PRIVATE RIGHT OF ACTION FOR DATA BREACHES UNDER THE CPRA

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)

INTERNET AND COMPUTER LAW YEAR IN REVIEW

BERKELEY CENTER FOR LAW & TECHNOLOGY

FEBRUARY 2025

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

Ian has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2024). He 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 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 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. 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. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, 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. Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named a Northern California Super Lawyer every year from 2004 through 2024 and a Southern California Super Lawyer for every year from 2007-2024. 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 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 intellectual property law issues. 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. Ian 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

1798.199.85 or an order pursuant to section 1798.99.55 against the same person for the same violation.[23]

The Agency (or a court) must consider the good faith cooperation of a business, service provider, contractor, or other person, in determining the amount of any administrative fine or civil penalty for a violation of the CPRA (and may not award both an administrative fine and civil penalty).[24]

26.13A[14] Private right of action for data breaches

The CCPA (and, as of January 1, 2023, the CPRA) affords a private right of action, with the possibility of recovering statutory damages, for consumers "whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices . . . ."[1] The private right of action created by the CCPA may be brought *only* for data breaches arising from a business's failure to maintain reasonable security measures, and not

---

[23]*See* Cal. Civ. Code § 1798.199.90(d).

[24]*See* Cal. Civ. Code § 1798.199.100.

[Section 26.13A[14]]

[1]Cal. Civ. Code § 1798.150(a)(1). *Personal information* in this section is defined by reference section 1798.81.5, which is narrower in scope than the CCPA's definition in section 1798.140(o). *Personal information* under section 1798.81.5 means either of the following:

(A) An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  (i) Social security number.
  (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
  (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  (iv) Medical information.
  (v) Health insurance information.
  (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

any other failures to comply with the CCPA.[2] Nevertheless, the potential availability of statutory damages has created a strong incentive for plaintiffs' class action lawyers to assert CCPA claims whenever a data security incident affects California residents. Whether a plaintiff in fact may assert a CCPA claim in state or federal court (and potentially seek class certification) generally depends on whether (1) the plaintiff is a resident of California, (2) the defendant is a *business* (as defined in the statute) subject to the CCPA,[3] (3)

---

a physical or digital photograph, unless used or stored for facial recognition purposes.

(vii) Genetic data.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

Cal. Bus. & Prof. Code § 1798.81.5(d)(1). *Personal information* does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records." *Id.* § 1798.81.5(d)(4).

Medical information means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional. *Id.* § 1798.81.5(d)(2).

Health insurance information means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. *Id.* § 1798.81.5(d)(3).

Genetic data means any data, regardless of its format, that results from the analysis of a biological sample of an individual, or from another source enabling equivalent information to be obtained, and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom. *Id.* § 1798.81.5(d)(5).

Under the CPRA, the definition of *personal information* applicable to lawsuits brought pursuant to section 1798.150(a)(1) will be expanded to also include an "email address in combination with a password or security question and answer that would permit access to the account . . . ." *Id.* § 1798.150(a)(1) (effective Jan. 1, 2023).

[2]Cal. Civ. Code § 1798.150(c).

[3]*See, e.g.*, *In re Blackbaud, Inc., Customer Data Breach Litig.*, Case No. 3:20-mn-02972-JMC, 2021 WL 3568394, at *4-6 (D.S.C. Aug. 12, 2021) (denying defendant's motion to dismiss where the plaintiffs adequately alleged that Blackbaud was a *business* under the CCPA in a case arising out of a ransomware attack).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

the incident occurred on or after January 1, 2020[4] and (4) resulted in the unauthorized[5] access and exfiltration, theft, or disclosure of specific *personal information* (defined more narrowly than under the CCPA generally),[6] (5) the personal information was unencrypted or unredacted at the time when exfiltrated, stolen, or disclosed,[7] (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.[8] 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

---

[4]*See, e.g.*, *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for failing to allege that the breach occurred after January 1, 2020, when the CCPA took effect, and failing to adequately allege the disclosure of personal information as defined by the statute); *see also Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 4992539, at *2 (N.D. Cal. July 28, 2021) (dismissing plaintiff's CCPA claim with prejudice).

[5]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

[6]*See* Cal. Civ. Code §§ 1798.150(a)(1), 1798.81.5; *see also, e.g., Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for, among other things, failing to adequately allege the disclosure of personal information as defined by the statute).

