The CCPA/CRA, BIPA, UCL and Beyond: A Primer on Privacy Class Actions and Litigation Avoidance

September 22, 2021

Speakers

Natalie Prescott, CIPP/US, CIPP/E, CIPM
Litigation and Privacy Class Action Attorney,
Mintz Levin

San Diego
nprescott@mintz.com // +1.858.314.1534

- IAPP Certified Information Privacy Professional (CIPP/US, CIPP/E), Certified Information Privacy Manager (CIPM), a published book author, and an award-winning trial lawyer. Focuses practice on bet-the-company cases, class actions, and complex litigation matters.
- Assists clients with defending data breach and privacy class actions, responding to regulatory inquiries into data security practices, data breach notifications, compliance, privacy policies, and incident management and response.

Vivek Narayanadas, CIPP/US, CIPP/E
VP, Legal
Shopify

San Diego
vivek.narayanadas@shopify.com

- Vice President, Legal at Shopify, a global publicly-traded company that operates an ecommerce platform that enables small businesses, entrepreneurs, and creators to sell their goods and services around the world.
- At Shopify, Vivek built, scaled, and now manages the company's privacy, intellectual property, litigation, regulatory affairs, government affairs, and antitrust functions.
- Relevant here, he oversees the teams that manage Shopify's privacy product counseling and governance function, their security incident response function, and their teams that manage all litigation, dispute, and regulatory investigations.

Maryam Rad
VP, Cyber Initiatives & Claims Director,
Lockton Companies

Los Angeles
MRad@lockton.com // +1.213.689.0504

- Cyber Initiatives & Claims Director at Lockton Companies, the world's largest privately held insurance broker, within its Global Cyber & Technology Practice, working on thought leadership and strategic initiatives.
- Assists clients navigating complex cybersecurity incidents, privacy liability matters, and errors and omissions claims, within a variety of industries, including technology, healthcare, manufacturing, retail, construction, legal services, and higher education.

Covered in this Presentation

- Latest Privacy Trends
- Cyber Insurance Market Trends
- Key U.S. Privacy Laws
- Collection of Personal Data
- Litigation Avoidance
- Insurance Claims Considerations
- Questions

Latest Privacy Trends

All Eyes Are on Privacy and Cybersecurity!

Top U.S. Verdicts, Settlements, and Penalties:

- **$61 million** TCPA *verdict* against Dish Network (50,000 calls); **$210 million** DOJ settlement with Dish.
- **$5 billion** FTC's *penalty* against Facebook (PI shared with third-party apps).
- **$12.6 million** FTC's CAN-SPAM Act *penalty* against IcloudWorx (spam emails).
- **$575 million + $700 million** FTC's *settlements* with Equifax (unencrypted SSNs).
- **$148 million** *fine* by New York AG against Uber (data breach, 57 million individuals).

Claims Against Directors and Officers:

- **$29 million** settlement of data breach shareholder derivative suits against Yahoo and its former officers and directors (for breach of fiduciary duty and concealing cyber attacks). *In re Yahoo! Shareholder Litigation*, Case No. 17-CV-307054 (Cal. Sup. Ct. Jan. 4, 2019).
- **Federal court denied the motion to dismiss** as to Equifax's former CEO and chairman of the board, who allegedly knew that Equifax's data protection systems were grossly inadequate, had the power to control cybersecurity policies and the statements made, and made misleading statements about the company's data security. *In re Equifax Inc. Securities Litigation*, 357 F. Supp. 3d 1189 (N.D. Ga. 2019).
- Delaware court found **directors may be individually liable** for a breach of their duty of loyalty if they fail to make a good-faith effort to implement "a reasonable board-level system of [compliance] monitoring and reporting." *Marchand v. Barnhill*, 212 A.3d 805, 821 (Del. 2019).

The SEC Places the Burden on the Board and Officers:

- The SEC: it is the **Board's role to (1) understand the risks, (2) ensure that the organization is addressing them, and (3) be responsible** for the company's adequate cybersecurity program.
- As part of their proxy statement, public companies must disclose the board's participation in cybersecurity efforts and risk management and specifically address "the nature of the Board's role in overseeing the management of that risk." *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 17 CFR Parts 229 and 249, SEC Release Nos. 33-10459 and 34-82746 (Feb. 6, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.
- The SEC settles with App Annie and its former CEO for $10 million for misrepresentations and misuse of confidential data.

