CCPA LITIGATION

Excerpted from Chapter 26 (Data Privacy) from the April 2020 updates to
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)

INTERNET, MOBILE AND DIGITAL LAW YEAR IN REVIEW: WHAT YOU NEED TO KNOW FOR 2021 AND BEYOND

ASSOCIATION OF CORPORATE COUNSEL

JANUARY 14, 2021

Ian C. Ballon
Greenberg Traurig, LLP

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

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

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West April 2020 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
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, Twitter, Facebook: IanBallon

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

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

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents companies in intellectual property litigation (including copyright, trademark, trade secret, patent, right of publicity, DMCA, domain name, platform defense, fair use, CDA and database/screen scraping) and in the defense of data privacy, cybersecurity breach and TCPA class action suits.

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, including a novel transactional approach to handling security breaches and exhaustive treatment of trends in data privacy, security breach and TCPA class action suits. 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 is a member of the consultative group for the Data Privacy Principles of Law project (ALI Principles of Law Tentative Draft 2019).

Ian was named the Lawyer of the Year for Information Technology Law in the 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America and was recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 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 is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He 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 2020). Ian 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.

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

on how to comply with the CCPA.[148]

The law also authorizes the Attorney General to bring a civil action against businesses, service providers, or any other person that violates the CCPA.[149] A business "shall be in violation" if it "fails to cure any alleged violation within 30 days after being notified of noncompliance."[150] The Attorney General may seek injunctive relief and a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation.[151] While the penalties *per violation* are small, it remains to be seen how the Attorney General will construe the term *violation* in regulatory enforcement actions. Whether a violation is defined in terms of an incident or a single act or omission, for example, or the number of people impacted, will be significant.

Revenue from litigation will be allocated to a Consumer Privacy Fund, which may be used exclusively to offset costs incurred by state courts and the California Attorney General in connection with the CCPA.[152] This creates a potential conflict of interest, in that unless the legislature allocates funds expressly for all the new work to be done under the statute, there will be added pressure on the Attorney General's Office to pursue litigation—and to recover penalties in litigation.

Private right of action for data breaches

The CCPA creates 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 . . . ."[153] The private right of action created by the CCPA may be brought only for data

---

[148]Cal. Civ. Code § 1798.155(a).

[149]Cal. Civ. Code § 1798.155(b).

[150]Cal. Civ. Code § 1798.155(a).

[151]Cal. Civ. Code § 1798.155(b).

[152]Cal. Civ. Code § 1798.160.

[153]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:

breaches arising from a business's failure to maintain reasonable security measures, and not any other failures to comply with the CCPA.[154] What constitutes a *reasonable* security measure is not defined in the statute. Hence, any time a California business suffers a security breach, it may be sued in a lawsuit where plaintiffs will challenge both the security measures adopted and a business's adherence to those measures. In such cases, where the issue is legitimately contested, causation may raise factual questions that could make a case difficult to resolve on motion practice.

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

(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).

[154]Cal. Civ. Code § 1798.150(c).

A person harmed by the data breach may bring an action to 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.[155] 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."[156] Nevertheless, a data breach impacting 100,000 consumers could invite putative class action suits seeking up to $75,000,000, which seems disproportionate. 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 at least $100,000,000. These calculations are wildly disproportionate to the harm experienced in most cases. They 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).[157] Given the potential for large awards in putative class action suits, the private cause of action created by the CCPA is likely to generate substantial litigation.

To bring a claim for statutory damages, 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. 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

---

[155]Cal. Civ. Code § 1798.150(a)(1).

[156]Cal. Civ. Code § 1798.150(a)(2).

[157]*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).

or class-wide statutory damages may be initiated against the business.[158]

This provision tracks the 30 day notice and cure period in the California Consumer Legal Remedies Act,[159] a statute popular with class action counsel. Under that statute, 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 . . . ."[160] It remains to be seen whether the Attorney General will promulgate regulations to elaborate on the type of "cure" that would meet this requirement of the statute (such as measures to mitigate the consequences of a breach and minimize the risk of similar future breaches) 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.[161]

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.[162]

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

---

[158]Cal. Civ. Code § 1798.150(b).

[159]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].

[160]Cal. Civ. Code § 1798.150(b).

[161]Cal. Civ. Code § 1798.150(b).