As noted earlier in this section, the definition of *personal information* applicable to lawsuits brought pursuant to section 1798.150(a)(1) will be expanded under the CPRA to also include an "email address in combination with a password or security question and answer that would permit access to the account . . . ." Cal. Civ. Code § 1798.150(a)(1) (effective Jan. 1, 2023).

[7]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized);

[8]*See generally supra* § 22.05[2][M] (analyzing the enforceability of consumer arbitration claims, which under the Federal Arbitration Act and Supremacy Clause of the U.S. Constitution, will preempt inconsistent state laws or judge made rules favoring litigation of disputes). The CCPA does not purport to bar arbitration and, if it did, it would conflict with, and be preempted by, the Federal Arbitration Act. *See supra* § 22.05[2][M].

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

later in this section).

CCPA claims frequently are brought as putative class action suits because of the potential availability of statutory damages. Whether a case proceeds as a class action depends on whether plaintiffs can meet their burden of showing entitlement to class certification.[9] Where claims are subject to binding and enforceable arbitration agreements, however, a class typically may not be certified either in court or in arbitration.[10]

Many purported CCPA claims in fact are not viable because the information at issue was accessed and exfiltrated, stolen, or disclosed in encrypted or redacted form (even if it may have been subsequently decrypted or recompiled); the exfiltration, theft, or disclosure was authorized; the data elements exfiltrated, stolen, or disclosed do not qualify as *personal information* for purposes of Cal. Civ. Code §§ 1798.150(a)(1) and 1798.81.5; the defendant is not a *business* subject to the CCPA based on its size, revenue or use of personal information; the breach occurred prior to January 1, 2020; or the dispute is subject to binding arbitration. Some of these issues may be addressed through preliminary motion practice,[11] while some require affirmative evidence and therefore would have to be addressed on

---

[9]Class certification is analyzed in section 25.07[2] in chapter 25 and is also addressed in connection with data privacy putative class action suits in section 26.15, and in connection the data breach putative class action suits in section 27.07 (in chapter 27).

[10]*See generally supra* § 22.05[2][M] (analyzing the enforceability of arbitration provisions in consumer cases, class action waivers, and class arbitration).

[11]*See, e.g.*, *Gershfeld v. Teamviewer US, Inc.,* Case No. SACV 21-00058-CJC(ADSx), 2021 WL 3046775, at *2 (C.D. Cal. June 24, 2021) (dismissing plaintiff's CCPA claim, in a putative class action suit, where the disclosure alleged did not result from defendant's alleged storage of information "in a nonencrypted and nonredacted fashion," and was authorized, not unauthorized); *Gardiner v. Walmart Inc.,* Case No. 20-cv-04618-JSW, 2021 WL 2520103, at *2-3 (N.D. Cal. Mar. 5, 2021) (dismissing plaintiff's CCPA claim for failing to allege that the breach occurred after January 1, 2020, when the CCPA took effect, and failing to adequately allege the disclosure of personal information as defined by the statute).

In a number of cases, plaintiffs have voluntarily dismissed CCPA claims in response to motions to dismiss. *See, e.g.*, *McCoy v. Alphabet, Inc.,* Case No. 20-cv-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021); *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *4 (N.D. Cal. Jan. 30, 2021); *Shay v. Apple Inc.,* 512 F. Supp. 3d 1066, 1070 (S.D. Cal. 2021).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

motion for summary judgment or at trial.

Where a CCPA claim is plausibly alleged, a business may defend the claim by arguing, among other things, that the breach did not involve personal information, that the breach was not caused by its violation of the duty to implement and maintain reasonable security procedures and practices (*i.e.,* no causation—the breach resulted for some other reason), that notwithstanding the breach the business took reasonable security measures, or that the plaintiff is not entitled to seek statutory damages because the business cured the action in response to a 30 day CCPA notice letter (or no such letter was sent, or the letter sent was defective in failing to specifically identify the violation to be cured).

What constitutes a *reasonable* security measure is not defined in the statute. Hence, where the issue is legitimately contested, causation may raise factual questions that could be difficult to resolve through motion practice in some cases. The adequacy of any alleged cure may also raise factual questions in some cases.

Where liability and entitlement to statutory damages are established, a defendant may argue that damages should be awarded at the lower end of the statutory damage range, rather than the higher end, based on the nonexclusive list of criteria set forth in the statute (and any others a defendant wishes the trier of fact to consider).[12]

A person harmed by the data breach may who can establish liability under the CCPA may recover statutory damages in the range of $100 - $750 "per consumer per incident or actual damages," whichever is greater, injunctive or declaratory relief, and any other relief that a court deems proper.[13] In assessing the amount of statutory damages, the court shall consider "any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."[14] Nevertheless, a data breach impacting 100,000 consumers could

[12]*See* Cal. Civ. Code § 1798.150(a)(2).

