CALIFORNIA'S IOT LAW ON THE SECURITY OF CONNECTED DEVICES

Excerpted from Chapter 27 (Cybersecurity: Information, Network and Data Security)
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)

STRATEGIES FOR DEFENDING CCPA AND OTHER CYBERSECURITY CLASS ACTION LITIGATION

9TH ANNUAL BCLT PRIVACY LAW FORUM
BERKELEY CENTER FOR LAW & TECHNOLOGY
OCTOBER 9, 2020

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

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. A list of selected recent cases may be found here.

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

who is authorized to sue for civil penalties.[12]

The Act also broadened the scope of New York's security breach notification statute, which is separately analyzed in section 27.08.

A copy of the SHIELD Act is set forth in section 27.09[35]. Guidance on how to conduct a risk assessment and draft a written information security program is set forth in section 27.13.

27.04[6][L] California's IoT Law on the Security of Connected Devices

California's IoT data security law,[1] Cal. Civil Code §§ 1798.91.04 to 1798.91.06, which took effect on January 1, 2020, requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device, and any information it contains, from unauthorized access, destruction, use, modification, or disclosure. Specifically, the law requires that a manufacturer[2] of a connected device[3] equip the device with a reasonable security feature[4] or features that are all of the following:

(1) Appropriate to the nature and function of the device.

---

[12]N.Y. Gen. Bus. Law, § 899-bb(2)(d).

[Section 27.04[6][L]]

[1]The Internet of Things (IoT) is a broad term used to refer to connected devices—such as smart refrigerators, smart televisions, wearable exercise monitors, self-driving cars, home security systems, and home or office climate control systems, among other things—that collect, store, or transfer information to other devices and networked computers, including personal data. *See generally supra* § 27.03B (explaining IoT).

[2]*Manufacturer* means "the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California. For the purposes of this subdivision, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device." Cal. Civil Code § 1798.91.05(c).

[3]*Connected device* means "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address." Cal. Civil Code § 1798.91.05(b).

[4]A *security feature* is "a feature of a device designed to provide security for that device." Cal. Civil Code § 1798.91.05(d).

    (2) Appropriate to the information it may collect, contain, or transmit.

    (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.[5]

Subject to these requirements, if a connected device is equipped with a means for authentication[6] outside a local area network, it will be deemed a *reasonable security feature* under the statute if either:

    (1) The preprogrammed password is unique to each device manufactured; or

    (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.[7]

The statute also includes four express exclusions. It may not be construed "to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device."[8]

It may not be construed "to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance . . ." with the statute.[9]

It may not be construed "to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user's discretion."[10]

And it may not be applied "to any connected device the functionality of which is subject to security requirements

---

[5]Cal. Civil Code § 1798.91.04(a). *Unauthorized access, destruction, use, modification, or disclosure* means "access, destruction, use, modification, or disclosure that is not authorized by the consumer." *Id.* § 1798.91.05(e).

[6]*Authentication* means "a method of verifying the authority of a user, process, or device to access resources in an information system." Cal. Civil Code § 1798.91.05(a).

[7]Cal. Civil Code § 1798.91.04(b).

[8]Cal. Civil Code § 1798.91.06(a).

[9]Cal. Civil Code § 1798.91.06(b).

[10]Cal. Civil Code § 1798.91.06(c).

under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority."[11]

California's IoT security law, which was the first U.S. statute to specifically address the security of information shared by connected devices, has been either applauded by security experts for taking a step in the right direction or criticized for focusing on adding "good" features instead of removing bad ones that subject devices to attacks.[12] It seems likely that other states or the federal government will seek to enact IoT regulations in the coming years.

27.04[6][M] Insurance Industry Data Security Laws

An increasing number of states—including **Alabama,**[1] **Connecticut** (effective October 1, 2020),[2] **Delaware,**[3] **Michigan** (effective January 20, 2020 and January 20, 2021),[4] **Mississippi,**[5] **New Hampshire,**[6] **Ohio,**[7] and **South Carolina**[8]—have enacted variations of the National Association of

---

[11]Cal. Civil Code § 1798.91.06(d).

[12]*See* Adi Robertson, *California just became the first state with an Internet of Things cybersecurity law*, The Verge, Sept. 28, 2018 (quoting Robert Graham); Edward Kovacs, *California IoT Cybersecurity Bill Signed into Law*, SecurityWeek, Oct. 1, 2018 (quoting Graham as stating that the law "will do little [to] improve security, while doing a lot to impose costs and harm innovation.").

[Section 27.04[6][M]]

[1]Ala. Code §§ 27-62-1 to 27-62-12; *infra* § 27.09[2] (setting forth the statute).

[2]Connecticut's Insurance Data Security Law, which is based on the National Association of Insurance Commissioners' Model Insurance Data Security Law, takes effect on October 1, 2020, and replaces Conn. Gen. Stat. Ann. § 38a-999b. The statute is set forth in section 27.09[8][B].

[3]Del. Code Ann. tit. 18, §§ 8601 to 8611; *infra* § 27.09[9] (setting forth the statute).

[4]Mich. Comp. Laws Ann. §§ 500.550 to 500.565 (effective January 20, 2021); *infra* § 27.09[25][B] (setting forth the provisions).

[5]Miss. Code Ann. §§ 83-5-801 to 83-5-825; *infra* § 27.09[27] (setting forth the statute).

[6]N.H. Rev. Stat. Ann. §§ 420–P:1 to 420–P:14; *infra* § 27.09[32] (setting forth the statute).

[7]*See* Ohio Rev. Code Ann. §§ 3965.01 to 3965.11; *infra* § 27.09[38][B] (setting forth the statute).

[8]*See* S.C. Code Ann. §§ 38-99-30 to 38-99-100; *infra* § 27.09[44] (set-

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!

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

"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

SUMMARY OF CONTENTS

****

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)