3) a 'sufficiently serious' intrusion by the defendant. *Lopez v. Apple, Inc*., 519 F. Supp. 3d 672, 690-91 (N.D. Cal. 2021). "Because of the similarity of the tests, courts consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 601 (9th Cir. 2020), *cert. denied,* 141 S. Ct. 1684 (2021); *see also, e.g., Lopez v. Apple, Inc*., 519 F. Supp. 3d at 690-91 (applying a "combined inquiry"); *In re Google Location History Litigation*, 514 F. Supp. 3d 1147, 1154 (N.D. Cal. 2021) (applying the combined inquiry).

[38]*See, e.g.*, *Lopez v. Apple, Inc*., 519 F. Supp. 3d 672, 690-91 (N.D. Cal. 2021) (dismissing claims for intrusion upon seclusion and privacy under the California Constitution (and breach of contract, for Privacy Policy provisions incorporated into Apple's software license agreement), premised on a newspaper article in the *Guardian,* which reported that some Apple devices had been subject to accidental triggers and review by third party contractors, where plaintiffs had not alleged "specific circumstances to show that Apple intercepted their confidential communications. Nor have they alleged that the scale or pervasiveness of the accidental triggers itself gives rise to a privacy invasion."); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1035-38 (N.D. Cal. 2021) (dismissing plaintiffs' California invasion of privacy claim, in a putative class action suit, where plaintiffs failed to allege "that Zoom actually shared *their* personal data with third parties.") (emphasis in original); *Williams v. Facebook, Inc*., 384 F. Supp. 3d 1043, 1052-53 (N.D. Cal. 2018) (dismissing plaintiffs' claim for misrepresentations or fraudulent omissions where the complaint quoted an "*Ars Technica* article as reporting 'Facebook never explicitly revealed that the data was being collected,' yet

California's notoriously-broad unfair competition statute requires a showing of actual injury. That statute—California Business and Professions Code section 17200[179]—allows claims for equitable relief or restitution[39] to be based on violations of statutes that do not expressly create independent causes of action[180] (as do unfair competition statutes in some other states[181]). 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.' "[182] A 17200 claim must be based on personal participation, not merely knowledge.[40] A claim

---

it provides no contact upload prompt against which to assess that assertion. FACC ¶ 23. As pleaded, the complaint appears to be based on selective information from the article without any suggestion plaintiffs know what the specific prompt or prompts were at the time they installed the apps. More needs to be averred to satisfy the applicable rules of pleading.").

Some class action complaints are framed from news reports or public statements or documents, rather than the actual experiences of named plaintiffs, on whose claims a complaint will rise or fall in connection with a motion to dismiss.

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

[39]*See, e.g.*, *Thomas v. Kimpton Hotel & Restaurant Group, LLC,* Case No. 19-cv-01860-MMC, 2020 WL 3544984, at *3-4 (N.D. Cal. June 30, 2020) (dismissing plaintiffs' 17200 claim in a putative cybersecurity breach class action suit where plaintiff failed to allege facts sufficient to support either a claim for injunctive relief or a claim for restitution).

[180]*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].

[181]*See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1327-28 (N.D. Ga. 2019) (denying defendant's motion to dismiss plaintiff's claim for negligence *per se* under Georgia law in a data breach case, premised on the defendant's alleged failure to maintain reasonable security pursuant to section 5 of the FTC Act).

[182]*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)).

[40]*See, e.g.*, *Yordy v. Plimus, Inc.*, No. 12-cv-00229-TEH, 2014 WL 1466608, at *2 (N.D. Cal. Apr. 15, 2014) ("Under the UCL, a defendant's

under section 17200 also 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."[183] Hence, a plaintiff generally may not maintain suit for privacy violations where the plaintiff obtained access to the defendant's service, app or product free of charge[184] unless the claim may be premised on the value of a product purchased in conjunc-

---

liability must be based on his 'personal participation in the unlawful practices' and 'unbridled control' over the unlawful practices; vicarious liability is insufficient. . . . Likewise, for an FAL claim, mere knowledge of the falsity of a third-party's statements is insufficient to support direct liability or an aiding-and-abetting theory of liability . . . .").

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

[184]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' 17200 claim based on Google's alleged collection of data stored in Internet cookies), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal with prejudice of plaintiffs' UCL claim where plaintiffs could not allege that they "lost money or property as a result of the unfair competition."), *aff'g*, 791 F. Supp. 2d 705, 714-15 (N.D. Cal. 2011) (dismissing with prejudice plaintiffs' UCL claim where plaintiffs alleged that the defendant unlawfully shared their "personally identifiable information" with third-party advertisers because personal information does not constitute property for purposes of a UCL claim; "Because Plaintiffs allege that they received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim."); *Rodriguez v. Google LLC*, Case No. 20-cv-04688-RS, 2021 WL 2026726, at *8 (N.D. Cal. May 21, 2021) (dismissing plaintiffs' UCL claim where the apps referenced in the amended complaint were free to download, plaintiffs did not allege any payment, and even if they had, the court could not conceive how, for example, in-app purchases would have been made *because* of Google, in a putative data privacy class action suit alleging that the defendant had collected information at variance with its representations about privacy); *Hart v. TWC Product and Technology LLC*, 526 F. Supp. 3d 592, 603-04 (N.D. Cal. 2021) (citing *Bass* in dismissing plaintiff's UCL claim, in which he alleged that TWC had "taken, maintained, transmitted, and devalued his valuable and private geolocation data" when he downloaded and used TWC's weather app, because "Hart 'has not shown how this information has economic value to *him*. That the information has external value, but no economic value to plaintiff, cannot serve to establish that plaintiff has personally lost money or property.' "); *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *6-7 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' UCL

tion with obtaining free services[185] or potentially for breach of a statutory duty to adhere to the terms of a company's privacy policy.[186] The risk of future harm likewise will not

---

claims in a putative cybersecurity breach class action suit because, "that Plaintiffs did not receive the full benefit of their bargain with Quora is not a loss of money or property because Plaintiffs did not pay for Quora's services."); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039-40 (N.D. Cal. 2019) (dismissing Adkins' 17200 claim where he could not plausibly allege a market for loss of value of his personal information or for failing to receive the benefit of his bargain, and where the risk of future harm and loss of time did not qualify as "lost money or property" as a result of unfair competition); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *11 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's claim with leave to amend where the plaintiff alleged that his PII was diminished in value based on Pandora's alleged use); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' UCL claim, with leave to amend, where plaintiffs did not allege that they lost money as a result of defendants' conduct, but instead merely alleged that defendants shared their personally identifiable information with third party advertisers).

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

[186]*See Svenson v. Google Inc.*, Case No. 13–cv–04080–BLF, 2015 WL 1503429, at *8-10 (N.D. Cal. Apr. 1, 2015) (denying defendants' motion to dismiss plaintiff's UCL claim, holding that plaintiff stated a claim under both the unlawful and unfairness prongs of the statute by alleging that the defendant failed to adhere to the terms of its own Privacy Policy in violation of Cal. Bus. & Prof. Code § 22576, and plaintiff alleged that defendants' payment processing services were not free because they allegedly retained a portion of the $1.77 app price for each transaction); *see generally supra* § 26.13[6] (analyzing the duty to post a privacy policy imposed on companies that collect personal information from California residents). In *Svenson*, the plaintiff pled around *In re Facebook Privacy*

suffice.[41] Courts have further rejected the argument that plaintiffs have a property interest in their personal information or electronic communications that amounts to lost property under section 17200.[187] That said, a plaintiff also must

---

Litig., 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal with prejudice of plaintiffs' UCL claim where plaintiffs could not allege that they "lost money or property as a result of the unfair competition.") by alleging the existence of a contract and a fee that does not appear to have been plausible in light of the actual written contract entered into by the plaintiff and defendants.

[41]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *3-6 (N.D. Cal. July 28, 2021) (dismissing with prejudice, for failure to adequately allege injury, plaintiff's California unfair competition claim based on amended allegations of loss of value of PII (where plaintiff did not allege that he had been unable to sell, profit from, or monetize his personal information and the court inferred that an expired credit card in any case had no value), risk of future harm (where plaintiff alleged he canceled the credit cards associated with the breach and that those cards had expired), out of pocket expenses and lost time (where plaintiff failed to allege that credit monitoring services were "reasonable and necessary"), and benefit of the bargain); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *3-7 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim in a data breach putative class action suit because, among other things, plaintiff could not plead a cognizable injury by alleging the future risk of identity theft, the loss of value of his PII, out of pocket expenses for credit monitoring, and the benefit of the bargain); *In re Yahoo! Inc. Customer Data Security Breach Litig.,* 313 F. Supp. 3d 1113, 1129-30 (N.D. Cal. 2018) (dismissing the UCL claims of certain plaintiffs who obtained free services from Yahoo and alleged that, as a result of various security breaches, they were at "substantial risk for identity theft . . . ," for failure to state a claim).

[187]*See, e.g.*, *In re Facebook Privacy Litig*., 572 F. App'x 494, 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' California statutory unfair competition claim, holding that the loss of sales value of personal information disclosed by a defendant, while sufficient to show damages for breach of contract and fraud claims, was insufficient to establish statutory standing for a UCL claim "because plaintiffs failed to allege that they 'lost money or property as a result of the unfair competition.' ") (quoting Cal. Bus. & Prof. Code § 17204)); *Cottle v. Plaid Inc*., Case No. 20-cv-03056-DMR, 2021 WL 1721177, at *14 & n.8 (N.D. Cal. Apr. 30, 2021) (dismissing plaintiff's California unfair competition claim for lack of statutory standing and disagreeing with *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 636-37 (N.D. Cal. 2021), as premised on four Article III standing cases, which had a different, lower threshold of harm that must be met than to establish UCL statutory standing); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *8 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim in a data breach putative class action suit because, among other things, " 'personal information' does not constitute money or property under the UCL."); *Adkins v. Facebook, Inc*., No. C 18-05982 WHA, 2019 WL 3767455, at *3 (N.D. Cal. Aug. 9, 2019) (denying

prove or allege inadequacy of legal remedies to state a claim under section 17200.[42]

Since many Internet sites and services provide free access, the requirement to show or prove that a plaintiff suffered injury in fact and has lost money or property as a result of the alleged unfair competition limits potential unfair competition claims against many of the more popular Internet and social media sites. The further requirement to show inadequacy of legal remedies presents an additional hurdle for plaintiffs in data privacy cases where damages also are sought.[43]

Absent injury, statutory unfair competition claims under the laws of other states similarly may not be viable.[188]

---

leave to amend because the Ninth Circuit in *In re Facebook Privacy Litigation* rejected the theory that the "lost value of [the plaintiff's] personal information" establishes standing under the UCL); *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1056 n.22 (N.D. Cal. 2014); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 862 (N.D. Cal. 2011).

[42]*See, e.g.*, *Shay v. Apple Inc.*, Case No.: 20cv1629-GPC(BLM), 2021 WL 1733385 (S.D. Cal. May 3, 2021) (dismissing plaintiff's UCL claim), *citing Sonner v. Premier Nutrition Corp*., 971 F.3d 834, 844 (9th Cir. 2020); *In re California Gasoline Spot Market Antitrust Litigation*, Case No. 20-cv-03131-JSC, 2021 WL 1176645, at *7-8 (N.D. Cal. Mar. 29, 2021) (dismissing plaintiff's UCL claim with leave to amend if plaintiffs had a good faith basis to allege inadequacy of legal remedies).