[13]Cal. Civ. Code § 1798.150(a)(1).

[14]Cal. Civ. Code § 1798.150(a)(2).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

invite putative class action suits seeking up to $75,000,000, will almost always be seems disproportionate to the harm caused (if any). And a breach impacting 1,000,000 state residents could result in a putative class action suit seeking $750,000,000, where the plaintiffs, if successful, would be entitled to a minimum of recovery of *at least* $100,000,000. These calculations are not only wildly disproportionate to the harm experienced in most cases, but also are disproportionate when compared to the actual amounts paid by companies to settle nation-wide cybersecurity breach class action suits (as analyzed in section 27.07 in chapter 27).[15] Given the potential for large awards in putative class action suits, the private cause of action created by the CCPA has generated substantial litigation since claims could first be asserted in court, on January 1, 2020.

To seek an award of statutory damages under the CCPA, either individually or as a putative class action suit, a consumer must provide a business "30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated," and allow the business 30 days to cure the violations, "prior to initiating any action against a business for statutory damages on an individual or class-wide basis. . . ."[16] If within the 30 days the business actually cures the noticed violation (assuming a cure is possible) and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, then no action for individual statutory damages or class-wide statutory damages may be initiated against the business.[17]

This provision was modeled on the 30 day notice and cure period in the California Consumers Legal Remedies Act,[18] a statute popular with class action counsel. Under that stat-

---

[15]*See infra* § 27.07. Grossly disproportionate awards potentially could be challenged on Due Process grounds. *See, e.g.*, *Golan v. FreeEats.com, Inc.*, 930 F.3d 950, 962-63 (8th Cir. 2019) (ruling that $500 minimum statutory damage awards totaling $1.6 Billion (based on 3.2 million phone calls allegedly placed in the course of one week), under the Telephone Consumer Protection Act, violated Due Process).

[16]Cal. Civ. Code § 1798.150(b) (emphasis added).

[17]Cal. Civ. Code § 1798.150(b).

[18]Cal. Civ. Code § 1782; *Laster v. T-Mobile USA, Inc.*, 407 F. Supp. 2d 1181, 1196 (S.D. Cal. 2005) (dismissing plaintiff's claim with prejudice because of plaintiff's failure to provide notice to defendants pursuant to section 1782(a)); *see generally supra* § 25.04[3].

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

ute, some class action lawyers have become adept at framing claims for which a "cure" is impossible. It is unclear how, if at all, a breach which has occurred could be cured. Indeed, the statute acknowledges that possibility in framing requirements "[i]n the event a cure is possible . . . ."[19] Nevertheless, it is generally desirable for defense counsel to respond to valid CCPA 30 day notification letters—*i.e.,* those that identify "the specific provisions of this title the consumer alleges have been or are being violated . . . ." While a business should avoid undertaking an obligation in response to a CCPA 30-day notice letter that could itself form the basis of a CCPA claim for noncompliance (as discussed below), any legitimate effort to cure could prevent a claimant (or class of claimants) from recovering statutory damages, create a jury question over whether plaintiffs are even entitled to recover statutory damages, or justify an award at the lower end of the range for statutory damages.

Some class action lawyers, concerned about beating other plaintiffs' counsel to file first following a security incident, have initiated legal action before the expiration of the 30-day period and waited to serve the complaint until the expiration of the period. In such cases, statutory damages would be unavailable because the statute is clear that notice and a full 30 days to cure must occur "*prior* to initiating any action against a business for statutory damages on an individual or class-wide basis . . . ."[20]

The CCPA thus sets up a number of potential substantive and procedural hurdles that a plaintiff must surmount to recover statutory damages. At the outset of the case, a defendant may be able to obtain a ruling through motion practice that the plaintiff is not entitled to recover statutory damages because the plaintiff did not provide notice and an opportunity to cure, is not entitled to maintain a CCPA action at all because the plaintiff is not a California resident or the defendant or information are not subject to the CCPA (based on the definitions of a *business* and *personal information*), or may not proceed in court (either individually, or to seek class certification) because the claim is subject to arbitration, depending on the facts alleged by the plaintiff and evidence that may be subject to judicial notice or otherwise presented to the court. While a defendant may be

[19]Cal. Civ. Code § 1798.150(b).

