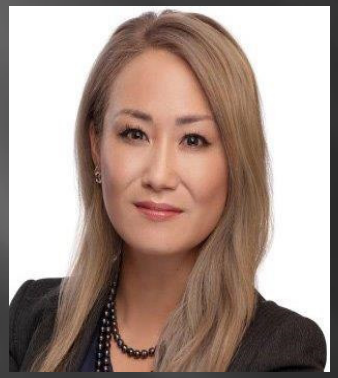
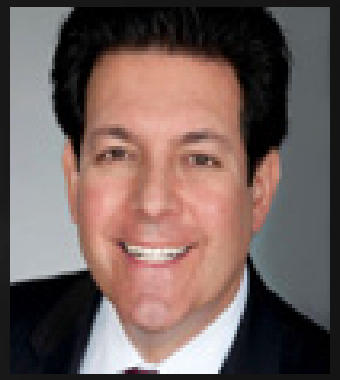
CCPA AND OTHER CYBERSECURITY LITIGATION



Mia Chiu
Vice President and General Counsel
Rakuten Rewards
mia.chiu@rakuten.com



Ian Ballon, JD, LLM, CIPP/US
Co-Chair, Global IP & Technology Practice Group
Greenberg Traurig LLP
(650) 289-7881 (310) 586-6575
Ballon@GTLaw.com
Facebook, Twitter, LinkedIn: Ian Ballon
www.IanBallon.net


E-Commerce
& Internet Law
Ian C. Ballon

http://www.ianballon.net/

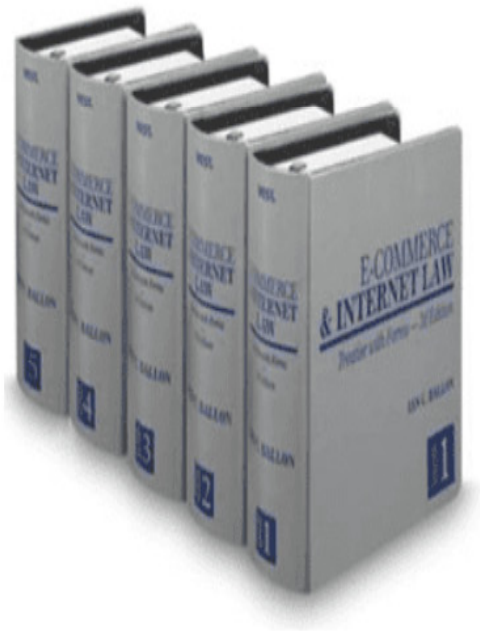
Search...

IANBALLON.NET

IAN C. BALLON

HOME | ABOUT THE AUTHOR | ABOUT THE TREATISE | MORE...

E-Commerce & Internet Law: Treatise with Forms - 2d Edition



BUY NOW

2020 UPDATES NOW AVAILABLE!!

The revised and updated edition of this comprehensive work provides you with a complete legal authority on e-commerce and Internet law, covering business-to-business and business-to-customer issues, regulatory issues, and emerging trends. It includes practice tips and forms and its unique organization facilitates finding quick answers to your questions. This valuable resource on Internet and e-commerce issues contains nearly 10,000 detailed footnotes, plus references to hundreds of unpublished court decisions, many of which are not available anywhere else.

CYBERSECURITY BREACH PUTATIVE CLASS ACTION LITIGATION

Cybersecurity Class Action Litigation

- Cybersecurity claims
  - Breach of contract (if there is a contract)
  - Breach of the covenant of good faith and fair dealing (if the contract claim isn't on point)
  - Breach of implied contract (if there is no express contract)
  - Breach of fiduciary duty, Negligence, Fraud, unfair competition
  - State cybersecurity statutes (especially those that provide for statutory damages and attorneys' fees)
  - California (and potentially Oregon) IoT Law, CCPA
- Securities fraud
  - In re Facebook, Inc. Securities Litigation, 405 F. Supp. 3d 809 (N.D. Cal. 2019) (dismissing plaintiffs' putative class action suit alleging that defendants made materially false and misleading statements and omissions concerning its privacy and data protection practices in violation of federal securities laws)
- Data privacy claims
  - Electronic Communications Privacy Act
    - Wiretap Act
    - Stored Communications Act
  - Computer Fraud and Abuse Act
    - $5,000 minimum injury
  - Video Privacy Protection Act
  - State laws
    - Illinois Biometric Information Privacy Act (recently adopted in other states)
    - Michigan's Preservation of Personal Privacy Act
    - California laws including the California Consumer Privacy Act (CCPA)
      - Other claims are preempted by the CCPA *only* if based on a violation of the CCPA
  - Breach of contract/ privacy policies
    - In re Equifax, Inc., Customer Data Security Breach Litigation, 362 F. Supp. 3d 1295, 1331-32 (N.D. Ga. 2019) (granting defendant's motion to dismiss breach of contract claims premised on Equifax's Privacy Policy)
    - Bass v. Facebook, Inc., 394 F. Supp. 3d 1024, 1037-38 (N.D. Cal. 2019) (dismissing claims for breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, quasi contract, and breach of confidence in a putative data security breach class action suit, where Facebook's Terms of Service included a limitation-of-liability clause)
  - Regulatory enforcement – the FTC and potentially state Attorneys General, including in California (under the CCPA)
    - FTC VTech (2018) and Vizio (2017) enforcement actions
    - Coordinate litigation and regulatory enforcement (usually confidential)