[43]*See, e.g.*, *Sonner v. Premier Nutrition Corp*., 971 F.3d 834, 843-44 (9th Cir. 2020) (affirming dismissal where plaintiff failed to allege a lack of adequate legal remedy because "the traditional principles governing equitable remedies in federal courts, including the requisite inadequacy of legal remedies, apply when a party requests restitution under the UCL and CLRA in a diversity action."); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *7-8 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's UCL claim, in a putative data breach class action suit, because, among other things, plaintiff alleged he suffered compensable damages, and rejecting the argument that plaintiff would have no adequate remedy at law if the court were to find his legal claims deficient).

[188]*See, e.g.*, *Shaulis v. Nordstrom, Inc.*, 865 F.3d 1, 10 (1st Cir. 2017) (holding that "a plaintiff bringing an action . . . under [Mass. Gen. Laws ch. 93A, § 2, which prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce"] must allege and ultimately prove that she has, as a result [of the statutory violation], suffered a distinct injury or harm that arises from the claimed unfair and deceptive act.") (quoting *Tyler v. Michaels Stores, Inc.*, 464 Mass. 492, 503, 984 N.E.2d 737 (2013)); *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1039 (N.D. Cal. 2019) (dismissing a plaintiff's unfair

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.[189] False advertis-

---

competition claim under Massachusetts law, where she alleged that she had downloaded the free version of two apps and therefore had not alleged injury, while denying motions brought by plaintiffs under New York and California law who had alleged that they had purchased premium versions, in putative class action suits alleging that defendants used apps designed for children to track online behavior on a device and user-specific level, and that defendants exploited the data, without disclosure or consent, for profit); *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 35-36 (2d Cir. 2017), *aff'g*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *10-13 (S.D.N.Y. Aug. 17, 2016) (affirming dismissal of plaintiffs' claims under N.Y. Gen. Bus. L. § 349 for failure to allege facts showing that they had suffered an injury cognizable under that section, in a putative class action suit based on defendants' alleged use of tracking cookies, because "§ 349 injury has been recognized only where confidential, individually identifiable information—such as medical records or a Social Security number—is collected without the individual's knowledge or consent."); *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *7-9 (S.D.N.Y. July 12, 2018) (dismissing plaintiff's claim against NaviStone, a marketing company and data broker that offered code to e-commerce vendors to help them identify who visited their websites by scanning visitors' computers for information that could be used for de-anonymization, for failing to satisfy the injury requirement of section 349); *Tyler v. Michaels Stores, Inc.*, 840 F. Supp. 2d 438, 448–51 (D. Mass. 2012) (dismissing a claim under Massachusetts' unfair trade practices statute, Mass. Gen. Laws ch. 93A, § 2 because receiving unwanted mail and other alleged injuries stemming from the defendant's alleged disclosure of her zip code information was not an injury cognizable under chapter 93A); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *5–6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend an unfair competition claim in a putative class action suit over the alleged use of browser and flash cookies because Washington's Consumer Protection Act requires "a specific showing of injury").

[189]*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

ing claims under California law[190] likewise will be dismissed where a plaintiff cannot show that it has suffered injury in fact and lost money or property.[191]

Similarly, a claim under California's Computer Crime law (CCCL), which is also known as the California Comprehensive Computer Data Access and Fraud Act (CDAFA),[192] which

---

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).

[190]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).

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

[192]Cal. Penal Code § 502. The statute imposes liability on any one of fourteen different grounds, including on any person who "[k]nowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network." *Id.* § 502(c)(2). CDAFA claims often rise or fall with claims asserted under the federal Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030, although unlike the CFAA there is no minimum monetary injury threshold required to sue under the CCCL. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 131-32 (N.D. Cal. 2020) (dismissing plaintiffs' claim where they could not allege that access was unauthorized based on a Terms of Use violation where the defendant was authorized for some but not all purposes and where plaintiffs offered no allegations about how 2FA offered Apple access to plaintiffs' information that was "somehow different from Apple's access through other Apple ID login methods."). A claim under section 502 is similar to a claim under the Computer Fraud & Abuse Act except that "the

may be premised on one or more of fourteen different grounds,[44] is only actionable where a plaintiff can show "dam-

---

California statute does not require *unauthorized* access. It merely requires *knowing* access." *U.S. v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016) (emphasis in original). *Access*, according to the Ninth Circuit, "includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *Id.*; *see also Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016) (affirming liability under section 502 where the defendant continued to access Facebook's servers after having received a cease and desist letter instructing it to stop doing so). Some court opinions in the Northern District of California have even held that a claim under section 502 may be stated by alleging the use of software designed to render ineffective any barriers that plaintiffs must wish to use to prevent access to their information. *See, e.g.*, *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1074-75 (N.D. Cal. 2021) (holding that plaintiffs adequately alleged a CDAFA claim "because Plaintiffs allege that Google's Analytics and Ad Manager core would render ineffective any barrier that Plaintiffs implemented."). According to one court, however, a claim under section 502 may not be viable where the data accessed is publicly available. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1115 n.13 (N.D. Cal. 2017).

[44]Liability may be imposed on anyone who:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

age or loss."[193] A CCCL/CDAFA claim also may be unavail-

(9) Knowingly and without permission uses the internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.

(10) Knowingly and without permission disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network.

(11) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network.

(12) Knowingly and without permission disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network.

(13) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section.

(14) Knowingly introduces any computer contaminant into any public safety infrastructure computer system computer, computer system, or computer network.

Cal. Penal Code § 502(c).

[193]*See* Cal. Penal Code § 502(e)(1) (providing that only an individual who has "suffer[ed] damage or loss by reason of a violation" of the statute may bring a civil action "for compensatory damages and injunctive relief or other equitable relief."); *Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' claim under section 502 where plaintiffs alleged loss of the value of personal data, which the Third Circuit held did not amount to damage or loss), *cert. denied*, 137 S. Ct. 36 (2016) *Cottle v. Plaid Inc.*, Case No. 20-cv-03056-DMR, 2021 WL 1721177, at *16-17 (N.D. Cal. Apr. 30, 2021) (dismissing plaintiffs' CDAFA claim, holding that the lost value of indemnification rights and alleged loss of the right to control their own data, loss of the value of their data, or loss of the right to protection of the data, did not amount to "damage or loss" within the meaning of the CDAFA, in a putative FinTech data privacy class action suit); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1043-44 (N.D. Cal. 2021) (dismissing, in a putative class action suit, plaintiffs' CDAFA claim alleging that Zoom failed to protect the privacy of user data and the security of its platform against breaches referred to as "Zoombombing," because plaintiffs failed to allege that Zoom disclosed any of their personal information); *Nowak v. Xapo, Inc.*, Case No. 5:20-cv-03643-BLF, 2020 WL 6822888, at *5 (N.D. Cal. Nov. 20, 2020) (dismissing

able absent circumvention; merely accessing information may not be enough.[194] A claim under section 502(c)(1) likewise will fail where electronic data was accessed or copied but not "altered, damaged, deleted or destroyed . . . ."[45]

---

plaintiff's CDAFA claim under Cal. Penal Code § 502(c)(6), with leave to amend, where the plaintiff alleged that third parties hacked into his cryptocurrency exchange account, stealing 500 Bitcoins which they deposited into wallet addresses owned by custodial cryptocurrency firms Indodax and Xapo, which plaintiff alleged employed inadequate policies and procedures to prevent use of their services for malicious activity, because, among other grounds, the court questioned whether plaintiff's loss was cognizable under section 502); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715–16 (N.D. Cal. 2011) (dismissing plaintiffs' section 502 claims, some with and some without prejudice), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their section 502 claim); *see generally infra* § 44.09 (analyzing section 502).

Unlike the Computer Fraud and Abuse Act, the CDAFA does not define *damage* or *loss* and does not require a minimum monetary threshold for loss to state a claim. *Cottle v. Plaid Inc.*, 2021 WL 1721177, at *16.

[194]*See, e.g., In re Google Android Consumer Privacy Litig.*, No. 11-2264, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013) ("Courts within this District have interpreted 'without permission' to require that a defendant access a network in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access."; internal quotation marks omitted).

[45]*See, e.g.*, *McGowan v. Weinstein,* 505 F. Supp. 3d 1000, 1020-21 (C.D. Cal. 2020) (dismissing actress Rose McGowan's claim, with leave to amend, alleging that various people associated with Harvey Weinstein gained unauthorized access to her laptop to obtain a copy of an unpublished manuscript that discussed Weinstein's alleged rape of McGowan, as part of a scheme to defraud and deceive her, because alteration, damage, deletion or destruction must be shown); *Ticketmaster L.L.C. v. Prestige Entertainment West, Inc.*, 315 F. Supp. 3d 1147, 1175 (C.D. Cal. 2018) (holding that Ticketmaster had not stated a claim under subsections (c)(1) and (c)(4) because those subsections both required that the defendants had altered, damaged, deleted, or destroyed the data in some way and while "Defendants' bots place a heavy load on Ticketmaster's system, and they cause Ticketmaster's system to relinquish tickets to Defendants against Ticketmaster's wishes, . . . [they] do not actually alter, damage, delete, or destroy data on Ticketmaster's systems. Precisely the opposite is true: the fact that Ticketmaster's systems continued to deliver tickets to Defendants' bots shows that Ticketmaster's systems continued to function as intended, without damage or alteration, while the bots operated. It is for this same reason that Ticketmaster has also failed to state a claim with respect to subsection (c)(5) of the CDAFA, which requires a showing of "disruption" or "denial" of computer services. Cal. Penal Code § 502(c)(5).").

Some state and federal privacy laws, including the Stored Communications Act, Wiretap Act and Computer Fraud and Abuse Act and CIPA, are subject to relatively short statute of limitations periods,[46] which may preclude claims that are not timely asserted.[47]

On the other hand, when timely, plaintiffs' lawyers have been able to state claims under various broadly worded statutes that were never intended to be a driver for consumer class action suits. For example, some courts have denied motions to dismiss putative data privacy class claims brought against a company for its data practices under the California Anti-Phishing Act,[48] reasoning that the plain terms of the

---

[46]*See, e.g.*, 18 U.S.C.A. § 2520(e) (stating that the Wiretap Act has a limitations period of "two years after the date upon which the claimant first has a reasonable opportunity to discover the violation" for Wiretap Act claims); 18 U.S.C.A. § 2707(f) (stating that the SCA has a limitations period of "two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation"); 18 U.S.C.A. § 1030(g) (stating that the CFAA has a limitations period of two years from "the date of the act complained of or the date of the discovery of the damage"); Cal. Civ. Proc. Code § 335.1 (setting a two year limitations period, which applies to intrusion upon seclusion claims); *Hart v. TWC Product and Technology LLC*, 526 F. Supp. 3d 592, 598-99 (N.D. Cal. 2021) (holding that a two-year statute of limitations applies to invasion of privacy claims brought under the California Constitution); *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 624 (N.D. Cal. 2021) (noting that the statute of limitations is one year for CIPA claims and two years for those brought under the Wiretap Act, Stored Communications Act and Computer Fraud and Abuse Act).

Under the Wiretap each interception is a discrete violation with its own statute of limitations. *See Bliss v. CoreCivic, Inc*., 978 F.3d 1144, 1148 (9th Cir. 2020). By extension, at least in the Ninth Circuit, CIPA and CDAFA claims also have statutes that run separately for each violation, which refer to "communication" or "act" in the singular. *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 625 (N.D. Cal. 2021), *citing* Cal. Penal Code §§ 631(a) (prohibiting the unauthorized interception of "any message, report or communication"), 632(a) (prohibiting the interception of a "confidential communication"), 502(e)(5) (stating that the statute of limitations is three years from "the date of the act complained of, or the date of the discovery of the damage, whichever is later").