[20]Cal. Civ. Code § 1798.150(b).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

able to win or narrow a claim through motion practice, a plaintiff may need to proceed to trial to prove its entitlement to recover under the CCPA, by showing that any security breach was caused by a defendant's failure to maintain reasonable practices, and to recover statutory damages (at least above the minimum $100 level[21]). Plaintiff's counsel also typically must be able to win a motion for class certification to make CCPA statutory damage claims worthwhile litigating in most instances. For all of these reasons, while many purported CCPA claims have been filed since January 1, 2020, few if any thus far have proceeded to judgment for the plaintiff. Most have been won (or moved to individual arbitration) by the defendants, settled, or await trial.

The CPRA largely retains section 1798.150 intact, but, effective January 1, 2023, section 1798.150 will also apply to businesses engaged in consumer credit collection and reporting.[22] It also will authorize legal action when a person's "email address in combination with a password or security question and answer that would permit access to the account"—and not just *personal information* as defined in sec-

---

[21]A plaintiff presumably could move for summary judgment if it could establish liability and sought only the minimum statutory award. Where a jury trial has been demanded, a defendant would be entitled to have the jury determine the amount of the award where any amount above the minimum was sought. *Cf. BMG Music v. Gonzalez,* 430 F.3d 888, 892 (7th Cir. 2005) (holding that the defendant did not have a right to a jury trial in a copyright infringement suit where the plaintiff sought and was awarded statutory damages at the lowest permissible level, on summary judgment), *cert. denied*, 547 U.S. 1130 (2006).

[22]The CPRA generally will not apply to "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency," as defined in 15 U.S.C.A. § 1681a(f), by a furnisher of information, as set forth in 15 U.S.C.A. § 1681s-2, "who provides information for use in a consumer report, as defined in" 15 U.S.C.A. § 1681a(d), and by a user of a consumer report as set forth in 15 U.S.C.A. § 1681b, but only to the extent this activity involves "the collection, maintenance, disclosure, sale, communication or use of such information by that agency, furnisher, or user . . . subject to regulation under the Fair Credit Reporting Act," 15 U.S.C.A. §§ 1681 *et seq*., "and the information is not collected, maintained, used, communicated, disclosed or sold except as authorized by the Fair Credit Reporting Act." *See* Cal. Civil Code § 1798.145(d) (effective Jan. 1, 2023). This exclusion, however, does not apply to the private cause of action for certain security breaches created by section 1798.150. *See id*. § 1798.145(d)(3) (effective Jan. 1, 2023).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

tion 1798.81.5(d)—has been subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.[23]

Effective January 1, 2023, the CPRA also will provide that the implementation and maintenance of reasonable security procedures and practices pursuant to Cal. Civil Code § 1798.81.5 following a breach may not be deemed a cure under the CPRA.[24] It also expands the data elements that could trigger a claim under the CPRA to include an email address in combination with a password or security question and answer that would permit access to the account.[25] Inferentially, prior to January 1, 2023, it may be possible to cure a CCPA 30 day claim by implementing and maintaining reasonable security procedures and practices pursuant to Cal. Civil Code § 1798.81.5.

The CPRA will, as of January 1, 2023, prohibit any waiver of "a representative action" waiver, including "any right to a remedy or means of enforcement . . . ."[26] This would render void any class action waiver in litigation. However, a stipulation for individual, not class-wide arbitration of CCPA claims that is part of a binding and enforceable arbitration provision subject to the Federal Arbitration Act should be enforceable based on binding U.S. Supreme Court precedent construing the Federal Arbitration Act and the Supremacy Clause of the U.S. Constitution[27] (although the issue of the validity of such a provision could be left to the arbitrator,

---

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

[24]Cal. Civil Code § 1798.150(b) (effective Jan. 1, 2023).

[25]Cal. Civil Code § 1798.150(a)(1) (effective Jan. 1, 2023).

[26]*See* Cal. Civil Code § 1798.192 (effective Jan. 1, 2023) ("Any provision of a contract or agreement of any kind, including a representative action waiver, that purports to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable.").