Security Breach Consumer Class Action Litigation

- Circuit split on Article III standing – Low threshold: 6th, 7th, 9th, DC vs. high threshold: 2d, 4th, 8th (3d)
- **Remijas v. Neiman Marcus Group, 794 F.3d 688 (7th Cir. 2015)**
- **Lewert v. P.F. Chang's China Bistro Inc., 819 F.3d 963 (7th Cir. 2016)**
- **Dieffenback v. Barnes & Noble, Inc., 827 F.3d 826 (7th Cir. 2018)**
- **Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) (2-1)**
- Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011), cert. denied, 566 U.S. 989 (2012)
- **Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017)**
  - Allegation that data breaches created an enhanced risk of future identity theft was too speculative to constitute an injury-in-fact
    - Rejected evidence that 33% of health related data breaches result in identity theft
    - Rejected the argument that offering credit monitoring services evidenced a substantial risk of harm (rejecting *Remijas*)
  - Mitigation costs in response to a speculative harm do not qualify as injury in fact
- **Whalen v. Michael's Stores, Inc., 689 F. App'x. 89** (2d Cir. 2017)
  - The theft of plaintiff's financial information was not sufficiently concrete or particularized to satisfy *Spokeo*
  - breach of implied contract, N.Y. Gen. Bus. L. § 349
  - Plaintiff made purchases via a credit card at a Michaels store on December 31, 2013
  - Michaels experienced a breach involving credit card numbers but no other information such as a person's name, address or PIN
  - plaintiff alleged that her credit card was presented for unauthorized charges in Ecuador on January 14 and 15, 2014, but she did not allege that any fraudulent charges were actually incurred by her prior to the time she canceled her card on January 15
- **Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), cert. denied, 138 S. Ct. 981** (2018)
  - following *Remijas v. Neiman Marcus Group, LLC* in holding that plaintiffs, whose information had been exposed but who were not victims of identity theft, had plausibly alleged a heightened risk of future injury to establish standing because it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the intent and ability to use the data for ill."
- **In re U.S. Office of Personnel Management Data Security Breach Litig.**, 928 F.3d 42 (D.C. Cir. 2019) (21mil records)
- **In re SuperValu, Inc., Customer Data Security Breach Litig., 870 F.3d 763 (8th Cir. 2017)**
  - affirming dismissal for lack of standing of the claims of 15 of the 16 plaintiffs but holding that the one plaintiff who alleged he suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract, state consumer protection and security breach notification laws and unjust enrichment
  - defendants experienced two separate security breaches, which they announced in press releases may have resulted in the theft of credit card information, including their customers' names, credit or debit card account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs). Plaintiffs alleged that hackers gained access to defendants' network because defendants failed to take adequate measures to protect customers' credit card information
  - **Rejected cost of mitigation (*Clapper*) (*Cf. P.F. Chang's*)**
- **In re Zappos.com, Inc.,** 888 F.3d 1020 (9th Cir. 2018), cert. denied, 139 S. Ct. 1373 (2019)
  - merely having personal information exposed in a security breach constitutes sufficient harm to justify Article III standing in federal court, regardless of whether the information in fact is used for identity theft or other improper purposes
  - **Bootstrapping -** Because other plaintiffs alleged that their accounts or identities had been commandeered by hackers, the court concluded that the appellants in *Zappos* – who did not allege any such harm – could be subject to fraud or identity theft
- **Causation/ damages – a major issue in most cases**
- **Settlement value**