[47]*See, e.g.*, *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 134-39 (N.D. Cal. 2020) (dismissing claims brought under the Computer Fraud and Abuse Act, CIPA, and the CCCL, in a putative data privacy class action suit alleging violations based on Apple's two-factor authentication login tool, as time barred).

[48]Cal. Bus. & Prof. Code § 22948.2. "An individual who is adversely affected by a violation of Section 22948.2 may bring an action . . . against a person who has directly violated Section 22948.2." *Id.* § 22948.3(a)(2).

statute do not require a showing of facilitating identity theft; merely use of the Internet to "solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business."[49] A court similarly declined to dismiss a claim for statutory larceny under California law in a data privacy case despite the absence of theft in any traditional sense of the word.[50]

Common law privacy claims may be difficult to assert in data privacy cases[195] absent an ability to characterize the al-

---

[49]*See, e.g.*, *Cottle v. Plaid Inc.*, Case No. 20-cv-03056-DMR, 2021 WL 1721177, at *20-22 (N.D. Cal. Apr. 30, 2021); *Wesch v. Yodlee, Inc.*, Case No. 20-cv-05991-SK, 2021 WL 1399291, at *8 (N.D. Cal. Feb. 16, 2021).

Identifying information under the statute includes a bank account number, account password, and "[a]ny other piece of information that can be used to access an individual's financial accounts . . . ." Cal. Bus. & Prof. Code § 22948.1(b).

[50]*See Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (denying defendant's motion to dismiss claims asserted under Cal. Penal Code § 484, which forbids theft, which is defined to include obtaining property "by . . . false . . . representation or pretense[,]" and Cal. Penal Code § 496(a), which prohibits the obtaining of property "in any manner constituting theft[,]" in a suit alleging that Google collected browser history information from users of Chrome who had opted not to sync this data with their Google accounts).

[195]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 294-95 (3d Cir. 2016) (affirming dismissal of plaintiffs' New Jersey intrusion upon seclusion claim against Google for allegedly using tracking cookies to track website activity by children because tracking cookies can serve legitimate commercial purposes and "Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 829-31 (N.D. Cal. 2020) (dismissing plaintiffs' California intrusion upon seclusion claim because "Plaintiffs have not alleged sufficient information about the conversations that were allegedly intercepted and recorded to establish that they were had under circumstances that would give rise to a reasonable expectation of privacy."); *Manigault-Johnson v. Google, LLC*, No. 18-cv-1032, 2019 WL 3006646, at *5-6 (D.S.C. Mar. 31, 2019) (following *Nickelodeon* in dismissing plaintiffs' South Carolina intrusion upon seclusion claim, in a putative class action suit alleging that defendants collected certain personal information from children under 13 without giving notice or obtaining advanced, verifiable consent, in violation of COPPA, because the Complaint failed to allege "a substantial and unreasonable intrusion, *i.e.*, facts showing that the intrusion occurred in a manner 'highly offensive' to a reasonable person.); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015) (dismissing

leged intrusion as highly offensive to a reasonable person.[196]

---

intrusion upon seclusion claims in a putative data privacy class action suit because plaintiffs "could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable"), *rev'd on other grounds*, 956 F.3d 589, 601-06 (9th Cir. 2020) (reversing dismissal of a subsequently amended Complaint containing more detailed allegations), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 987-88 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' intrusion upon seclusion claim based on plaintiffs' inability to meet the "high bar" to allege the requisite "intrusion [that is] highly offensive to a reasonable person" where Google was alleged to have comingled user data across accounts and disclosed it to third party app developers, allegedly in violation of its Privacy Policy); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (finding unauthorized disclosure to third parties of an iDevice user's unique device identifier number, personal data, and geolocation information to not be an egregious breach of social norms); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding disclosure of LinkedIn data insufficiently offensive); Department of *Labor v. McConnell*, 305 Ga. 812, 817-19, 828 S.E.2d 352, 359-60 (2019) (affirming dismissal of plaintiff's negligence, invasion of privacy and breach of fiduciary duty claims, where the Department of Labor had sent an email to approximately 1,000 Georgians who had applied for unemployment benefits, which included a spreadsheet that listed the name, social security number, home phone number, email address, and age of over 4,000 state residents, because there was no general duty of care to safeguard personal information to support a negligence claim under Georgia law and where there was no confidential relationship to support a breach of fiduciary duty claim, and no intrusion on plaintiff's seclusion, to support a common law claim for invasion of privacy, because the information disclosed did not affect reputation and the matters disclosed were not offensive and objectionable); *see generally supra* §§ 12.02[3][B], 26.08 (analyzing tort of unreasonable intrusion on seclusion, at greater length).

[196]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 295 (3d Cir. 2016) (vacating an order dismissing plaintiffs' intrusion upon seclusion claim against Viacom based on the collection of information using allegedly duplicitous tactics, where the Nickelodeon website allegedly included the false message: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"; "Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149-52 (3d Cir. 2015) (holding that plaintiffs stated claims under the California Constitution and California tort law where plaintiffs alleged practices that allegedly went beyond disclosed tracking to allegedly include overriding cookie blocking software to access information and involved alleged misstatements about its practices), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601-06 (9th Cir. 2020) (reversing dismissal,

Alleged data privacy violations also may be difficult to as-

---

holding that plaintiffs stated a claim for intrusion upon seclusion by alleging that Facebook surreptitiously used plug-ins to track logged-out users' browsing histories when they visited third-party websites and then compiled the browsing histories into personal profiles that allegedly were sold to advertisers), *cert. denied,* 141 S. Ct. 1684 (2021); *Calhoun v. Google LLC,* 526 F. Supp. 3d 605, 629-31 (N.D. Cal. 2021) (holding that plaintiffs stated a claim for intrusion upon seclusion by alleging that Google collected user data from Chrome browser users who chose not to sync their browser histories with their Google accounts); *Brown v. Google LLC,* 525 F. Supp. 3d 1049, 1075-80 (N.D. Cal. 2021) (holding that plaintiffs stated a claim for intrusion upon seclusion by alleging that the defendant collected browsing history from users while they were in private browsing mode); *In re Google Location History Litigation*, 514 F. Supp. 3d 1147, 1153-58 (N.D. Cal. 2021) (denying defendant's motion to dismiss plaintiffs' amended claims for intrusion upon seclusion and under the California Constitution for allegedly secretly tracking and storing geolocation data, finding that plaintiffs' amended allegations adequately pleaded a protectable privacy interest and highly offensive intrusion); *New Mexico ex rel. Balderas v. Tiny Lab Productions,* 457 F. Supp. 3d 1103, 1123-27 (D.N.M. 2020) (denying defendants' motion to dismiss where the State of New Mexico alleged that defendant ad networks were liable for intrusion on seclusion by "intentionally designing the . . . embedded SDKs to surreptitiously obtain, improperly gain knowledge of, review, and/or retain New Mexico citizens' activities" through persistent identifiers embedded in apps directed at children); *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1031-37 (N.D. Cal. 2019) (holding that plaintiffs stated claims for intrusion upon seclusion and invasion of privacy under the California Constitution, in putative class action suits alleging that defendants used apps designed for children to track online behavior on a device and user-specific level, and that defendants exploited the data, without disclosure or consent, for profit, observing that "a mobile phone has become 'almost a "feature of human anatomy"' that provides a wealth of personal information about its user. *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)). Cell phones and mobile devices are 'compulsively' carried and used by most people, *see, e.g., Carpenter*, 138 S. Ct. at 2218, including kids. The persistent identifiers and other data harvested to track users on these ubiquitous mobile devices involve collection practices that exceed those of the cookies in *Nickelodeon* . . . ."); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1231-33 (C.D. Cal. 2017) (denying defendants' motion to dismiss plaintiffs' intrusion upon seclusion claims under California, Florida and Washington law and invasion of privacy under the California Constitution and the Massachusetts Privacy Act where plaintiffs alleged that the interactivity function on Vizio Smart TVs remained on even when it had been turned off, resulting in the collection of information about plaintiffs' identities and television viewing histories); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 991-93 (N.D. Cal. 2015) (denying defendants' motions to dismiss intrusion on seclusion claims arising from the transfer of contact information from users' mobile address books when users selected the "Find Friends" feature to connect with friends on social networks).

sert 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."[197]

Some claims also suffer because of efforts to shoehorn novel privacy theories into existing unfair competition, statutory or common law remedies.[198] For example, in *Steinberg v.*

---

[197]*In re SAIC Corp.*, 45 F. Supp. 2d 14, 28 (D.D.C. 2014); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' invasion of privacy claims under the California Constitution and common law where plaintiffs alleged that the defendant disclosed to third parties their LinkedIn IDs and the URLs of the LinkedIn profile pages that the users viewed because "[a]lthough Plaintiffs postulate that these third parties could, through inferences, de-anonymize this data, it is not clear that anyone has actually done so."). In *SAIC*, Judge James E. Boasberg, Jr. explained that "[i]f no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated." *Id.* at 28-29, *citing* 5 C.F.R. § 297.102 (Under Privacy Act, "[d]isclosure means providing *personal review* of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian.") (emphasis added); *Walia v. Chertoff*, No. 06—6587, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008) ("accessibility" is not the same as "active disclosure"); *Schmidt v. Dep't of Veterans Affairs*, 218 F.R.D. 619, 630 (E.D. Wis. 2003) (Disclosure is "the placing into the view of another information which was previously unknown," requiring that information be "actually viewed."); *Harper v. United States*, 423 F. Supp. 192, 197 (D.S.C. 1976) (Disclose means "the imparting of information which in itself has meaning and which was previously unknown to the person to whom it was imparted."); *Fairfax Hospital v. Curtis*, 492 S.E.2d 642, 644 (Va. 1997) (violation where third party "possess[ed]" and "reviewed" records); *see also Storm v. Paytime, Inc.*, 90 F. Supp. 3d. 359, 368 (M.D. Pa. 2015) (dismissing Pennsylvania privacy claims of employees for lack of standing where no information had been disclosed to a third party after a cyber-attack on the defendant's payroll provider).

[198]*See, e.g.*, *New Mexico ex rel. Balderas v. Tiny Lab Productions*, 457 F. Supp. 3d 1103, 1121-23 (D.N.M. 2020) (dismissing the State's New Mexico Unfair Practices Act claim under N.M. Stat. Ann. § 57-12-3, alleging that ad networks defendants violated the UPA by violating COPPA and by making "material misrepresentations and omissions" through "public-facing documents" related to their "privacy- and COPPA-violative conduct[,]" because none of the allegedly unfair, deceptive, or unconscionable practices were done "in connection with the sale, lease, rental, or loan of goods or services" as required by the UPA); *Department of Labor v. McConnell*, 305 Ga. 812, 817-19, 828 S.E.2d 352, 359-60 (2019) (affirming dismissal because there was no general duty of care to safeguard personal information under Georgia law and none could be inferred from the enactment of Georgia's security breach notification statute or a statute prohibit-

CVS Caremark Corp.,[199] 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 (or re-identify) 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[200] places no restrictions on the use of information once de-identified.[201] Plaintiffs' unfair competition and unjust enrichment claims were dismissed based on the lack of any value to the information, among other grounds.[202]

A claim for common law trespass generally requires a showing of substantial impairment, not merely unauthorized access.[203] For this reason, plaintiffs in putative behavioral advertising privacy class action suits may have difficulty

---

ing use and display of social security numbers, and because plaintiff could not state breach of fiduciary duty or invasion of privacy claims—where the Department of Labor had sent an email to approximately 1,000 state residents who had applied for unemployment benefits, which included a spreadsheet that listed the name, social security number, home phone number, email address, and age of over 4,000 state residents—because there was no confidential relationship to support a breach of fiduciary duty claim, and no intrusion on plaintiff's seclusion, to support a common law claim for invasion of privacy because the information disclosed did not affect reputation and the matters disclosed were not offensive and objectionable).

