Procopio

Latest Developments in Privacy Law

What's Happening Now & What to Expect in the Near Future

May 16, 2023

Elaine F. Harwell, CIPP/US, CIPM
Partner, Procopio
Elaine.Harwell@Procopio.com
619.906.5780

Chris Ghazarian
General Counsel, DreamHost
Christopher.Ghazarian@DreamHost.com
213.787.4401

Data Privacy Laws:

Where are we today?

- Data privacy laws impact any business that collects information from customers, clients, employees, or other businesses, in any form.
- No single omnibus data privacy law in the U.S. (still)
  - Federal statutes primarily sector-specific; state statutes more focused on rights of individual consumers
- California's focus on consumer privacy
  - First state to pass a comprehensive consumer data privacy law, the California Consumer Privacy Act of 2018 (CCPA)
  - November 2020, California voters voted to amend the CCPA, the California Privacy Rights Act (CPRA)
- Other states have since followed CA with their own comprehensive consumer data privacy laws (VA, CO, CT, UT, IN, IA, TN), more being contemplated
- Federal data privacy law? Not yet, but: American Data Privacy and Protection Act?

California Focus:

California Consumer Privacy Act (CCPA)

- The CCPA (now in effect with amendments)
  - Consumer Rights: to know, delete, correct, opt-out of sale/sharing, non-discrimination
  - New Business Obligations: notices to consumers *and* employees, limitations on data "sales" and "sharing" for cross-context behavioral advertising
  - Enforcement (of amendments and newly adopted regulations) begins 7/1/23
- Threshold application to the law:
  - $25MM annual gross revenue; or
  - Collection of 100,000 or more residents' PI; or
  - 50% of annual revenue from sale of PI

Key New CCPA Definitions: Sensitive Information

- Consumer's SSN, driver's license, state ID card, or passport number
- Account log-in, financial account, debit card, or credit card number along with any required access credentials
- Precise geolocation
- Racial or ethnic origin, religious or philosophical beliefs, or union membership
- Contents of a consumer's mail, email, and text messages, unless business is the intended recipient
- Consumer's genetic data
- Biometric information for purpose of uniquely identifying the consumer
- Personal information collected and analyzed concerning a consumer's health
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

Key New CCPA Definitions: Sensitive Personal Information

- Right to limit use and disclosure of sensitive personal information:
  - Consumer can direct business to only use sensitive personal information for "that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services"
    - Ex: precise geolocation used by a map application is reasonably expected, but not by a gaming application where info is not needed to deliver service
  - Sensitive personal information collection and processing not subject to right to limit where collection and processing is not for the purpose of inferring characteristics about a consumer

Key New CCPA Definitions: Selling and Sharing

- Selling – under the CCPA, this is the transfer of a consumer's personal information to another CCPA-covered business or third party for monetary or other valuable consideration.
  - Regulators have interpreted this very broadly.
  - Under the CPRA, without a proper contract in place, any transfer of personal information risks being considered a "sale."
- Sharing is a new concept under the CPRA and is disclosing personal information to a third party for cross-context behavioral advertising.
  - Very specific and narrow definition meant to close a gap under the CCPA.
  - Defined as the targeting of advertising to a consumer based on the personal information obtained from their activity across businesses, distinctly branded websites, applications or services, other than which the consumer intentionally interacts

Key Business Obligations: Opt-Outs of Sale/Share

- CCPA's (and other state laws) providing rights for consumers to opt-out of targeted advertising
- Rights, when exercised, restricts the use of third-party data to retarget consumers
- Under the CCPA:
  - "Do Not Sell My Personal Information" links
  - Privacy notice disclosures
  - Clarifications from the CA Attorney General - third party cookies on websites are likely "selling"
  - The CPRA's "share" provision provided further clarification on questions around targeted advertising

Key Business Obligations: Global Privacy Control

- Global Privacy Control (GPC) signals – must be treated as a valid opt-out-of-sale/sharing requests
  - CA and CO both make this a requirement
  - Upon detection of GPC, must block appropriate transfers of personal information (those qualifying as a “sale” or “share”)

CCPA: Regulations

- First set of rulemaking package:
  - Addressed regulations concerning DPAs, consumer opt-out mechanisms, mandatory recognition of opt-out preference signals, dark patterns, and consumer request handling
  - Finalized and approved by the Office of Administrative Law (OAL); no substantive changes from the final draft submitted by the California Privacy Protection Agency (CPPA) in February
  - Now in effect; will be enforced July 1, 2023
- Second set for rulemaking expected soon?
  - Will address cybersecurity audits, privacy risk assessments, profiling
  - CPPA meeting on May 15, 2023

CCPA Enforcement: Examples

- Sephora
  - Only public enforcement action thus far (announced 8/24/22)
  - Alleged violations of the CCPA and the CA Unfair Competition Law
  - Attorney General (AG) asserted Sephora provided its third party business partners with access to customer data in exchange for advertising or analytics services – these were "sales" triggering basic obligations, such as notice disclosures and allowing customers to opt-out
  - AG also asserted failure to comply with GPC signal
  - Resulted in $1.2 million settlement and certain injunctive relief
- AG has signaled focus on GPC signal and opt-out rights
  - Announced enforcement sweep targeting multiple online retailers
  - Retailers out of compliance where found to be using web tracking technologies to make consumers' personal information available to third parties in exchange for services like advertising or analytics without offering opt-out mechanism
  - Opt-outs should be simple and effective