[27]*See Stolt-Nielsen S.A. v. AnimalFeeds Int'l Corp.*, 559 U.S. 662 (2010); *see also Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1415-19 (2019) (holding that ambiguity in an arbitration agreement does not provide sufficient grounds for compelling classwide arbitration); *Epic Systems Corp. v. Lewis*, 138 S. Ct. 1612, 1623 (2018) (explaining that "*Concepcion*'s essential insight remains: courts may not allow a contract defense to reshape traditional individualized arbitration by mandating classwide arbitration procedures without the parties' consent."); *see generally supra*

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

and not a court, if the arbitration provision includes a delegation clause and this issue is not carved out from the delegation provision[28]). Arbitration issues in connection with consumer data privacy and cybersecurity claims are analyzed more extensively in section 22.05[2][M] in chapter 22.

It remains to be seen whether the Attorney General will promulgate regulations under the CPRA to provide more detailed guidance on the type of "cure" that would meet the requirement of the statute (such as measures to mitigate the consequences of a breach and minimize the risk of similar future breaches) beyond the new statutory limitation on cure attempts made pursuant to Cal. Civil Code § 1798.81.5, or whether the issue will be fleshed out in litigation. Given the size of potential statutory damage awards and the ambiguity surrounding what constitutes *reasonable security,* a merely symbolic right to cure would be of little benefit to businesses.

If a business is able to cure and provides an express written statement to a consumer, but operates in breach of the express written statement, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the CCPA that postdates the written statement.[29]

No notice, however, is required for an individual consumer to initiate an action solely for actual pecuniary damages suffered as a result of an alleged violation.[30]

Significantly, the cause of action established by section 1798.150 applies "only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law."[31] A violation of the CCPA therefore could *not* form the basis for a claim under California's notorious unfair competition law, California Business & Professions Code section

---

§ 22.05[2][M].

[28]*See, e.g.*, *Lamps Plus, Inc. v. Varela*, 139 S. Ct. 1407, 1415-19 (2019) (holding that ambiguity in an arbitration agreement does not provide sufficient grounds for compelling classwide arbitration, which is only permissible when expressly agreed upon); *see generally supra* § 22.05[2][M] (analyzing the issue in depth).

[29]Cal. Civ. Code § 1798.150(b).

[30]Cal. Civ. Code § 1798.150(b).

[31]Cal. Civ. Code § 1798.150(c).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

17200,[32] which typically affords a cause of action for violation of other statutes, laws or regulations.[33] The private enforcement right created by the CCPA is actually quite narrow (and will remain so even when the CPRA takes effect). Nevertheless, the potential availability of statutory damages means that section 1798.150 will ontinue to be heavily litigated by class action counsel seeking a generous settlement or award on behalf of a putative class of those whose information was exposed in a security breach. Further, the ambiguous nature of the standard of care—to "implement and maintain reasonable security procedures and practices"—means that regardless of culpability, any time a business experiences a security breach that exposes the information of California residents, class action counsel will have an incentive to file suit.

While section 1798.150 insulates companies from private causes of action for violations of the CCPA other than for security breaches, this protection would not apply to claims brought by residents of other states against companies that adopt the CCPA across the board, and not merely for personal information from California residents. Businesses therefore should weigh the pros and cons of implementing the CCPA narrowly, only for California residents, or more broadly. While a broad application may make sense for some companies from an operational perspective or for customer relations, it also potentially could expose a company to greater liability from residents of states other than California, whose laws would not provide any safe harbor from litigation for undertaking, but failing to adhere to, any of the provisions of the CCPA. Although a claim by a resident of another state could not be premised on a violation of the

---

[32]*See, e.g.*, *Silver v. Stripe, Inc.*, Case No. 4:20-cv-08196-YGR, 2021 WL 3191752, at *7 (N.D. Cal. July 28, 2021) (dismissing plaintiffs' California unfair competition claim to the extent based on an alleged violation of the CCPA).

[33]*See, e.g.*, Cal. Bus. & Prof. §§ 17200 *et seq.* Section 17200 "borrows" violations from other laws by making them independently actionable as unfair competitive claims. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143–45, 131 Cal. Rptr. 2d 29 (Cal. 2003). 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.' " *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1151–52 (9th Cir. 2008) (citations omitted); *see generally supra* § 25.04[3].