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

[200] 45 C.F.R. §§ 160.103, 164.502(d)(1) to 164.502(d)(2); *supra* § 26.11.

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

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

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

stating a claim even where unauthorized access is alleged.[204]

Where a plaintiff cannot state a claim under ECPA because access was found to be authorized by a Privacy Policy, TOU or otherwise, the plaintiff also may have difficulty establishing a claim for common law invasion of privacy premised on the same unauthorized access.[205] Privacy

---

[204]*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 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.").

[205]*See, e.g.*, *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953, 955 (N.D. Cal. 2017) (dismissing putative class claims under the Wiretap Act, California Constitution, California Information Privacy Act, and for California common law invasion of privacy, for allegedly sharing sensitive medical information, based on consent provided pursuant to Facebook's Data Policy and Cookie Policy), *aff'd*, 745 F. App'x 8 (9th Cir. 2018) ("He who consents to an act is not wronged by it." (quoting Cal. Civ. Code § 3515)); *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

claims arising at common law or arising under 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[206] or unique mobile device identifier numbers, personal data and geolocation information[207] (except in limited circumstances[208]). Similarly, in

---

and an email sent to subscribers advising them that the Policy had been updated, notified subscribers that CenturyTel, an ISP, used cookies and web beacons to gather information on its subscribers' browsing history, which it shared with NebuAd, a provider of tailored advertising services); *Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13, 2010) (dismissing plaintiff's invasion of privacy claim where the complaint sufficiently alleged plaintiff's subjective expectation of seclusion or solitude but this subjective expectation was not objectively reasonable in light of the disclosures in defendant's Subscriber Agreement and Privacy Notice and notice that use of the defendant's service constituted acceptance of the terms of the Subscriber Agreement and Privacy Notice; also dismissing plaintiff's ECPA claim, but denying defendant's motion with respect to trespass and CFAA claims), *vacated on other grounds*, 722 F.3d 1151, 1157-61 (9th Cir. 2013) (holding that the lower court erred in declining to compel arbitration). In the words of the *Deering* court, "there is no [objectively] reasonable expectation of privacy when a plaintiff has been notified that his Internet activity may be forwarded to a third party to target him with advertisements." *Deering v. CenturyTel, Inc.,* No. CV-10-63-BLG-RFC, 2011 WL 1842859, at *2 (D. Mont. May 16, 2011).

[206]*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.").

[207]*See In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 294-95 (3d Cir. 2016) (affirming dismissal of plaintiffs' New Jersey intrusion upon seclusion claim against Google for allegedly using tracking cookies to track website activity by children because tracking cookies can serve legitimate commercial purposes and "Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 829-31 (N.D. Cal. 2020) (dismissing plaintiffs' California intrusion upon seclusion claim because "Plaintiffs have not alleged sufficient information about the conversations that were allegedly intercepted and recorded to establish that they were had under circumstances that would give rise to a reasonable expectation of privacy."); *In re Facebook Internet*

a data breach case, a plaintiff could not state a claim for

Tracking Litig., 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015) (dismissing intrusion upon seclusion claims in a putative data privacy class action suit because plaintiffs "could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable" because 'Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit . . . [and] should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.' "; citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007)), *rev'd on other grounds*, 956 F.3d 589, 601-06 (9th Cir. 2020) (reversing dismissal of a subsequently amended Complaint containing more detailed allegations), *cert. denied*, 141 S. Ct. 1684 (2021); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 987-88 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' intrusion upon seclusion claim based on plaintiffs' inability to meet the "high bar" to allege the requisite "intrusion [that is] highly offensive to a reasonable person"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (holding that the alleged disclosure to third parties of the unique device identifier numbers of Apple mobile devices, personal data stored by users on those devices and geolocation information did not involve an egregious breach of social norms and therefore was not actionable under California's constitutional right to privacy); *see also In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *10 (N.D. Cal. Mar. 26, 2013) (following *iPhone Application Litigation* in dismissing plaintiff's constitutional right to privacy claim where plaintiffs alleged that Google allowed third party affiliates such as AdMob and AdWhirl to obtain unencrypted user data); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *14-15 (N.D. Cal. Mar. 26, 2013) (following *iPhone Application Litigation* in dismissing plaintiff's claim with leave to amend where the plaintiff merely alleged that Pandora obtained his PII and provided it to advertising libraries for marketing purposes, allegedly in violation of Pandora's privacy policy).

[208] *See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 295 (3d Cir. 2016) (vacating an order dismissing plaintiffs' intrusion upon seclusion claim against Viacom based on the collection of information using allegedly duplicitous tactics, where the Nickelodeon website allegedly included the false message: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"; "Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149-52 (3d Cir. 2015) (holding that plaintiffs stated claims under the California Constitution and California tort law where plaintiffs alleged practices that allegedly went beyond disclosed tracking to allegedly include overriding cookie blocking software to access information and involved alleged misstatements about its practices) *cert. denied*, 137 S. Ct. 36 (2016); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 629-31 (N.D. Cal. 2021) (holding that plaintiffs stated a claim for intrusion upon seclusion by alleging that Google collected user

invasion of privacy claim under Illinois law where he could not allege that the exposure of his information as a result of the breach resulted in an intrusion into private life that was intentional or a disclosure to the public at large.[51]

A plaintiff may be unable to state a 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 permitting the collection, use or dissemination of personal information.[209] A state law conver-

---

data from Chrome browser users who chose not to sync their browser histories with their Google accounts); *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1075-80 (N.D. Cal. 2021) (holding that plaintiffs stated a claim for intrusion upon seclusion by alleging that the defendant collected browsing history from users while they were in private browsing mode); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962 (N.D. Cal. 2015) (dismissing conversion and injunctive relief claims but denying defendants' motions to dismiss intrusion on seclusion claims arising from the transfer of contact information from users' mobile address books when users selected the "Find Friends" feature to connect with friends on social networks).

[51]*See Sweet v. BJC Health System*, Case No. 3:20-CV-00947-NJR, 2021 WL 2661569, at *8 (S.D. Ill. June 29, 2021) (dismissing plaintiff's claim). As explained by the court: "Under Illinois law, a party alleging intrusion into private life must show that the intrusion was intentional. *Lovgren v. Citizens First Nat. Bank of Princeton*, 126 Ill. 2d 411, 128 Ill. Dec. 542, 534 N.E.2d 987, 988 (Ill. 1989). Public disclosure, on the other hand, requires a showing that the information was disclosed to the public at large. *Cordts v. Chicago Tribune Co*., 369 Ill. App.3d 601, 307 Ill. Dec. 790, 860 N.E.2d 444, 450 (Ill. App. 2006)." 2021 WL 2661569, at *8.

[209]*See, e.g.*, *Huynh v. Quora, Inc.*, Case No. 18-cv-07597-BLF, 2019 WL 11502875, at *12 (N.D. Cal. Dec. 19, 2019) (dismissing plaintiffs' unjust enrichment claim, in a putative cybersecurity breach class action suit, because, under California law, unjust enrichment is an action in quasi-contract, which does not lie when an enforceable, binding agreement exists defining the rights of the parties); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888, at *5 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' New York unjust enrichment claim where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in defendant's Privacy Policy; "Consent . . . negates Plaintiffs' unjust enrichment claim because it removes the necessary element that 'the circumstances [of the enrichment] were such that equity and good conscience require defendants to make restitution.' "); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit over the alleged use of browser and flash cookies where the defendant's potential use of browser and flash cookies was disclosed to users in the defendant's "Conditions of Use and Privacy Notice" so therefore any use was not inequitable and because "Plaintiffs have not plead any facts from which the Court might infer that Defendant's decision to record, collect,

sion claim may suffer the same defect.[210] 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.[211]

Although not analyzed to date in a data privacy case,

---

and use its account of Plaintiffs' interactions with Defendant came at Plaintiffs' expense."); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 718 (N.D. Cal. 2011) (dismissing plaintiffs' unjust enrichment claim with prejudice where plaintiffs assented to Facebook's "Terms and Conditions and Privacy Policy"), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their unjust enrichment claim).

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

[211]*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).[212]

Court also have rejected bailment claims in data privacy[52] (and data breach[53]) cases.

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[213] or zip code data[214] or the sale of de-identified personal

---

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

[52]*See, e.g.*, *Bell v. Blizzard Entertainment, Inc.*, No. 12-CV-09475, 2013 WL 12132044, at *9 (C.D. Cal. July 11, 2013) ("No court has held that personal information is a chattel that can be bailed").

[53]*See, e.g.*, *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) ("Plaintiffs allege that third parties stole the information, not that Target wrongfully retained that information."); *In re Sony Gaming Networks & Consumer Data Security Breach Litig.*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127 (N.D. Cal. 2008); *Richardson v. DSW, Inc.*, No. 05 C 4599, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005) (dismissing bailment and Illinois Consumer Fraud Act claims, in a security breach case).

[213]*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).

information.[215] Courts also have dismissed unjust enrichment claims based on the transfer of data simply because there is no separate market for data and plaintiffs could not articulate a basis for quantifying a benefit that allegedly had been conferred.[216]

Under the laws of some states, including California,[54] Illi-

---

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

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

[216]*See, e.g.*, *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 925 F.3d 955, 966 (8th Cir. 2019) (affirming dismissal of plaintiff's unjust enrichment claim in a cybersecurity breach case under Illinois law, where "[c]ommon sense counsels against the viability of Holmes's theory of unjust enrichment. Holmes paid for groceries, the price of which would have been the same whether he paid with cash or a credit card. He did not pay a premium 'for a side order of data security and protection.' ") (quoting *Irwin v. Jimmy John's Franchise, LLC*, 175 F. Supp. 3d 1064, 1072 (C.D. Ill. 2016) (applying Arizona law)); *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 912 (8th Cir. 2016) (affirming dismissal of plaintiff's claim for unjust enrichment under Minnesota law in a data privacy case, where the plaintiff alleged neither a benefit conferred in exchange for protection of his PII, nor that has he shown how GameStop's retention of his subscription fee would be inequitable).

[54]Since 2011, California courts have not recognized unjust enrichment as a separate claim. *See Hill v. Roll Int'l Corp*., 195 Cal. App. 4th 1295, 1307, 128 Cal. Rptr. 3d 109, 118 (1st Dist. 2011) (holding that ""[u]njust enrichment is not a cause of action, just a restitution claim.""); *see also, e.g., Astiana v. Hain Celestial Group, Inc*., 783 F.3d 753, 762 (9th Cir. 2015) (explaining that "in California, there is not a standalone cause of action for 'unjust enrichment,' which is synonymous with 'restitution.' "); *McCoy v. Alphabet, Inc*., Case No. 20-cv-05427-SVK, 2021 WL 405816, at *12 (N.D. Cal. Feb. 2, 2021) (dismissing plaintiff's claim for unjust enrichment because "it is not a cause of action."); *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 was not viable under California law); *In re iPhone Application Litig*., 844 F. Supp. 2d 1040,

1075–-76 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment based on *Hill v. Roll Int'l Corp.*); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 814–-15 (N.D. Cal. 2011) (dismissing a claim for unjust enrichment in light of *Hill v. Roll Int'l Corp*., ""[n]otwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment . . . ."); *In re iPhone Application Litig*., Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011) (dismissing plaintiff's claim for unjust enrichment, finding there is no longer any such cognizable claim under California law); *De Havilland v. FX Networks, LLC,* 21 Cal. App. 5th 845, 870, 230 Cal. Rptr. 3d 625, 646 (2d Dist. 2018) ("Unjust enrichment is not a cause of action."), *cert. denied,* 139 S. Ct. 800 (2019); *Bank of N.Y. Mellon v. Citibank, N.A.,* 8 Cal. App. 5th 935, 955, 214 Cal. Rptr. 3d 504, 520 (2d Dist. 2017) ("Unjust enrichment is not a cause of action, . . . or even a remedy, but rather 'a general principle, underlying various legal doctrines and remedies' . . . . It is synonymous with restitution.").