CCPA Enforcement: Examples

- Other topics of interest to the AG:
  - Dark patterns
    - Confusing or unclear language and toggle options in order to opt-out of sale of information, “on” to opt in or out?
    - Double negatives
    - Multiple steps or layers to exercise rights
  - Do Not Sell links
    - Working links
    - Links describing how to manage cookies, but no mechanism to stop the sale of personal information not permitted
  - Privacy Policies
    - Meeting all disclosures requirements under the law
    - Explicitly state whether “selling” under the CCPA
  - Service Provider contracts
    - Contain necessary restrictions on the use of processed personal information

CCPA Updates: Challenges

- California Chamber of Commerce has filed a legal challenge to toll CPRA enforcement
  - Action filed on March 30, 2023 in state court (Sacramento) for declaratory and injunctive relief to toll the planned July 2023 enforcement of the CPRA
  - Complaint argues that Prop 24 required CPPA to publish regulations one year before the date of enforcement so that businesses would have adequate time to implement the law with the benefit of the regulations
  - Hearing currently scheduled for June 30, 2023

What's Happening Elsewhere?

Other State Privacy Legislation

- Washington passed the My Health My Data Act
  - Reflects dramatic expansion of protections for consumer health data, including consumer health data not traditionally protected by HIPAA
- Multiple BIPA-like legislative proposals introduced:
  - Arizona's "Act Relating to Biometric Information" (SB 1238)
  - New York's "Act Prohibiting Private Entities From Using Biometric Data for Advertising" (AB S02390)
  - Vermont's "Act Relating to Protection of Personal Information" (121)
- Utah passes first-of-its-kind Social Media law requiring robust age verification and prohibiting Utah residents under age 18 from opening an account unless express consent by parent; parents can also access content of minor's account
- Montana approves a statewide ban of TikTok

What's Happening Elsewhere?

AI Regulation

- AI Regulation in the United States
  - California introduces AB 331 that would impose assessment requirements on the private sector's use of AI technologies; draws on Biden Administration's Blue Print for AI Bill of Rights
  - Colorado Division of Insurance releases draft Algorithm and Predicative Model Governance Regulation
  - FTC releases artificial intelligence Guidance: Keep Your AI Claims in Check and other warnings to companies to avoid unfair or misleading practices in AI
  - In healthcare space, FDA announced intention to regulate many AI-powered clinical decision support tools as devices
  - Executive Order from Biden Administration directing federal agencies to address "discrimination" within algorithms used by technology companies
  - Biden Administration announced it has begun a study into possible rules to regulate AI like ChatGPT. Public comments due June 12, 2023.
  - NIST released Artificial Intelligence Risk Management Framework 1.0
  - U.S. Senator Chuck Schumer announced in April development of a framework for regulation; currently in review and receiving expert input
  - USPTO seeking public comment regarding AI inventions
- AI Regulation in Europe
  - EU AI Act – anticipated to be passed later this year
  - UK's approach – AI White Paper published 3/29/23, AI Regulation: A Pro-Innovation Approach
  - European Parliament issued open letter pushing the EU to impose a new set of rules to govern the use of AI tools, despite that EU is already considering the AI Act.
  - Italy temporarily bans ChatGPT and then shortly thereafter lifts ban after new privacy controls implemented to address immediate concerns

What's Happening Elsewhere? Cybersecurity

- NIST Cybersecurity Framework 2.0
- FBI releases 2022 Internet Crime Report
  - 800,944 complaints (many more unreported), with losses exceeding $10.3 billion
  - Phishing schemes were number one crime reported, and for the first time, investment schemes reported the highest financial loss to victims
- White House releases National Cybersecurity Strategy
- New York releases guide to help businesses adopt effective data security measures to protect personal information

What's Happening Elsewhere?

Increased resources, enforcement, and litigation

- FTC proposed hiring an additional 310 full-time employees, including 62 dedicated to "increasingly complex consumer protection investigations, including privacy and data security issues"
- CPPA anticipates doubling staff in next year (currently 26 staff attorneys)
- European Data Protection Board announced Data Protection Officer (DPO) initiative: the 26 Data Protection Authorities across the EEA will be focusing on designation and position of data protection offices
  - Focus will be on whether DPOs have the appropriate position within their organization and appropriate resources to carry out their tasks
- Bloomberg reports that BIPA litigation in Illinois sees increase after Supreme Court ruling in *Cothron v. White Castle*, which held that every scan of biometric data was an independent violation of the law

Thank you!

Questions?

Elaine F. Harwell, CIPP/US, CIPM
Partner, Procopio
elaine.harwell@procopio.com
619.906.5780

Chris Ghazarian
General Counsel, DreamHost
Christopher.Ghazarian@DreamHost.com
213.787.4401

Procopio