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

CCPA *per se,* the failure of a business to adhere to its stated practices or procedures potentially could be actionable under theories of express or implied contract or unfair competition.[34]

The CCPA also leaves in place an array of other California privacy laws, which could form the basis for litigation against a business—even if noncompliance with the CCPA (other than a security breach within the terms of section 1798.150) is not be actionable in a private lawsuit.[35] Section 1798.150 precludes other claims premised on CCPA violations, but does not preclude claims based on other theories of law. For example, regardless of whether a business is subject to the CCPA, if it has an online presence, it must nonetheless post a privacy policy that complies with Cal-OPPA, Cal. Bus. & Prof. Code §§ 22575, *et seq*. Presumably the requirement that a business disclose "personally identifiable information" that it collects under Cal-OPPA would overlap with a business's disclosure requirements under the CCPA, given the extremely broad definition of *personal information* in section 1798.140(h) of the CCPA.[36] Indeed, Cal-OPPA mandates additional disclosure requirements in an online privacy policy that do not completely coincide with the CCPA, such as allowing consumers to "request changes to any personally identifiable information collected," if a business provides that option, how a business responds to "do not track" signals, and whether use of the website might allow third-parties to collect additional information, for example, through the use of cookies.[37] Unlike the CCPA, Cal-OPPA provides a private right of action[38] and potentially could support a claim for a violation of California's unfair competition statute, Cal. Bus. & Prof. Code § 17200.[39]

Similarly, businesses (including even small businesses not subject to the CCPA, if they have at least 20 employees) are still required to disclose if their personal information is shared with others for direct marketing, and if so allow

---

[34]*See generally infra* §§ 26.14, 26.15.

[35]*See generally supra* § 26.13[6].

[36]*See* Cal. Bus. & Prof. Code § 22577(a); *supra* § 26.13[6][B].

[37]*See* Cal. Bus. & Prof. Code § 22575(b).

[38]*See* Cal. Bus. & Prof. Code § 22576.

[39]*See Svenson v. Google Inc.*, Case No. 13-cv-04080-BLF, 2015 WL 1503429, at *8-10 (N.D. Cal. Apr. 1, 2015); *see generally supra* § 26.13[6].

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

customers to opt out, pursuant to the "Shine the Light" Law.[40] Disclosures under the Shine the Light Law must be, in at least some ways, more fulsome than pursuant to the CCPA because the law requires businesses to disclose the "names and addresses" of third parties that have received a customer's personal information, and "examples of the products or services marketed" to customers, "if known," "sufficient to give the customer a reasonable indication of the nature of the third parties' business."[41] Further, a business is afforded less time—only 30 days—to comply with a disclosure request under the Shine the Light Law[42] than under the CCPA. The Shine the Light Law, unlike the CCPA, provides a private right of action for customers injured by a violation (although injury in most cases may be difficult to prove).[43]

Data breach claims under the CCPA potentially may be joined by other causes of action in litigation. California law predating the CCPA provides that any customer injured by a violation of its security breach notification statute may institute a civil action to recover damages[44] or injunctive relief,[45] in addition to any other remedies that may be available.[46] Among other things, the breach of the notification statute itself could be actionable as an unfair trade practice under California law if damages can be shown.[47] Absent any injury traceable to a company's failure to reasonably notify customers of a data breach, however, a plaintiff may not have standing to bring suit for a defendant's alleged failure to maintain reasonable security measures, at least in federal court.[48] CCPA and other California law claims, of course, could be brought in California state courts.

---

[40]*See* Cal. Civ. Code § 1798.83; *supra* § 26.13[6][D].

[41]Cal. Civ. Code § 1798.83(b)(3).

[42]Cal. Civ. Code § 1798.83(b)(1)(C).

[43]*See* Cal. Civ. Code § 1798.84; *see generally supra* § 26.13[6][D].

[44]Cal. Civil Code § 1798.84(b).

[45]Cal. Civil Code § 1798.84(e).

[46]Cal. Civil Code § 1798.84(g).

[47]*See* Cal. Bus. & Prof. Code §§ 17200 *et seq.*; *see generally supra* §§ 27.01, 27.04[6] (discussing how the breach of an unrelated statute may be actionable under § 17200).

[48]*See, e.g.*, *Rahman v. Marriott International, Inc.*, Case No. SA CV 20-00654-DOC-KES, 2021 WL 346421 (C.D. Cal. Jan. 12, 2021) (dismissing plaintiff's complaint under the CCPA and for breach of contract, breach of implied contract, unjust enrichment and unfair competition, for lack of Article III standing, in a suit arising out of Russian employees accessing

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

As analyzed more extensively in other sections of this treatise,[49] other claims typically joined in security breach and data privacy litigation include claims for breach of contract (if there is a contract, or if a privacy policy is incorporated by reference in a user agreement and allegedly breached), breach of the covenant of good faith and fair dealing (if the claim isn't directly prohibited by the contract), breach of implied contract (if there is no express contract), breach of fiduciary duty, negligence, fraud, and claims under other states' cybersecurity laws.[50]