THE CALIFORNIA CONSUMER PRIVACY ACT

CCPA Putative Class Action Litigation

- The private right of action narrowly applies only to security breaches and the failure to implement reasonable measures, not other CCPA provisions
- But plaintiffs may recover statutory damages of between $100 and $750
- The CCPA creates a private right of action for consumers "whose nonencrypted or 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 . . . ."
- What is *reasonable* will be defined by case law
- $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."
- 30 day notice and right to cure as a precondition to seeking statutory damages (modeled on the Consumer Legal Remedies Act)
  - Can one "cure" a breach?
  - If cured, a business must provide "an express written statement" (which could later be actionable)
- 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"
- CCPA claims typically are joined with other cybersecurity breach or data privacy claims

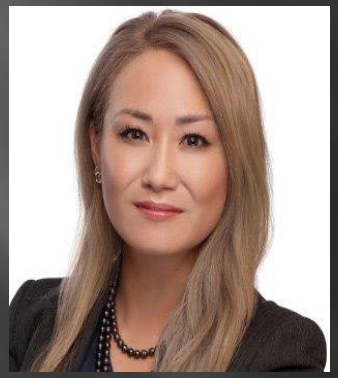
Strategies for CCPA & Other Cybersecurity litigation

- For CCPA claims – do you respond to the 30 day notice and if so how?
- For all claims – can you compel arbitration
- Motions to Dismiss
  - Standing – depends on the circuit and the claims
  - Failure to state a claim
  - CCPA – were the elements of a claim met?
- Summary judgment
- Class Certification
- Privilege issues
- Trial
- Settlement
- How to avoid class action litigation/ Does the CCPA even apply?
  - Encrypt your data and comply with the CCPA (or make sure to avoid its application)….
  - Craft a binding and enforceable arbitration provision and include it in every contract with consumers under the FAA (not state law), avoiding or complying with AAA requirements
  - Make sure your online and mobile consumer contract formation process conforms to the law in the worst jurisdictions
  - Where you don't have privity of contract, make sure you are an intended beneficiary of an arbitration clause in a contract with a business partner who does have privity (because you will be sued!)
  - Explore insurance coverage

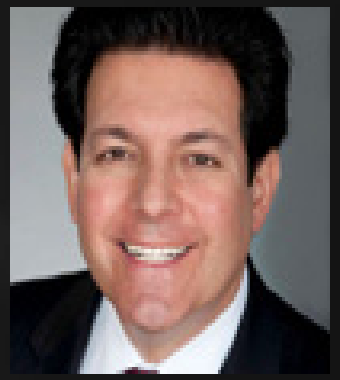
Cyber Litigation In-House Prep Checklist

- Consumer-Facing T&Cs and PP
  - Audit T&Cs and PPs made available to consumers on a persistent basis--where are they linked to/from? (global footer, hamburger menus, FAQs)
  - Version history for terms and conditions and privacy policies and ensure all links point to the latest version
  - Sign-in/sign-up flows within different entry points (SEM, Paid Marketing)for incorporation of and reacknowledgement flows or messaging for in-app updates to T&Cs and PPs. Review to ensure enforceable agreement and sufficient notice to consumers of relevant provisions
- Contract Provisions and Ancillary Documentation
  - Review Data Processing Addendums, confidential information, security schedules, arbitration, representations and warranties to comply with applicable laws, insurance, and governing law provisions in agreements
  - Understand interplay of any applicable representations and warranties, indemnity obligations, and limitation of liability and any insurance coverage
  - Look out for security questionnaires completed as part of vendor due diligence or other security policies that are incorporated by reference into your definitive agreement
- Data incident process
  - Review all existing processes within you company (information security, legal, IT)
  - Confirm all external-facing policies (posted publicly or sent under NDA to third parties) are accurate
  - Identify privilege issues, if any, and how to mitigate
  - Do table-top exercises (or follow process and do post-mortems on minor data incidents) to ensure processes are working in the event of a major data breach
- Identify your resources and limitations in advance
  - Understand your insurance coverage, if any, (including breach coaching, policy exclusions, panel counsel limitations)
  - Interview your attorneys in advance to determine who to call
  - Make sure other vendors are working together with in-house and outside counsel (crisis PR, security forensics, e-discovery)
  - Contemplate internal distraction and costs (marketing teams, data/BI, security)

CCPA AND OTHER CYBERSECURITY LITIGATION



Mia Chiu
Vice President and General Counsel
Rakuten Rewards
mia.chiu@rakuten.com



Ian Ballon, JD, LLM, CIPP/US
Co-Chair, Global IP & Technology Practice Group
Greenberg Traurig LLP
(650) 289-7881 (310) 586-6575
Ballon@GTLaw.com
Facebook, Twitter, LinkedIn: Ian Ballon
www.IanBallon.net