

CALIFORNIA'S IOT LAW ON THE SECURITY OF CONNECTED DEVICES

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

2019 MIDWEST INTELLECTUAL PROPERTY INSTITUTE
MINNEAPOLIS
SEPTEMBER 26 & 27, 2019

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 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, LL.M., 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
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 internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits. A list of recent cases may be found at <http://www.gtlaw.com/Ian-C-Ballon-experience>.

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), which includes extensive coverage of intellectual property law issues. In addition, he serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact.

Ian was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America. In both 2018 and 2019 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. 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

(<http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx>).

Mr. Ballon was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and 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 2019), and has been listed as a Northern California Super Lawyer every year from 2004 through 2018 and as one of the top 100 lawyers in California. He is also 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. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

Covered Entity’s cybersecurity program” must be made available to the superintendent upon request.⁴³

A full set of the regulations 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 takes effect on January 1, 2020, will require 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 as of January 1, 2020, a manufacturer² of

applicable and based on its Risk Assessment:

- (1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and
- (2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

Id. The regulation also requires retention of records for three or five years, depending on the record. *See id.* § 500.06(b).

⁴³N.Y. Comp. Codes R. & Regs. tit. 23, § 500.02(d).

[Section 27.04[6][L]]

¹The 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).

a connected device³ equip the device with a reasonable security feature⁴ or features that are all of the following:

- (1) Appropriate to the nature and function of the device.
- (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 authentication⁶ 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

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).

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

⁵Cal. 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).

⁷Cal. Civil Code § 1798.91.04(b).

⁸Cal. Civil Code § 1798.91.06(a).

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 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.

27.05 The Payment Card Industry (PCI) Security Standard and Related State Laws

The Payment Card Industry Security Standards Council (PCI SSC) adopted the PCI Data Security Standard (PCI DDS) as a uniform set of security guidelines for major credit card companies, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International.¹ Any business processing, storing or transmitting payment card data must be PCI DSS compliant or risk being audited and fined and even losing the right to process credit card payments. Indeed, in 2006, Visa alone levied \$4.6 million in fines against businesses

⁹Cal. Civil Code § 1798.91.06(b).

¹⁰Cal. Civil Code § 1798.91.06(c).

¹¹Cal. Civil Code § 1798.91.06(d).

¹²See 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 27.05]

¹<https://www.pcisecuritystandards.org/>.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

Ian C. Ballon

**NEW AND
IMPORTANT
FEATURES
FOR 2019
NOT FOUND
ELSEWHERE**

**THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR – NOW A
5 VOLUME SET!**



To order call **1-888-728-7677**
or visit **legalsolutions.thomsonreuters.com**

Key Features of E-Commerce & Internet Law

- ◆ The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- ◆ Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- ◆ The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- ◆ Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- ◆ Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- ◆ Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- ◆ AI, screen scraping and database protection
- ◆ Strategies for defending cybersecurity breach and data privacy class action suits
- ◆ Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right 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 icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ How to enforce judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by 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
- ◆ 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/ 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
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

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. Database Protection, Screen Scraping 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 Protection and Misappropriation

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
 15. Drafting Agreements in Light of Model and Uniform Contract Laws: UCITA, the UETA, Federal Legislation and the EU Distance Sales Directive
 16. Internet Licenses: 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. Taxation of Electronic Commerce
 34. Antitrust Restrictions on Technology Companies and Electronic Commerce
 35. State and Local Regulation of the Internet
 36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

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

37. Defamation, Torts and the Good Samaritan Exemption (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. The Liability of Platforms (including Website Owners, App Providers, eCommerce Vendors, Cloud Storage and Other Internet and Mobile Service Providers) for User Generated Content and Misconduct
 50. Cloud, Mobile and Internet Service Provider Liability and 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 based 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 matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.



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 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 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 named as the Lawyer of the Year for information technology law in the 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 E-Commerce in Palo Alto.

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, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

NEW AND IMPORTANT FEATURES FOR 2019

- > A comprehensive analysis of 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)
- > An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- > The **CLOUD Act** (chapter 50)
- > Understanding **the TCPA after ACA Int'l** and significant new cases & circuit splits (chapter 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)
- > **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- > Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- > The complex array of potential liability risks from, and remedies for, **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)
- > **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- > Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- > **Website and mobile accessibility** (chapter 48)
- > **The Music Modernization Act's Impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- > **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- > Cutting through the jargon to make sense of **clickwrap, browsewrap, scrollwrap and sign-in wrap agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- > The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- > **Click fraud** (chapter 28)
- > 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)
- > **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 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)

SAVE 20% NOW!!

To order call **1-888-728-7677**
or visit legalsolutions.thomsonreuters.com,
enter promo code **WPD20** at checkout

List Price: \$2,567.50
Discounted Price: \$2,054