State privacy legislation
(and more)

Justin Brookman, Consumer Reports Advocacy

Development of US law on privacy

- Brandeis argues for “right to be left alone” in 1890
- Articulation(s) of Fair Information Practice Principles
  - Transparency, data minimization, security, accountability, &c.
- Sectoral specific laws emerge
  - Fair Credit Reporting Act (FCRA)
  - Children’s Online Privacy Protection Act (COPPA)
  - Health Information Portability and Accountability Act (HIPAA)
  - Video Privacy Protection Act (VPPA)
- But no comprehensive privacy law

Current state of federal privacy law

- Lags rest of world
  - GDPR, similar laws elsewhere
- Section 5 of the Federal Trade Commission Act
  - Prohibition on “deceptive” business practices
    - “Don’t lie”
    - But may extend to material omissions
  - Prohibition on “unfair” business practices
    - Three-part test, including demonstration of “substantial harm”
    - Used aggressively on data security cases to mandate reasonable security
    - FTC has applied sparingly on privacy cases (Facebook, Vizio)
    - Unclear how far this authority could extend

States have historically taken the lead on privacy and security

- Constitutional protections
  - CA, recent NH ballot initiative
- State data breach notification laws (all)
- State security laws
- Additional sectoral protections (*e.g.*, CMIA)
- California Consumer Privacy Act of 2018 (CCPA) — first comprehensive privacy legislation in US

The sudden advent of the CCPA

- Ballot initiative proposed by real estate developer Alastair MacTaggart in mid-2017
- Cambridge Analytica breaks — tremendous media and consumer backlash on privacy
- CA legislators worry about difficulty in amending voter referendum, introduce legislation designed to offer compromise solution
- Small working group develops legislation in ~month
  - Passed with minimal amendments and signed by governor
  - MacTaggart agrees to withdraw ballot initiative

Scope

- All entities doing in business in California and
  - > $25m revenues/year,
  - Data on 50k people, or
  - Derives ½ of income from selling personal data
- Nonprofits?
- Covered information — very broad!
  - Includes online and offline data
  - Carve-out for deidentified data

New rights: transparency

- Obligation to provide pre-collection information about data collection and sharing practices
  - Types of data collected
  - For what purposes
  - Categories of data sources
  - Categories of third parties with which data is shared (sold or service providers)

New rights: access

- Consumers have the right to request specific pieces of information from any covered business
  - If verifiable consumer request
  - Prompt, free of charge, twice a year
  - Portable data format
  - Also, categories of data sold to third parties, and categories of third parties with which data is sold

New rights: opt-out of sharing

- Consumers have the right to tell businesses not to sell your information
  - Sell defined broadly
- Important exceptions — shared for limited “business purposes” to service providers
- Opt-out *not* subject to verification
- How will it apply to online ad (and other third-party) tracking?

New rights: special protections for minors

- Can’t sell information about minors under 16 without affirmative consent
  - 13-16 — consent of the minor
  - Under 13 — consent of the adult

Limits (?) on discriminatory treatment against users who exercise privacy rights

- A company cannot charge more or offer lower quality to a user who exercises privacy rights . . . *unless* "that difference is reasonably related to the value provided to the consumer by the consumer's data"
- A company may offer financial incentives for collection, sale, or deletion of information
- Financial incentive can't be "unjust, unreasonable, coercive, or usurious"
- One of the most significant (and controversial) changes from the ballot initiative

Enforcement

- Primarily enforced by CA Attorney General
  - Penalty of $2500/$7500 per violation
  - BUT, if you can *cure* the violation within 30 days of receiving notice, you can escape liability (also controversial)
  - Consumer Privacy Fund
- Local/whistleblowers/private right of action largely stripped out
- PRA limited to violations of existing data security law

Attorney General implementing regulations

- Attorney General's office directed to issue clarifying regulations on a number of topics:
  - Definition of personal data
  - Verifiable consent
  - How opt-out works

What CCPA doesn’t do

- Doesn’t really address collection or use by first parties
- Not an opt-in regime (which GDPR might be)
- No data minimization requirements
- Certain existing legal regimes protected — CMIA, GLB

What's next?

- CA legislature agreed to narrow clerical amendments in fall
- Big fight over substantive amendments in 2019
- AG implementing regulations
- Goes into effect in 2020 . . . unless
- Legal challenges under Commerce Clause, First Amendment, &c . . .

Security legislation

- In addition to data breach notification legislation, nearly half of states have data *security* legislation
  - Range from “use reasonable measures” to fairly prescriptive
  - Not part of CCPA because already enacted
- Roughly consistent with authority the FTC has asserted under its UDAP authority
- Cybersecurity legislation
  - CA enacted first cybersecurity law (covering misuse of connected devices separate from information leakage) in 2018

Federal legislation

- Will this all be preempted by the federal government anyway?
  - Bipartisan support (in theory) for comprehensive federal privacy, security, breach notification legislation
- Given precedent of breach notification legislation . . . probably not.

Questions?

Justin Brookman
Consumer Reports Advocacy
justin.brookman@consumer.org