The cause of action created by the CCPA, by providing a remedy of statutory damages, has increased the number of California putative class action suits brought following a security breach. Given the liberal standing requirements for security breach cases in the Ninth Circuit,[51] many of these claims have been brought in federal court, although suits by California residents against California companies need to be

---

putative class members' names, addresses, and other publicly available information, because the sensitivity of personal information, combined with its theft, are prerequisites to finding that a plaintiff adequately alleged injury in fact); *see also, e.g.*, *Cahen v. Toyota Motor Corp.,* 717 F. App'x 720 (9th Cir. 2017) (affirming the lower court's ruling finding no standing to assert claims that car manufacturers equipped their vehicles with software that was susceptible to being hacked by third parties); *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); *see generally infra* § 27.07 (analyzing claims raised in security breach litigation).

[49]*See supra* § 27.07 (cybersecurity breach putative class action litigation); *infra* § 26.15 (data privacy putative class action litigation).

[50]*See generally infra* §§ 26.15 (data privacy litigation), 27.04[6] (state data security laws), 27.07 (cybersecurity breach litigation), 27.08[10] (remedies under state and U.S. territorial security breach notification statutes).

[51]*See, e.g., In re Zappos.com, Inc.,* 888 F.3d 1020, 1023-30 (9th Cir. 2018) (holding that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court), *cert. denied*, 139 S. Ct. 1373 (2019); *see generally infra* § 27.07 (comparing the relatively liberal standing requirements for security breach cases in the Ninth Circuit to case law from other circuits).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

brought in state court, because of the lack of diversity jurisdiction, unless plaintiffs are able to also sue for violations of federal statutes or allege jurisdiction under the Class Action Fairness Act (CAFA),[52] for putative class action suits. Indeed, CCPA claims have been brought in federal court in other states as well.

To minimize the risk of class action litigation arising under the CCPA, businesses should enter into binding contracts with consumers that contain enforceable arbitration provisions governed by the Federal Arbitration Act (which preempts state law), including a delegation clause to maximize its potential enforceability.[53] Crafting a binding and enforceable arbitration provision is addressed in section 22.05[2][M] in chapter 22, which also includes a sample form. Ensuring that contract formation for online and mobile agreements conforms to the law in those jurisdictions most hostile to electronic contracting is analyzed extensively in section 21.03 in chapter 21. Where a business does not have privity of contract with consumers but could be sued for violating the CCPA, it should seek to become an intended beneficiary of the arbitration clauses in effect between its business partners and consumers who could file suit, if it is possible to do so.[54] It should also ensure that its partners' arbitration provisions and processes for online and mobile contract formation conform to best practices. Businesses also may wish to explore whether they have adequate insurance coverage (and the right to select counsel).

Beyond class action litigation, the CCPA's requirement for contractual undertakings and obligations by service providers and third parties (or contractors, under the CPRA) leaves open the possibility for litigation between or among *businesses*, *service providers* and *third parties*, as those terms

---

[52]28 U.S.C.A. § 1332(d); *see generally infra* § 26.15 (discussing CAFA jurisdiction in connection with data privacy litigation).

[53]*See, e.g., Henry Schein, Inc. v. Archer & White Sales, Inc.*, 139 S. Ct. 524, 529 (2019) (holding that "[w]hen the parties' contract delegates the arbitrability question to an arbitrator, a court may not override the contract" and "possesses no power to decide the arbitrability issue . . . even if the court thinks that the argument that the arbitration agreement applies to a particular dispute is wholly groundless"); *Rent-A-Center, West v. Jackson*, 561 U.S. 63 (2010); *see generally supra* § 22.05[2][M].

[54]*See supra* §§ 22.05[2][P] (analyzing third-party beneficiaries in Terms of Use agreements), 22.05[2][M][vi] (drafting tips for consumer arbitration provisions).

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

are defined under the statute. To anticipate potential claims, entities should pay close attention to indemnification provisions in these contracts (including potential indemnification for litigation and administrative enforcement actions brought by the California Attorney General or, on or after July 1, 2023, by the California Privacy Protection Agency, pursuant to the CPRA).

It is possible that, at some point, Congress may act to preempt the CCPA prior to the time the CPRA is scheduled to enter into force on January 1, 2023.