Some federal district court judges accept unjust enrichment, or at least quasi contract, as a stand-alone claim, not a remedy, even though California state courts appear to hold otherwise. *See, e.g.*, *Hart v. TWC Product and Technology LLC*, 526 F. Supp. 3d 592, 604-05 (N.D. Cal. 2021) (holding that plaintiff sufficiently pleaded a claim by alleging that TWC unjustly benefited from the use of his location data; "Although this Court has previously dismissed an unjust enrichment claim after concluding that there is no cause of action for unjust enrichment under California law, . . . it has more recently allowed such a claim to proceed . . . in accord with the Ninth Circuit, which has explained that an unjust enrichment claim may survive either 'as an independent cause of action or as a quasi-contract claim for restitution.' *ESG Capital Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016)."); *Williams v. Facebook, Inc*., 384 F. Supp. 3d 1043, 1057 (N.D. Cal. 2018) ("California courts typically consider unjust enrichment a principle of quasi-contract which gives rise to restitution. *See Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231, 166 Cal. Rptr. 3d 864 (2014). Courts can 'construe the cause of action as a quasi-contract claim seeking restitution' to avoid an unjust benefit conferred to the defendant 'through mistake, fraud, coercion, or request.' *Astiana v. Hain Celestial Grp., Inc*., 783 F.3d 753, 762 (9th Cir. 2015) (quoting 55 Cal. Jur. 3d Restitution § 2)."). The basis for doing so, is the Ninth Circuit's statement that unjust enrichment may survive either "as an independent cause of action or as a quasi-contract claim for restitution." *ESG Capital Partners, LP v. Stratos*, 828 F.3d 1023, 1038 (9th Cir. 2016) (holding that to allege unjust enrichment as an independent cause of action, a plaintiff must know that the defendant received and unjustly retained a benefit at the plaintiff's expense).

This view, however, appears to be a misreading of California law. As explained in an unreported Ninth Circuit opinion, "the California Supreme Court . . . clarified California law, allowing an independent claim for unjust enrichment to proceed in an insurance dispute." *Bruton v. Gerber Products Co*., 703 F. App'x 468, 470 (9th Cir. 2017), *citing Hartford Casualty Insurance Co. v. J.R. Marketing, L.L.C*., 61 Cal. 4th 988, 1000, 190 Cal. Rptr. 3d 599, 353 P.3d 319 (2015). *Hartford Casualty*, however, does

not support this reading. The opinion in *Hartford* did not squarely address the question of whether unjust enrichment was a remedy or an affirmative claim (or potentially both); The Supreme Court specifically limited its holding in that case to the facts and procedural history at bar. 353 P.3d at 326 ("We emphasize that our conclusion hinges on the particular facts and procedural history of this litigation."); *see also Abuelhawa v. Santa Clara University,* Case No. 20-CV-04045-LHK, 2021 WL 1176689, at *9-10 (N.D. Cal. Mar. 29, 2021) (Judge Koh) (strongly criticizing the misreading of California law on this point; "*Bruton* and *Hartford* are inapposite in two respects. First, subsequent California Court of Appeal decisions have recognized *Hartford*'s narrow scope. In 2019, for instance, a California Court of Appeal distinguished *Hartford* and held that plaintiff's claims for restitution were not "cognizable." *A.J. Fistes Corp. v. GDL Best Contractors, Inc*., 38 Cal. App. 5th 677, 697 (2019), as modified (Aug. 13, 2019), review denied (Nov. 13, 2019). The *A.J. Fistes* Court recognized that *Hartford*'s unusual facts cabined its holding. . . . Second, published post-*Hartford* decisions by California Courts of Appeal have confirmed that '[u]njust enrichment is not a cause of action.' *De Havilland*, 21 Cal. App. 5th at 870 (quoting *Hill*, 195 Cal. App. 4th at 1307). *Hartford* was decided in 2015. As recently as May 2020, a California Court of Appeal flatly held—without objection from the California Supreme Court despite two petitions for review—that 'summary adjudication of [an unjust enrichment] claim was proper because California does not recognize a cause of action for unjust enrichment.' *Hooked Media Grp., Inc. v. Apple Inc*., 55 Cal. App. 5th 323, 336, reh'g denied (June 19, 2020), transferred without decision on review (Sept. 23, 2020), publication ordered (Sept. 30, 2020), review denied (Dec. 31, 2020). Likewise, in 2018 and 2017, years after the *Hartford* decision in 2015, other California Courts of Appeal held that 'unjust enrichment is not a cause of action.' *De Havilland*, 21 Cal. App. 5th at 870 (quoting *Hill*, 195 Cal. App. 4th at 1307); *Bank of New York Mellon*, 8 Cal. App. 5th at 955 (same)."); *Khasin v. R.C. Bigelow, Inc*., No. 12-cv-02204-WHO, 2015 WL 5569161, at *1 (N.D. Cal. Sept. 21, 2015) ("The only aspect of the [*Hartford*] opinion that could be portrayed as a 'change' of law is narrowly confined to the question of the unjust enrichment of insureds' counsel when counsel's fees are excessive and not incurred for the benefit of the insured."); *ValveTech, Inc. v. Aerojet Rocketdyne, Inc.,* Case # 17-CV-6788-FPG, 2018 WL 4681799, at *5 (W.D.N.Y. Sept. 28, 2018) (making this same argument).

Subsequent state court opinions have persisted in holding that unjust enrichment is not a separate claim and have not read *Hartford* in the same way as the Ninth Circuit in *Bruton. See, e.g.*, *De Havilland v. FX Networks, LLC,* 21 Cal. App. 5th 845, 870, 230 Cal. Rptr. 3d 625, 646 (2d Dist. 2018) ("Unjust enrichment is not a cause of action."), *cert. denied,* 139 S. Ct. 800 (2019); *Bank of N.Y. Mellon v. Citibank, N.A.,* 8 Cal. App. 5th 935, 955, 214 Cal. Rptr. 3d 504, 520 (2d Dist. 2017) ("Unjust enrichment is not a cause of action, . . . or even a remedy, but rather 'a general principle, underlying various legal doctrines and remedies' . . . . It is synonymous with restitution."); *see also, e.g.*, *Abuelhawa v. Santa Clara University,* Case No. 20-CV-04045-LHK, 2021 WL 1176689, at *9-10 (N.D. Cal. Mar. 29, 2021) (Judge Koh) ("As published Ninth Circuit precedents have long required, this Court sitting in diversity 'must follow the decision

nois,[218] New Jersey,[219] and possibly Texas,[55] a separate claim may not even be asserted for unjust enrichment, which is viewed by those states as a request for restitution, not a separate cause of action. Even where recognized, a claim for unjust enrichment may not be viable if the data does not have a value or enrich the defendant.[220]

---

of the intermediate appellate courts of the state unless there is convincing evidence that the highest court of the state would decide differently.' . . . Nothing suggests that the California Supreme Court would extend *Hartford* to the instant case. Thus, this Court must follow the repeated holdings of California Courts of Appeal. Because '[u]njust enrichment is not a cause of action,' Plaintiffs' unjust enrichment claim cannot proceed. *De Havilland*, 21 Cal. App. 5th at 870 (quoting *Hill*, 195 Cal. App. 4th at 1307)").

[218]*See Sheridan v. iHeartMedia, Inc.*, 255 F. Supp. 3d 767, 781 (N.D. Ill. June 5, 2017) (dismissing plaintiffs' unjust enrichment claim, holding that unjust enrichment is not an independent cause of action), *citing Gagnon v. Schickel*, 368 Ill. Dec. 240, 983 N.E.2d 1044, 1052 (2012).

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

[55]*See Elias v. Pilo,* 781 F. App'x 336, 338 n.3 (5th Cir. 2019) (collecting cases and observing that "[c]ourts of appeals in Texas appear split on whether unjust enrichment is an independent cause of action.").

[220]*See, e.g.*, *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 36-37 (2d Cir. 2017), *aff'g*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *13 (S.D.N.Y. Aug. 17, 2016) (affirming dismissal of plaintiffs' claim where they failed to plead injury based on misappropriation of the value of their browsing information). *But see Moeller v. American Media, Inc.*, 235 F. Supp. 3d 868, 875-76 (E.D. Mich. 2017) (holding that plaintiff stated a claim for unjust enrichment under Michigan law, which requires a plaintiff to allege (1) the receipt of a benefit by the defendant from the plaintiff and (2) an inequity resulting to the plaintiff because of the retention of that benefit, where plaintiff alleged that defendants' allegedly unlawful disclosure of plaintiffs' personal information rendered their magazine subscriptions from defendants less valuable and that the defendants retained this benefit); *see also Perlin v. Time, Inc.*, 237 F. Supp. 3d 623, 643 (E.D. Mich. 2017) (holding that plaintiff stated a plausible unjust enrichment claim by alleging that she conferred a benefit on defendant by paying subscription

California likewise does not recognize a separate cause of action for restitution, which is a remedy that a plaintiff may elect, not a claim.[221]

Even negligence claims may be difficult to sustain in the absence of injury.[222] Just because plaintiffs may be able to allege sufficient injury for purposes of Article III standing, does not mean that the same allegation constitutes injury for purposes of a negligence claim.[56] Negligence generally requires a showing of (1) a legal duty to use due care, (2) a

---

fees and providing personal information, which the defendant allegedly monetized by selling to "data miners" including information allegedly prohibited from disclosure by Michigan's Preservation of Personal Privacy Act, and that the defendant retained this benefit); *Raden v. Martha Stewart Living Omnimedia, Inc.*, Case No. 16-12808, 2017 WL 3085371, at *4 (E.D. Mich. July 20, 2017) (following *Moeller* and *Perlin*).

[221]*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).

[222]*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).

[56]*See, e.g.*, *Krottner v. Starbucks Corp.,* 406 F. App'x 129, 131 (9th Cir. 2010) (affirming dismissal of plaintiffs' negligence and implied contract claims, in a suit arising out of a security breach caused when a laptop was stolen, after reiterating that the same appellate panel's "holding that Plaintiffs-Appellants pled an injury-in-fact for purposes of Article III standing does not establish that they adequately pled damages for purposes of their state-law claims."), *citing Doe v. Chao*, 540 U.S. 614, 624–25 (2004) (explaining that an individual may suffer Article III injury and yet fail to plead a proper cause of action); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *5 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's negligence, breach of contract, and UCL claims in a data breach putative class action suit, noting that "the allegations required to sufficiently plead injury-in-fact for purposes of Article III standing are not the same as those required to plead damages for purposes of state law claims."); *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; "While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law."), *aff'd mem.*, 380 F. App'x 689 (9th Cir. 2010).

breach of that duty, (3) injury and (4) proximate causation (that the breach was the proximate or legal cause of injury).[223] To state a claim, a plaintiff in a data privacy case generally must show an "appreciable, nonspeculative, present injury."[224] Further, in most states, purely economic losses generally are not recoverable as tort damages under the economic loss rule.[225] Negligence claims potentially may be

---

[223]*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).