[162]Cal. Civ. Code § 1798.150(b).

law."[163] What this means is that a violation of the statute could *not* form the basis for a claim under California's notorious section 17200, which typically affords a cause of action for violation of other statutes, laws or regulations.[164] The private enforcement right created by the CCPA thus is actually quite narrow. Nevertheless, the potential availability of statutory damages means that it will 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 need to 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. Although a claim by a resident of another state could not be premised on a violation of the CCPA *per se,* the failure of a business to adhere to its stated practices or procedures potentially could be actionable under theories of

---

[163]Cal. Civ. Code § 1798.150(c).

[164]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].

express or implied contract or unfair competition.[165]

The CCPA also leaves in place an array of other California privacy laws, which could form the basis for litigation against a business on grounds other than a security breach—even if noncompliance with the CCPA itself would not be actionable in a private lawsuit.[166] 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.[167] 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.[168] Unlike the CCPA, Cal-OPPA provides a private right of action[169] and potentially could support a claim for a violation of California's unfair competition statute, Cal. Bus. & Prof. Code § 17200.[170]

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 customers to opt out, pursuant to the "Shine the Light" Law.[171] Disclosures under the Shine the Light Law must be, in at least some ways, more fulsome than pursuant to the

---

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

[166]*See generally supra* § 26.13[6].

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

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

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

[170]*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].

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

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."[172] Further, a business is afforded less time—only 30 days—to comply with a disclosure request under the Shine the Light Law[173] 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).[174]

Security 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[175] or injunctive relief,[176] in addition to any other remedies that may be available.[177] 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.[178] 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.[179] CCPA and other California law claims, of course, could be brought in California state courts.

---

[172]Cal. Civ. Code § 1798.83(b)(3).

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

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

[175]Cal. Civil Code § 1798.84(b).

[176]Cal. Civil Code § 1798.84(e).

[177]Cal. Civil Code § 1798.84(g).

[178]*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).

[179]*See, 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 informa-

Other claims typically joined in security breach and 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.[180]

The cause of action created by the CCPA, by providing a remedy of statutory damages, will likely increase 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,[181] some of these claims will be brought in federal court, although suits by California residents against California companies likely would need to be brought in state court, because of the lack of diversity jurisdiction, unless plaintiffs are able to also sue for violations of federal statutes.

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.[182] Crafting a binding and enforceable arbitration provision is addressed in section

---

tion 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).

[180]*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).

[181]*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); *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).

[182]*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

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. 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 means it is also likely that the CCPA will result in litigation between or among *businesses*, *service providers* and *third parties*, as those terms 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 regulatory enforcement actions brought by the California Attorney General).

It is possible that, at some point, Congress may act to preempt the CCPA. The statute 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.[183] Dormant Commerce Clause arguments thus far have been rebuffed in lower court chal-

---

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].

[183]*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).

lenges to various state privacy laws[184]—albeit ones substantially less burdensome or expensive for out-of-state companies to comply with. The 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[185]—suggests there potentially could be merit to an argument that the CCPA burdens interstate commerce. Dormant Commerce Clause case law is analyzed in chapter 35.

Data privacy class action litigation is analyzed in section 26.15. Security breach class action suits are analyzed in section 27.07.

---

[184]*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 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).

[185]*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

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2020

Ian C. Ballon

APRIL 2020 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

- Antitrust in the era of techlash
- The California Consumer Privacy Act, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- Artificial intelligence & machine learning
- Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- TCPA law and litigation - 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
- 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
- AI, screen scraping and database protection
- Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- IP issues including Copyright and Lanham Act fair use, 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, 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 and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property 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 (2009-2020), 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 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also serves as Executive Director of Stanford University Law School's Center for 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).

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

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

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

NEW AND IMPORTANT FEATURES FOR 2020

- **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)
- The **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- **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)
- Making sense of the Circuit Split under the **TCPA (3d, 7th and 11th vs. 2d and 9th)** & other significant new case law (ch. 29)
- Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- Copyright, patent, ADA and other **troll litigation – and ways to combat it** (ch. 4, 8, 48)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- **Screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- **State online dating and revenge porn laws** (chapter 51)
- **Expanding and contracting anti-SLAPP case law** construing different state laws (ch 37)
- **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- **eSIGN case law** (chapter 15)
- **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)
- **Defending cybersecurity and data privacy class action suits -** case law, trends and strategy (chapters 25, 26, 27)
- **The Music Modernization Act's Impact on copyright preemption, the CDA, and DMCA protection for pre-1972 musical works** (ch 4, 37, 49)
- **Cybersafety standards and best practices for youth audiences in social media, apps, games & networks** (by Parry Aftab) (ch. 51)
- 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)
- **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)
- **Music licensing** (updated by Tucker McCrady) (chapter 17)
- **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)
- **Idea protection & misappropriation** (ch 13)
- Revisiting **links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)