The CCPA also may be challenged, to the extent it regulates interstate commerce, under the dormant Commerce Clause, although the drafters of the CCPA were careful to provide that the collection or sale of information that takes place "wholly outside of California," is not subject to the CCPA.[55] Dormant Commerce Clause arguments thus far have been rebuffed in lower court challenges to various state privacy laws[56]—albeit ones substantially less burdensome or expensive for out-of-state companies to comply with. The

---

[55]*See* Cal. Civ. Code § 1798.145(a)(6). A state law that regulates wholly out-of-state conduct may be struck down under the dormant Commerce Clause. *See, e.g., Publius v. Boyer-Vine,* 237 F. Supp. 3d 997 (E.D. Cal. 2017) (holding that a California law that purported to prohibit a Massachusetts blogger from compiling and posting the names, home addresses, and phone numbers, of members of the California legislature who voted in favor of gun control measures, likely violated the dormant Commerce Clause).

[56]*See, e.g., Ades v. Omni Hotels Management Corp.*, 46 F. Supp. 3d 999 (C.D. Cal. 2014) (holding that the California Invasion of Privacy Act regulated only calls with a nexus to the state and had the purpose of preventing privacy harms to Californians. Accordingly, it did not merit strict scrutiny under the dormant Commerce Clause, even though it might create incentives for parties to alter their nationwide behavior because those effects were deemed incidental); *see also, e.g., In re Facebook Biometric Information Privacy Litig.*, Case No. 3:15-cv-0373-JD, 2018 WL 2197546, at *4 (N.D. Cal. May 14, 2018) (denying summary judgment based on the argument that subjecting the defendant to liability under the Illinois Biometric Information Privacy Act for processing facial recognition data on servers located exclusively outside of Illinois violated the dormant Commerce Clause, because liability under the statute would not force the defendant "to change its practices with respect to residents of other states."); *Monroy v. Shutterfly, Inc.,* Case No. 16 C 10984, 2017 WL 4099846, at *7-8 (N.D. Ill. Sept. 15, 2017) (denying defendant's motion to dismiss plaintiff's suit under the dormant Commerce Clause; "Monroy's suit, as well as his proposed class, is confined to individuals whose biometric data was obtained from photographs uploaded to Shutterfly in Illinois. Applying BIPA in this case would not entail any regulation of

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

cost of compliance—estimated by the California Attorney General to be up to $55 Billion initially, with ongoing compliance costs from 2020 to 2030 estimated to range from $467 million to more than $16 billion[57]—suggests there potentially could be merit to an argument that the CCPA burdens interstate commerce. Dormant Commerce Clause case law is analyzed in section 35.04 in chapter 35.

Putative data privacy class action litigation is analyzed in section 26.15. Putative data breach class action litigation is analyzed in section 27.07.

26.13A[15] Non-waiver

The CCPA provides that any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under the statute, including, but not limited to any right to a remedy or means of enforcement, "shall be deemed contrary to public policy and shall be void and unenforceable."[1] Effective January 1, 2023, the CPRA will add to this section a prohibition on "a representative action waiver . . . ."[2]

This provision "shall not prevent a consumer from declining to request information from a business, declining to opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out."[3]

Shutterfly's gathering and storage of biometric data obtained outside of Illinois. It is true that the statute requires Shutterfly to comply with certain regulations if it wishes to operate in Illinois. But that is very different from controlling Shutterfly's conduct in other states."); *see generally infra* §§ 35.01 *et seq.* (analyzing the application of the dormant Commerce Clause to internet statutes).

[57]*See* California Department of Justice—Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), http://www.dof.ca.gov/Forecasting/Economics/Major__Regulations/Major__Regulations__Table/documents/CCPA__Regulations-SRIA-DOF.pdf

[Section 26.13A[15]]

[1]Cal. Civ. Code § 1798.192.

[2]Cal. Civ. Code § 1798.192 (effective Jan. 1, 2023).

[3]Cal. Civ. Code § 1798.192.

PAGE PROOFS - SUBJECT TO REVISION
© 2023 Ian C. Ballon, www.IanBallon.net

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

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

Chapter 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

Chapter 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

Chapter 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

Part IV. Privacy, Security and Internet Advertising

25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

Chapter 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

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

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

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

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

Part VIII. Theft of Digital Information and Related Internet Crimes

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

Volume 5

Chapter 46. Identity Theft
47. Civil Remedies for Unlawful Seizures

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

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

Part X. Civil Jurisdiction and Litigation

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

"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)

SAVE 20% NOW!! To order call 1-888-728-7677
or visit lanBallon.net
enter promo code WPD20 at checkout

List Price: $3,337.00
Discounted Price: $2,669.60