[224]*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; "Under California law, the breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action for negligence. . . . While Ruiz has standing to sue based on his increased risk of future identity theft, this risk does not rise to the level of appreciable harm necessary to assert a negligence claim under California law."), *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).

[225]*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); *Community Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803, 817-18 (7th Cir. 2018) (holding, under Illinois and Missouri law, that the economic loss rule barred issuing banks' tort claims against a retail merchant arising from the merchant's failure to adopt adequate security measures to prevent a data breach that resulted in the disclosure of information about the banks' customers' use of their credit and debit cards, even though there was no direct contract between the banks and the merchant, where the merchant assumed

disclaimed in user contracts, although gross negligence may not be disclaimed in some states.[226] 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

---

contractual data security responsibilities in joining the credit card networks, and all parties in the card networks expected other parties to comply with industry-standard data security policies as matter of contractual obligation); *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *6 (N.D. Cal. July 28, 2021) (dismissing with prejudice plaintiff's negligence claim where plaintiff was in privity of contract for the sale of goods with defendant and could not allege a special relationship); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1038-40 (N.D. Cal. 2021) (dismissing, in a putative data privacy class action suit, plaintiffs' California negligence claim alleging that Zoom failed to protect the security of its platform against breaches referred to as "Zoombombing," which allegedly exposed users to harmful material, based on the economic loss rule); *Gardiner v. Walmart Inc.*, Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *8-9 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's negligence claim in a data breach putative class action suit because plaintiff's claim for the value of lost time constituted an economic loss and the plaintiff could not plead the existence of a special relationship); *In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014) (dismissing plaintiffs' California, Illinois and Massachusetts negligence claims under the economic loss rule in data security breach putative class action suit); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' negligence claim in a data privacy putative class action suit, holding that under California law injuries from disappointed expectations from a commercial transaction must be addressed through contract, not tort law); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528–31 (N.D. Ill. 2011) (dismissing plaintiffs' negligence and negligence *per se* claims under the economic loss rule in a security breach putative class action suit); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (dismissing plaintiff's negligent misrepresentation claim under the economic loss doctrine in a putative class action suit involving the alleged disclosure of plaintiff's email address and the potential dissemination of certain personal information from her Emigrant Bank account); *see generally infra* § 27.07 (analyzing the economic loss doctrine and narrow exceptions to it applied in a minority of jurisdictions).

[226] *See, e.g.*, *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, 402 F. Supp. 3d 767, 799-800 (N.D. Cal. 2019) (denying defendant's motion to dismiss plaintiff's claim for gross negligence because, under California law, exculpatory clauses that may waive liability for ordinary negligence are not effective to waive claims based on gross negligence).

ordinary purposes" for which the goods were intended.[227]

Intentional or negligent misrepresentation, deceit and fraud claims likewise need to be pled with specificity.[228]

In suits brought by Utah residents, Utah's Notice of Intent to Sell Nonpublic Personal Information Act generally requires a commercial entity that enters into a commercial transaction with a consumer who provides it with nonpublic personal information to give notice to the consumer before the entity discloses nonpublic information to a third party for compensation (subject to certain exceptions).[57] The statute is not frequently asserted in litigation, however, because class action relief is unavailable; only individual claims may

---

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

[228]*See, e.g., Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1194 (N.D. Cal. 2020) (dismissing, with leave to amend, claims for intentional misrepresentation and omission, deceit by concealment or omission under Cal. Civ. Code §§ 1709, 1710, and negligent misrepresentation, for lack of reliance, in a putative data privacy class action suit alleging that Facebook tracked plaintiffs' device location and IP address when its Privacy Policy stated that these data elements would be collected "depending on the permissions you've granted."); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1228-34 (C.D. Cal. 2017) (dismissing (with leave to amend) plaintiffs' claims for fraud, negligent misrepresentation, and false advertising, but denying defendants' motion to dismiss plaintiffs' fraudulent omission, invasion of privacy and unjust enrichment claims, in a putative data privacy class action suit involving Vizio smart TVs).

[57]Utah Code Ann. § 13-37-201.

be pursued.[58]

Class Certification

Even where Internet privacy claims survive motions to dismiss or summary judgment, they may be ill-suited for class certification because the proposed classes are defined in terms of conduct for which no records exist, and are therefore unascertainable,[229] or involve numerous individualized inquiries[230] into issues of consent, causation, reliance,

---

[58]*See* Utah Code Ann. § 13-37-203(3); *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *5 (N.D. Cal. July 28, 2021) (denying defendant Jones' individual request to dismiss plaintiff's claim, but dismissing the Utah Class Claims based on section 13-37-203).

[229]*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).

[230]*See, e.g.*, *Orduno v. Pietrzak*, 932 F.3d 710, 715-17 (8th Cir. 2019) (affirming the lower court's order denying certification of a putative class of people whose personal information had been wrongfully accessed by Dayton's police chief, in violation of the Driver's Privacy Protection Act, where individual questions predominated because putative class members would have had to show that the defendant "knowingly" used personal information "from a motor vehicle record, for a purpose not permitted by law" pursuant to 18 U.S.C.A. § 2724(a), which would require evidence of the particular circumstances under which their particular information was accessed, to determine whether the defendant's purpose was impermissible); *Dancel v. Groupon, Inc.*, Case No. 18 C 2027, 2019 WL 1013562 (N.D. Ill. Mar. 4, 2019) (denying certification of a proposed class of Instagram users, alleging violations of the Illinois Right to Publicity Act, arising out of Groupon's alleged practice of using photos posted to Instagram (other than those set to private) that were tagged with the accounts of particular businesses, to make small versions of those photos visible to Groupon users visiting the Groupon Deal and Merchant pages for those businesses, because the issue of whether a given putative class member was identified to a reasonable audience by the defendant's use of ImageURLs (such as charlotteagenda, kban7 and artisbarbie) "is inherently a question of fact that cannot be answered with the same evidence across the putative class."), *aff'd*, 949 F.3d 999 (7th Cir. 2019) (affirming the lower court's order denying certification where the question of whether a person's user name is part of their identity would have to be decided on a username-by-username basis); *Opperman v. Kong Technologies, Inc.*, Case No. 13-cv-00453-JST, 2017 WL 3149295 (N.D. Cal. July 25, 2017) (denying class certification in an invasion of privacy case alleging that Apple had misrepresented the security features on some of its devices, because plaintiffs could not show that common issues predominated over individual questions or provide a feasible way of measuring damages; "Plaintiffs have not shown that class members saw, heard, or relied upon representations about the specific security features—sandboxing and the Curated App Store—at issue in the case."); *Peterson v. Aaron's, Inc.*, Civil

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.*,[231] 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.[232]

Similarly, in *In re Google Inc. Gmail Litigation*,[233] the court declined to certify a class action suit where common ques-

---

Action No. 1:14-CV-1919-TWT, 2017 WL 364094, at *6-10 (N.D. Ga. Jan. 25, 2017) (denying certification in a suit alleging that a franchisee unlawfully accessed their Rent-to-Own computers from a remote location and collected private information stored on them including, when activated, screen shots, keystrokes, and webcam images, because intrusion upon seclusion claims require highly individualized analyses, as would issues of consent and damages); *Backhaut v. Apple Inc.*, Case No. 14-CV-02285-LHK, 2015 WL 4776427 (N.D. Cal. Aug. 13, 2015) (denying certification of a proposed class alleging that Apple wrongfully intercepted, stored, and otherwise prevented former Apple device users from receiving text messages sent to them from current Apple device users as unascertainable and one in which individualized issues would predominate over common questions, after concluding that plaintiffs lacked Article III standing to sue for injunctive relief and therefore were limited to damages on their claims under the Wiretap Act and California law), *aff'd on other grounds*, 723 F. App'x 405 (9th Cir. 2018) (affirming summary judgment for the defendant and therefore finding it unnecessary to reach the issue of the propriety of class certification).

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

[232] *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).

[233] *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).

tions 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.

In some cases, the claims remaining after motion practice are so limited that the named representative's claims are not typical of the class he or she seeks to represent and the named representative therefore is not an adequate representative. In *Svenson v. Google Inc.*,[234] for example, after several rounds of briefing motions to dismiss, class discovery and Google's motion for summary judgment, the court granted Google summary judgment on the remaining three claims for breach of contract, breach of the duty of good faith and fair dealing and unfair competition under Cal. Bus. & Prof. Code § 17200.[235] In the alternative, the court denied class certification because Svenson was subject to a unique defense to the contract claims, in that she asserted injury resulting from her lost expectation of privacy protection, but she purchased the "SMS MMS to Email" App at issue in the case for a second time on Google Play *after* discovering Google's alleged practice of granting sellers potential access to buyers' information and *after* filing the lawsuit. Accordingly, Judge Beth Labson Freeman ruled that, under those circumstances, the court would deny Svenson's motion for class certification for failure to establish typicality and adequacy of representation within the meaning of Federal Rule of Civil Procedure 23(a), even if it had not granted summary judgment in favor of Google.[236]

Whether putative class members can establish Article III standing to assert common claims also may impact class determinations.[237] Needless to say, where the named plaintiff

---

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

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

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

[237]*See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) (holding that only 1,853 of 8,185 individuals in a certified class had standing); *Gonzalez v. Corning,* 885 F.3d 186, 193-95 (3d Cir. 2018) (affirming denial of class certification where the plaintiffs could not establish commonality under Rule 23(a) because they lacked Article III standing to assert the one issue common to the putative class which was in the nature of an advisory

lacks standing, a class may not be maintained.[238]

Class certification also may be improper where enforcement of a Privacy Statement under multiple different state laws would undermine a finding of commonality.[239]

Efforts to avoid a finding that common questions predominate by defining the class in such a way that only those with meritorious claims are class members will generally fail because a so-called "fail-safe" class would allow putative class members to seek a remedy but not be bound by an adverse judgment (members would either win or, by virtue of losing, would not be deemed part of the class and therefore not bound by any judgment).[240]

On the other hand, in *Harris v. comScore,*[241] a court certified a class in a suit alleging Stored Communications Act and Computer Fraud and Abuse Act violations arising out of comScore's alleged practice of tracking the browsing activities of users who downloaded its tracking software. Likewise, claims under the Illinois Biometric Privacy Act have been

---

opinion and therefore nonjusticiable); *see generally supra* § 25.07 (internet class actions); *infra* § 27.07[2] (analyzing *Ramirez*).

[238]*See, e.g.*, *NEI Contracting & Engineering, Inc.*, 926 F.3d 528, 532-33 (9th Cir. 2019) (affirming decertification of a class, following the determination that the named plaintiff lacked Article III standing, in a suit brought under the California Invasion of Privacy Act, alleging that the defendant violated CIPA by recording customer orders without consent).

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

[240]*See, e.g.*, *Orduno v. Pietrzak*, 932 F.3d 710, 715-17 (8th Cir. 2019) (affirming the lower court's order denying certification of a putative class of people whose personal information had been wrongfully accessed by Dayton's police chief, in violation of the Driver's Privacy Protection Act, where individual questions predominated because putative class members would have had to show that the defendant "knowingly" used personal information "from a motor vehicle record, for a purpose not permitted by law" pursuant to 18 U.S.C.A. § 2724(a), which would require evidence of the particular circumstances under which their particular information was accessed, to determine whether the defendant's purpose was impermissible, and plaintiff's proposed "fail-safe" class was impermissible).