Cyber Insurance Market Trends

Cyber Insurance Market Trends

- Hardening Market Conditions
  - Ransomware claims and resultant business interruption losses
  - Increased legislative activity
  - Regulatory enforcement actions
  - Privacy litigation losses

- Cyber Market Response
  - Increased underwriting scrutiny
  - Reduced limits
  - Restrictions on coverage
  - Rate increases

Key U.S. Privacy Laws

TCPA (47 USC § 227)

What does this law regulate?

- **Telemarketing and advertising**.

When does it apply?

- Federal law; applies nationwide in the USA.
- When companies use an autodialer, robocalls, pre-recorded calls or send unwanted texts or faxes.

What should companies do?

- Check do-not-call ("DNC") registries.
- Record and honor DNC requests.
- Avoid an autodialer (calls dialed by a computer).
- Send marketing texts only with consent; provide and honor unsubscribe options.
- Obtain and document consent.
- The **penalty is $500 per *each* violation** ($1,500 for willful violations).

BIPA (740 ILCS 14/1)

What does this law regulate?

- **Companies that possess, collect, or use biometric information** of Illinois residents.

What is “biometric” information?

- A wide variety of identifiers such as retina scans, iris scans, fingerprints, palm prints, voice recognition, facial-geometry recognition, DNA recognition, gait recognition, and even scent recognition.

What should companies do?

- Consider if biometric technology is necessary.
- Develop a written policy, promptly destroy data, provide advance notice to the individuals, obtain consent, and allow opt-out.
- The **penalty is $1,000** for *each* negligent violation, or $5,000 penalty for *each* willful or reckless violation.

CIPA (Cal. Penal Code § 630)

What does this law regulate?

- Confidential communications.
- **Recording of calls** without the caller's knowledge and consent, wiretapping, eavesdropping.

Where does it apply?

- To recordings, eavesdropping, wiretapping of confidential communications involving California residents.
- Some other U.S. states have similar laws.

What should companies do?

- Disclose at the outset that the call is being monitored or recorded.
- The penalty for violating this law is **$5,000 per *each* violation**.

The CCPA (Cal. Civ. Code § 1798.150)

- What does this law regulate?
  - **For-profit companies** that do business in California and **collect personal information of California consumers** and (1) have annual gross revenues of **$25 million**; or (2) annually buy, sell, receive, or share PII of **50,000 or more** [100,000 under CPRA] **California consumers** or (3) derive **50% or more of annual revenues** from selling PII.
- What is "personal information"?
  - PII: "[I]nformation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- What should companies do?
  - Within 45 days of receiving a verifiable request, the company must disclose what information it collected, from whom, to whom it disclosed it, why, and whether it sold it; it must honor the consumer's right to deletion and the right to opt out of the sale of PII.
  - The companies must establish an intake mechanism; develop policies and procedures for verification; update online privacy policy; address security; amend service agreements; and train employees.
- Private right of action: Statutory damages between **$100 and $750** or actual damages, *per* violation.
- AG enforcement: Penalties between **$2,500 and $7,500** for negligent vs. intentional violations, *per* violation.

The CCPA → the CCPA 2.0

New Privacy Rights	
CCPA	**CPRA**
Right to know/access	Right to know/access
Right to delete	Right to delete
Right to opt-out of third-party sales	Right to opt-out of third-party sales and sharing
Right to non-discrimination	Right to non-discrimination
	Right to limit use/disclosure of sensitive PII
	Right to correct
	Right to access information about automated decision-making
	Right to opt-out of automated decision-making technology

The CCPA vs. CPRA Comparison

Requirements	CCPA	CPRA	Requirements	CCPA	CPRA
Right to know what info business collects about you	✓	✓	Storage limitation: right to prevent storing for longer than necessary	X	✓
Right to say “no” to sale of your info	✓	✓	Data minimization: right to prevent collection of more info than necessary	X	✓
Right to delete	✓	✓	Right to opt out of geolocation ads	X	✓
Security: business must keep info safe	✓	✓	Override of privacy in emergencies	X	✓
Portability: right to access info in portable format	✓	✓	Transparency around “profiling” and “automated decision making”	X	✓
Protection for minors	✓	✓	California Privacy Protection Agency	X	✓
“Do Not Sell My Info” button	✓	✓	Chief Auditor who can audit businesses	X	✓
Ability to browse without pop-ups or sale of your info	X	✓	Restricts onward transfer to protect PI	X	✓
Penalties if email + password stolen due to negligence	X	✓	Requires regular cybersecurity audits by high-risk data processors	X	✓
Right to restrict use of sensitive PI	X	✓	Requires regular risk assessments by high-risk data processors	X	✓
Right to correct your data	X	✓	Protection against future legislation	X	✓