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

certified as a class action.[242]

Cases have been certified as liability classes seeking damages.[59] Courts also may certify equitable classes pursuant to Rule 23(b)(2) even where a common question class action would be inappropriate.[243]

While suits seeking to frame uses of new technologies as computer crime violations on the whole have not been very successful on the merits, potential claims may be easier to plead where a plaintiff can show a real injury and a clear lack of consent or authorization. For example, a court may allow a claim to proceed where a defendant is alleged to have engaged in conduct materially different from what was represented.[244] 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.[245]

---

[242]*See, e.g.*, *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019) (affirming certification of a 23(b)(3) common question class of Illinois users of Facebook's website for whom the website created and stored a face template after June 7, 2011), *cert. denied*, 140 S. Ct. 937 (2020); *Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 699 (N.D. Cal. 2019) (certifying an equitable class, but denying certification of damages class).

[59]*See, e.g.*, *Williams v. Apple,* 338 F.R.D. 629 (N.D. Cal 2021) (certifying a class of iCloud cloud storage subscribers who alleged that Apple failed to disclose that their data was being stored on remote servers and facilities not operated by Apple).

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

[244]*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).

[245]Not all privacy policies will support breach of contract claims. *See, e.g.*, *In re Equifax, Inc., Customer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1331-32 (N.D. Ga. 2019) (granting defendant's motion to dismiss breach of contract claims premised on Equifax's Privacy Policy, because "even if the Plaintiffs establish[ed] that the Privacy Policy was part of this express contract, the terms of the agreement provide that Equifax will not 'be liable to any party for any direct, indirect, special or other consequential damages for any use of or reliance upon the information found at this web site.' Thus, even assuming the Privacy Policy was incorporated by reference, under the terms of this agreement the Plaintiffs

Likewise, where there is a security breach and resulting harm, a plaintiff may be able to state a claim.[246]

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.[247] The Act provides for statutory damages in cases

---

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

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

Breach of contract claims also will fail where plaintiffs make allegations that contradict the actual terms of a Privacy Policy. *See, e.g.*, *In re Google Assistant Privacy Litigation*, 457 F. Supp. 3d 797, 832-33 (N.D. Cal. 2020) (dismissing plaintiffs' breach of contract claim where plaintiff's allegations were contradicted by the terms of the Privacy Policy).

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

[247]*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 Informa-

where violations may be shown.

State law claims premised on child privacy violations may be preempted by the Children's Online Privacy Protection Act,[60] which has been construed as preempting liability for commercial activities or actions by operators in interstate or foreign commerce in connection with an activity or action that is inconsistent with the treatment of those activities or actions under COPPA.[61] Some courts have ruled that state law claims that would impose different obligations from COPPA will be found preempted, while those consistent with COPPA will not be deemed preempted.[62] At least one court,

---

tion Security & Privacy News (Autumn 2011); *see generally supra* § 26.13[6][E] (analyzing the case and underlying statute).

[60]15 U.S.C.A. §§ 6501–6506; *see generally supra* § 26.13[2] (analyzing the statute and associated regulations).

[61]*See* 15 U.S.C.A. § 6502(d); *see generally supra* § 26.13[2][F] (analyzing COPPA preemption).

[62]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 291-93 (3d Cir. 2016) (rejecting the argument that common law intrusion upon seclusion claims brought by minor children who alleged that their personal information had been collected using allegedly duplicitous tactics was preempted by COPPA because the claim rested on common law duties that were compatible, not inconsistent with COPPA; "the wrong at the heart of the plaintiffs' intrusion claim is not that Viacom and Google collected children's personal information, or even that they disclosed it. Rather, it is that Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses. Understood this way, there is no conflict between the plaintiffs' intrusion claim and COPPA. While COPPA certainly regulates whether personal information can be collected from children in the first instance, it says nothing about whether such information can be collected using deceitful tactics. Applying the presumption against preemption, we conclude that COPPA leaves the states free to police this kind of deceptive conduct."), *cert. denied*, 137 S. Ct. 624 (2017); *New Mexico ex rel. Balderas v. Tiny Lab Productions,* 457 F. Supp. 3d 1103, 1120-21 (D.N.M. 2020) (dismissing as preempted New Mexico's state law claims against various ad networks, which were premised on the collection of personal information from children, using Tiny Lab's child-directed apps, without the requisite parental consent, and which alleged the same conduct underlying New Mexico's COPPA claims against the defendants in the same case, which the court dismissed, because allowing the state law claims to proceed could have resulted in inconsistent treatment; but denying Google's motion to dismiss state law claims because the court had denied Google's motion to dismiss New Mexico's COPPA claim against Google and "to allow Plaintiff's state law claims against Google to proceed would result in the imposition of liability only for conduct that violates COPPA, and thus would not run afoul of COPPA's express preemption provision."); *see also New Mexico ex rel. Balderas v. Tiny Lab Productions,* 516 F. Supp.

however, has taken a broader view of the scope of COPPA preemption of civil claims brought by litigants other than the FTC or a state Attorney General, holding that allowing private civil litigants to sue for violations of COPPA under state law would run afoul of COPPA's express preemption clause due to the inconsistency with the remedial scheme that assigns enforcement of COPPA to the FTC and state attorneys general[63]

State law claims may also be preempted (and federal claims precluded) 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, in certain instances, by the Communications Decency Act.[248] The immunity, however, does not apply, among other things, to claims brought under the federal Electronic Com-

---

3d 1293 (D.N.M. 2021) (granting Google's motion for reconsideration on the proper interpretation of the "mixed-audience exception" to the COPPA rule, but reaffirming its holding).

[63]*Hubbard v. Google LLC,* 508 F. Supp. 3d 623, 630-32 (N.D. Cal. 2020). Northern District of California Judge Beth Labson Freeman expressly rejected preemption analysis that looked to whether a claim was consistent or inconsistent with COPPA. *See id.* at 630-32. In holding plaintiffs' state law claims preempted, Judge Freeman considered the Third Circuit's analysis in *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 291-93 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017), to be instructive, observing that "the Third Circuit would not have reached the same conclusion absent the allegations of deceit, which it expressly found to go beyond the provisions of COPPA." 508 F. Supp. 3d at 632. She distinguished *New Mexico ex rel. Balderas v. Tiny Lab Productions,* 457 F. Supp. 3d 1103, 1120-21 (D.N.M. 2020) as a suit brought by New Mexico's Attorney General, who is authorized to enforce violations of COPPA under the statute's remedial scheme. 508 F. Supp. 3d at 632. She also noted that while not the basis of the preemption decision, "it appears there was deception alleged on the part of the Tiny Lab defendants, who marketed the subject applications as 'suitable and safe for children.' " *Id.*; *see generally supra* § 26.13[2][F] (analyzing COPPA preemption).

[248]*See* 47 U.S.C.A. § 230(c); *see also, e.g.*, *Obado v. Magedson*, 612 F. App'x 90, 91-94 (3d Cir. 2015) (affirming dismissal of plaintiff's claim for invasion of privacy against various service providers, search engines and domain name registrars for republishing and allegedly manipulating search engine results, based on the CDA); *Carafano v. Metrosplash.com. Inc.*, 339 F.3d 1119, 1125 (9th Cir. 2003) (holding plaintiff's privacy claim preempted); *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *5-6 (N.D. Cal. Mar. 1, 2021) (dismissing putative class action plaintiffs' California right of publicity claim under Cal. Civ. Code § 3344 and common law intrusion upon seclusion claim (as well as claims for unjust enrichment and unlawful and unfair business practices under Cal. Bus. & Prof. Code § 17200), arising out of defendant's use of

munications Privacy Act[249] "or any similar State law."[250]

If plaintiffs assert that their identity is confidential or want to preserve their privacy, they may seek leave to file a complaint under seal, obscure a person's name in public filings, sue as a John Doe, or take other action.[251] In *In re Ashley Madison Customer Data Security Breach Litigation*,[252] for example, the court ruled that unnamed plaintiffs in a putative class action suit did not need to identify themselves in connection with a public filing but that named plaintiffs, who sought to represent a putative class of users of the

---

their yearbook photos and related information in its subscription database, based on CDA immunity pursuant to 47 U.S.C.A. § 230(c)(1)); *In re Zoom Video Communications Inc. Privacy Litigation*, 525 F. Supp. 3d 1017, 1028-35 (N.D. Cal. 2021) (dismissing as precluded by section 230(c)(1) in a putative class action suit, claims for failing to protect the security of Zoom against breaches referred to as "Zoombombing," which allegedly exposed users to harmful third party content, to the extent plaintiffs' claims challenged the harmfulness of third party content and derived from defendant's status as publisher or speaker); *Gavra v. Google Inc.*, 5:12-CV-06547-PSG, 2013 WL 3788241 (N.D. Cal. July 17, 2013) (dismissing with prejudice an attorney's claim for invasion of privacy arising from Google's alleged failure to remove unflattering videos posted by a former client); *Regions Bank v. Kaplan*, 8:12-CV-1837-T-17MAP, 2013 WL 1193831, at *18 (M.D. Fla. Mar. 22, 2013) (dismissing plaintiff's claim for invasion of privacy arising from a "Fraud-Net" alert bulletin published by a third party on the Florida Bankers Association's website); *Shah v. MyLife.Com, Inc.*, 3:12-CV-1592 -ST, 2012 WL 4863696, at *3 (D. Or. Sept. 21, 2012) (recommending that defendants' motion to dismiss be granted; holding that MyLife.com and Google, Inc. "cannot be sued for simply republishing information provided by third parties, including any claim under state law for invasion of privacy by an internet posting of personal information obtained from another party."); *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).

[249]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]).

[250]47 U.S.C.A. § 230(e)(4).

[251]*See generally infra* § 37.02[A] (analyzing anonymity and pseudonymity in litigation).

[252]*In re Ashley Madison Customer Data Security Breach Litigation*, MDL No. 2669, 2016 WL 1366616 (E.D. Mo. Apr. 6, 2016).

online "dating" website for married people looking to cheat on their spouses, had to disclose their identities—given the importance of the role of a class representative—so that the public, including putative class members who they sought to represent, knew who was guiding and directing the litigation. The court ruled, however, that they did not need to be specifically identified by name; they merely needed to be identifiable.[253]

---

[253] *In re Ashley Madison Customer Data Security Breach Litigation*, MDL No. 2669, 2016 WL 1366616, at *4 (E.D. Mo. Apr. 6, 2016). District Court Judge John Ross explained that the decision to allow pseudonyms is within a court's discretion. Courts have allowed plaintiffs to proceed under fictitious names in instances such as (1) where the plaintiff is challenging government activity, (2) where the plaintiff is required to disclose information of the utmost intimacy, and (3) where the plaintiff risks criminal prosecution through the information contained in the pleading. *Id.* at *2 (quoting and citing earlier cases). He explained:

> In cases involving intensely personal matters, "the normal practice of disclosing the parties' identities yields to a policy of protecting privacy." *Southern Methodist Univ.*, 599 F.2d at 712-13 (citation and internal quotations marks omitted). Courts have generally allowed plaintiffs to litigate under pseudonym in cases involving allegations of sexual abuse and assault because they concern highly sensitive and personal subjects. *See e.g., St. Louis University*, 2009 WL 910738 (allowing rape victim to use a pseudonym because her privacy interest outweighed the public's right to access judicial records); *Doe v. Cabrera*, 307 F.R.D. 1, 5 (D. D.C. 2014) (same); *Doe H.M. v. St. Louis County*, No. 4:07-CV-2116-CEJ, 2008 WL 151629, *1 (E.D. Mo. 2008) (permitting use of pseudonym in case involving child sexual abuse). Likewise, cases involving abortion and birth control use, homosexuality and transsexuality, AIDS, and the welfare of abandoned or illegitimate children, have been deemed to involve information sufficiently sensitive and private to warrant anonymity. *Southern Methodist Univ.,* 599 F.2d at 712-13 (citations omitted); *Lindsey v. Dayton-Hydson Corp*., 592 F.2d 1118, 1125 (10th Cir. 1979); *Doe v. Blue Cross & Blue Shield of Wis*., 112 F.3d 869, 872 (7th Cir. 1997); *Doe v. Blue Cross & Blue Shield of Rhode Island*, 794 F. Supp. 72, 74 (D.R.I. 1992); *W.G.A*., 184 F.R.D. 616. *See also Doe v. Stegall*, 653 F.2d 180, 186 (5th Cir. 1981) (plaintiff allowed to proceed anonymously in light of threats of violence made against him for challenging prayer and Bible reading in schools). "The common thread running through these cases is the presence of some social stigma or the threat of physical harm to the plaintiffs attaching to disclosure of their identities to the public record." *Blue Cross & Blue Shield of Rhode Island*, 794 F. Supp. at 74 (quoting *Doe v. Rostker*, 89 F.R.D. 158, 161 (N.D. Cal.1981)).