The CPRA: Key Changes

- **Effectively requires data minimization.**
- **Doubles CCPA's number of consumers/households to 100,000.**
- **Creates the California Privacy Protection Agency.**
- "Contractor" – an entity 'to whom a business makes available a consumer's personal Information for a business purpose pursuant to a written contract with the business."
- "Share" – by a business to a third party for cross-context behavioral advertising for the benefit of a business where no money is exchanged.
- Expands categories of PII. Allows enforcement by District and City Attorneys.
- **Adds "Sensitive Personal Information" (SSN, DL, biometric, geolocation, financial info, race, etc).**
- Somewhat expands the scope of private right of action by expanding definition of PII.
- Automatic $7,500 for violations involving minors.
- Use limitation: limits collection/retention/use to what is necessary to provide goods or services.
- **Removes 30-day cure period for AG enforcement actions (but not for private lawsuits).**

Collection of Personal Data

“Sensitive Personal Information”

- Important new definition under the CPRA
- New categories of protected information and higher level of protection
- New regulations anticipated – new opportunities for consumer/business confusion
- New disclosure requirements
- New link requirement!

“Sensitive Personal Information” (“SPI”)

“‘Sensitive personal information’ means: (1) personal information that reveals (A) a consumer’s social security, driver’s license, state identification card, or passport number; (B) a consumer’s account log-In, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (C) a consumer’s precise geolocation; (D) a consumer’s racial or ethnic origin, religious or philosophical beliefs, or union membership; (E) the contents of a consumer’s mail, email and text messages, unless the business is the intended recipient of the communication; (F) a consumer’s genetic data; and (2)(A) the processing of biometric information for the purpose of uniquely identifying a consumer; (B) personal information collected and analyzed concerning a consumer’s health; or (C) personal information collected and analyzed concerning a consumer’s sex life or sexual orientation. Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) of Section 1798.140 shall not be considered sensitive personal information or personal information.”

What are categories of SPI?

- **ID Numbers**
- **Account Details**
- **Location Data**
- **Diversity Data**
  - Racial or ethnic origin, religious or philosophical beliefs, or union status
- **Mail Content**
  - Contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication
- **DNA Information**
- **Biological Data**
  - Processing of biometric information for purpose of uniquely identifying a consumer's personal information collected and analyzed concerning a consumer's health, or personal information collected and analyzed concerning a consumer's sex life or sexual orientation

Data Breach Litigation Triggers

PII Categories	CCPA	CPRA
Social Security Number (with name)	✓	✓
Driver's license number (with name)	✓	✓
California identification card number (with name)	✓	✓
Tax identification number (with name)	✓	✓
Passport number (with name)	✓	✓
Military identification number (with name)	✓	✓
Other unique government (with name)	✓	✓
Financial account number (which permits access to the account) (with name)	✓	✓
Credit or debit card number (with required security code or password) (with name)	✓	✓
Medical information (with name)	✓	✓
Health insurance information (with name)	✓	✓
Unique biometric data (with name)	✓	✓
Username and password that would permit access to an online account	X	✓

Litigation Avoidance

Litigation Avoidance Tips

- Data minimization
- Written cyber incident response and business continuity plans
- Ensure your organization has:
  - Penetration tests and table-top exercises.
  - Periodic risk assessment of vendors and their policies.
  - Employee training and education.
  - Channels for identifying and reporting problems.
  - Experienced legal team on speed dial.
- Know what type of data your company collects, uses, and shares.
- Allocate appropriate resources to privacy and cyber security.
- Review and update privacy policies regularly.
- Arbitration clauses.
- Class action waivers.
- When sued, develop a case-specific, creative motion and settlement strategy.
- When settling a class action, get the broadest class definition possible.
- Protect incident reports from disclosure.

Insurance Claims Considerations

Insurance Claims Considerations

- Cyber insurance policies:
  - First-party coverage
    - What type of incidents can potentially trigger first party coverage?
  - Third-party claims
    - What is considered a “claim?”
- Best practices in the event of a first party incident and/or third party liability claim:
  - Provide timely notification to insurer(s)
  - Consider the insurer’s approved list of vendors and resources
  - Obtain consent of insurer(s)
  - Communicate with insurer(s) on a regular basis
  - Cooperate with insurer(s)
  - Evaluate the interplay of multiple potential coverages/policies

Questions