2016 WL 1366616, at *3. Judge Ross reasoned that in *Ashley Madison,* plaintiffs' privacy interests were "not as pronounced" as those in the cases discussed above, but he nevertheless found that the possible injury to plaintiffs rose above "the level of mere embarrassment or harm to reputation" and therefore weighed against public disclosure. *Id.* at *4. He elaborated that "[t]he disclosure of Plaintiffs' identities could expose their sensitive personal and financial information—information stolen from Avid when its computer systems were hacked—to public scrutiny and exacerbate the privacy violations underlying their lawsuit." *Id.*; *see gener-*

As noted earlier, many putative class action cases settle. Class action settlements may or may not be structured to provide payments and/or equitable relief, in addition to an award of attorneys' fees to class counsel.[254] Many settlements

---

ally infra § 37.02[2][A] (analyzing anonymity and pseudonymity in litigation).

[254]*See, e.g.*, *In Re Google Inc. Cookie Placement Consumer Privacy Litigation*, 934 F.3d 316, 321, 325-32 (3d Cir. 2019) (vacating and remanding a $5.5 Million *cy pres*-only 23(b)(2) settlement in a case resolving claims over Google's alleged use of web browser "cookie" to track data from internet users, brought under the California constitution and intrusion upon seclusion); *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1121-24 (9th Cir. 2020) (approving settlement of ECPA Title I Wiretap Act and California Invasion of Privacy Act (CIPA) claims alleging nonconsensual capturing, reading, and use of website links included in private messages sent or received by users and warding $3.89 million in attorneys' fees and costs; "given how little the class could have expected to obtain if it had pursued claims further based on the facts alleged here (and, correspondingly, how little it gave up in the release), it was not unreasonable that the settlement gave the class something of modest value."); *In re Google Referrer Header Privacy Litig.*, 869 F.3d 737 (9th Cir. 2017) (affirming a *cy pres* only settlement and holding that the district court did not abuse its discretion in awarding $2.125 million in attorneys' fees), *vacated,*, 139 S. Ct. 1041 (2019) (remanding for consideration of whether plaintiffs had Article III standing); *Fraley v. Batman*, 638 F. App'x 594 (9th Cir. 2016) (affirming approval of *cy pres* class action settlement with Facebook), *cert. denied*, 137 S. Ct. 68 (2016); *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 Consumers Legal Remedies Act, and California Computer Crime Law (Cal. Penal Code § 502), and for remedies for unjust enrichment), *cert. denied*, 571 U.S. 1003 (2013); *In re TikTok, Inc., Consumer Privacy Litigation*, MDL No. 2948, 2021 WL 4478403 (N.D. Ill. Sept. 30, 2021) (granting preliminary approval to the proposed settlement of a putative class action suit alleging violations of the Illinois Biometric Information Act, the Computer Fraud and Abuse Act, the Video Privacy Protection Act, California's Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 et seq., California's False Advertising Law, *id.* §§ 17500 *et seq.*, the right to privacy under the California Constitution, Cal. Const. art. I, § 1, the consumer protection statutes of multiple states, and claims for California intrusion upon seclusion and unjust enrichment, comprised of a $92 million settlement fund and injunctive relief, among other things); *In re Google LLC Street View Electronic Communications Litigation*, __ F. Supp. 3d __, 2020 WL 1288377, at *4-17 (N.D. Cal. 2020) (granting final approval of a cy pres settlement in an ECPA (Wiretap Act) suit, awarding plaintiffs' counsel 25% of the value of the settlement in fees, or $3,039,625); *In re Yahoo Mail Litigation*, No. 13-cv-4980-LHK, 2016 WL 4474612 (N.D.

also include incentive awards to named representatives.[64]

Cal. Aug. 25, 2016) (granting final approval of a class action settlement); *Perkins v. LinkedIn Corp.*, Case No. 13-CV-04303-LHK, 2016 WL 613255 (N.D. Cal. Feb. 16, 2016) (granting final approval of a $13 million settlement for a class of approximately 20.8 million users, and awarding from that sum $3,250,000 in attorney's fees and $1,500 incentive awards each to nine plaintiff representatives); *Berry v. Schulman*, 807 F.3d 600 (4th Cir. 2015) (affirming approval of a FCRA settlement class); *In re LinkedIn User Privacy Litigation*, 309 F.R.D. 573 (N.D. Cal. 2015) (approving a settlement by a class of users who alleged that LinkedIn had failed to adequately protect user information for premium subscribers); *Kim v. Space Pencil, Inc.*, No. C 11-03796 LB, 2012 WL 5948951 (N.D. Cal. Nov. 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); *see generally supra* § 25.07[2] (analyzing class certification, settlement, and *cy pres*-only settlements).

Approval for proposed data privacy class action settlements has sometimes been denied. *See, e.g.*, *In re Target Corp. Customer Data Security Breach Litig.*, 847 F.3d 608 (8th Cir. 2017) (reversing and remanding class action settlement); *Matera v. Google, Inc.*, Case No. 15-CV-04062-LHK, 2017 WL 1365021 (N.D. Cal. Mar. 15, 2017) (denying preliminary approval to a proposed class action settlement over concerns about the clarity of notice and adequacy of evidence submitted in support of the proposed settlement). Where approval has not been obtained, it may be possible for the parties to modify the terms of the proposed settlement to address a court's concerns, and later obtain approval. *See, e.g.*, *In re Target Corp. Customer Data Security Breach Litigation*, 892 F.3d 968 (8th Cir. 2018) (affirming final approval of a class action settlement, following remand); *see generally infra* § 27.07[5] (analyzing major cybersecurity breach class action settlements).

[64]The Eleventh Circuit has held that incentive awards are akin to a salary and a bounty and are impermissible. *See Johnson v. NPAS Solutions, LLC,* 975 F.3d 1244, 1255-61 (11th Cir. 2020) (reversing approval of a TCPA class settlement that paid the named representative $6,000, holding that *Trustees v. Greenough*, 105 U.S. 527 (1882) and *Central Railroad & Banking Co. v. Pettus*, 113 U.S. 116 (1885) "prohibit the type of incentive award that the district court approved here—one that compensates a class representative for his time and rewards him for bringing a lawsuit. Although it's true that such awards are commonplace in modern class-action litigation, that doesn't make them lawful, and it doesn't free us to ignore Supreme Court precedent forbidding them."); *see also In re Equifax Inc. Customer Data Security Breach Litigation*, 999 F.3d 1247 (11th Cir. 2021) (applying *Johnson* in reversing a cybersecurity breach class action settlement on the issue of incentive awards to the named plaintiffs).

Other circuits have routinely allowed service awards to "compensate class representatives for work done on behalf of the class, to make up for

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.[255]

The volume of putative privacy class action suits filed since 2010 underscores that privacy suits, whether or not meritorious, may impose a significant cost on Internet and mobile companies. All members of a settlement class also must have Article III standing.[65]

Businesses may limit their risk of exposure to class action litigation by users or customers where there is privity of contract by including binding arbitration provisions and class action waivers in consumer contracts. As analyzed at length in section 22.05[2][M], arbitration provisions (including those containing a prohibition on class-wide remedies) are generally enforceable in standard form consumer contracts, including Terms of Use, as a result of the U.S. Supreme Court's 2011 decision in *AT&T Mobility, LLC v. Concepcion*[256] and subsequent case law. Class action waivers in contracts litigated in court, however, may or may not be enforceable,

---

financial or reputational risk undertaken in bringing the action, and, sometimes, to recognize their willingness to act as a private attorney general." *Rodriguez v. West Publishing Corp*., 563 F.3d 948, 958–59 (9th Cir. 2009).

[255]*See supra* § 25.07[2].

[65]*See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208 (2021) (holding that, where a class has been certified, "[e]very class member must have Article III standing in order to recover individual damages."). The Court declined to address whether every class member must demonstrate standing before a court certifies a class (*id.* n.4), but plainly the prosepect that, as in *Ramirez* – where the majority of the class was determined to lack standing following trial on the merits—potential standing issues have implications for typicality, adequacy of representation, predominance. manageability, and the definition of a proposed class, among other issues that courts must grapple with under Rule 23 in ruling on motions for class certification. Since standing may be raised at any time during the litigation, and must exist at all times, and for all claims and for each form of relief sought (*id.* at 2207-08; *Uzuegbunam v. Preczewski,* 141 S. Ct. 792, 796 (2021)), standing may play an even greater role in class certification decisions than it did prior to *Ramirez*. *See generally infra* § 27.07[2][B] (analyzing *Ramirez* in greater detail and in connection with cybersecurity breach putative class action suits).

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

depending on the jurisdiction whose law is applied.[257]

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.[258] Judges, however, closely scrutinize unilateral contracts with consumers and will not enforce arbitration provisions if assent to the proposed agreement has not been obtained[259] 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.[260]

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].

Class certification issues in internet and mobile cases are analyzed more extensively in section 25.07[2] in chapter 25.

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.

---

[257]*See supra* § 22.05[2][M].

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

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

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

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2023

Ian C. Ballon

2023 UPDATES – INCLUDING NEW AND IMPORTANT FEATURES

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator – a 5 volume-set & On Westlaw!

To order call 1-888-728-7677
or visit IanBallon.net

Key Features of E-Commerce & Internet Law

- AI, ML, screen scraping and data portability
- Antitrust in the era of techlash
- The CPRA, Virginia, Colorado and Nevada pricy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Software copyrightability and fair use after *Google v. Oracle*
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- The law of SEO and SEM – and its impact on e-commerce vendors
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi,* patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- Enforcing judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Applying the First Sale Doctrine to virtual goods
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Click fraud
- Copyright and Lanham Act fair use
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

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

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

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

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

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

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

****

ABOUT THE AUTHOR

****

IAN C. BALLON

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

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

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

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2023, 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

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

Mr. Ballon is also 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.lanBallon.net).

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

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2023

- **Antitrust in the era of techlash** (chapter 34)
- **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurty breach, data privacy, AdTech and TCPA class action suits.**
- **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid,* 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States,* 141 S. Ct. 1648 (2021)** (ch5)
- **FOSTA-SESTA** and ways to maximize CDA protection (ch 37)
- **IP aspects of the use of #hashtags** in social media (ch 6)
- The **CLOUD Act** (chapter 50)
- **Virginia, Colorado and Nevada privacy laws** (ch 26)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Digital economy litigation strategies**
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- **Website and mobile accessibility** under the ADA and state laws (chapter 48)
- **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **AdTech law** (chapter 28, Darren Abernethy)
- **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- **eSIGN case law** (chapter 15)