The State of Privacy Law

Kelly McCanlies, FIP, CIPP/US, CIPM, CIPT

Agenda

- Common Terms
- “Patchwork” laws
  - Federal
  - State
  - Case law
- Comprehensive laws
  - General Data Protection Regulation (GDPR)
  - California Consumer Privacy Act (CCPA)
- Trending privacy issues
  - Facial recognition
  - Geolocation data
  - Data Brokers
  - Internet of Things

Common Terms

- Data Privacy

  Data Privacy focusses on permissible data collection and use.

- Data Security

  Data security focuses on the administrative, physical, and technical controls required to deter unauthorized access.

Common Terms (cont.)

- Personal Information (PI)
  - 2006: HRS 5487-N

    "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

    (1) Social security number;

    (2) Driver's license number or Hawaii identification card number; or

    (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account.
- Personally Identifiable Information (PII)
  - FTC
    - 2000:

      PII is information that is linked to a specific individual including, but not limited to, name, postal address, email address, Social Security number, or driver's license number.

    - 2012:

      COPPA - added photos, persistent identifiers, location (street name plus city)

    - 2016:

      "We now regard data as personally identifiable when it can be reasonably linked to a particular person, computer, or device… In many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test."

Federal Privacy Laws – Sector Specific

- 1914 - Federal Trade Commission Act
  Unfair or deceptive acts or practices
- 1970 - Fair Credit Reporting Act
- 1974 - Privacy Act
  Applies to federal agencies
- 1974 - Family Educational Rights and Privacy Act
  Records from schools that receive US DOE funds
- 1991 - Telephone Consumer Protection Act
- 1996 - Health Insurance Portability and Accountability Act
  Protected Health Information (PHI)
  Covered entities - health care providers, health plans, health care clearinghouses and business associates.
- 1996 Telecommunications Act
  Customer Proprietary Network Information (CPNI)
- 1998 - Children's Online Privacy Protection
  Websites or online services directed to children under the age of 13
  Notice to and consent from parents
- 1999 -Gramm-Leach-Bliley Act
  "Nonpublic Personal Information" (NPI)
- 2003 - Fair and Accurate Credit Transactions Act
  Preventing identity theft, instituted the Red Flag Rule
- 2003 - Controlling the Assault of Non-Solicited Pornography And Marketing
  Commercial emails.
- 2003 – Do Not Call Act

State Privacy Laws

- Data breach notification laws
  - California - SB 1386 (2002)
  - Hawaii - 487 N (2006)
    - HRS 487 J and R
  - All 50 states, Guam, Puerto Rico, Virgin Islands, DC
  - Common clauses:

    Definitions "Doing business in" clause Encryption safe harbor "Risk of harm" threshold
- Credit card laws
  - Transactions - California Song Beverly "lemon law"
  - PCI - Minnesota, Nevada, Massachusetts, Washington
- Biometrics
  - Illinois, Texas and Washington
  - Proposed in New York, Michigan, Florida and Alaska
  - Illinois - Biometric Information Privacy Act

Comprehensive laws - GDPR

- Who is regulated?

  Data controllers and data processors that process personal data:

  - in the context of activities of the EU establishment, regardless of whether the data processing takes place within the EU.
  - in connection with offering goods or services in the EU, or monitoring their behavior.

  A **controller** determines the purposes and means of processing personal data. A **processor** is responsible for processing personal data on behalf of a controller.

  The controller or processor envisages offering services to data subjects in one or more Member States in the Union.

- Who is protected and what is protected?

  'Personal data' means any information relating to an identified or identifiable natural person ('Data Subject').

  The information must be part of a filing system or be stored in a computer.

GDPR: Subject Requests

A data controller must:

- Verify the identity of a data subject before responding to a request.
- Respond to requests without undue delay and at the latest within one month., extendable for up to two more months if necessary after data subject notice.
- Give reasons if the data controller does not comply with any requests.

Requests can be either verbal or in writing.

Requests do not have to be free to data subjects.

GDPR: Major Provisions

- Right to access
  Data subjects have a right to access their personal data, including receiving a copy and to obtain certain information about the data controller's processing.

- Right to rectification
  Includes the right to correct inaccurate personal data and complete incomplete personal data.

- Right to deletion
  Data subjects have the right to request erasure of personal data under six circumstances (the right to be forgotten). Data controllers must also take reasonable steps to inform any other data controllers also processing the data.

- Right to restrict processing
  Opt-out of processing data for marketing purposes.
  Right to object to processing for profiling, direct marketing, and statistical, scientific, or historical research purposes.
  Withdraw consent for processing activities. An alternative to requesting the erasure of data and is mostly exercised when individuals contest the accuracy of information, the way it is processed or if they want the data to be erased but the organization has a legal obligation to retain it.

- Right to data portability
  Receive a copy of the personal data in a structured, commonly used and machine readable format.
  Transmit the personal data to another data controller (including directly by another data controller where possible).

- ~~Right to opt out of sale~~

- Right to opt out of automated decision making
  Data subjects have the right to not be subject to automated decision making, including profiling which has legal or other significant effects on the data subject, subject to certain exceptions.

GDPR: Major Provisions (cont.)

- Private right of action
  Establishes a private right of action for material or non-material damage caused by a data controller or data processors.
- Notice
  Data controllers must provide detailed information about its personal data collection and data processing activities. The notice must include specific information depending on whether the data is collected directly from the data subject or a third party.
- Notification
  Data controllers or processors have 72 hours to report to a Data Protection Authority, if there an incident "leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
- Risk assessment
  Notification is required if the incident leads to a potential risk to people's rights and freedoms. If a company decides that a breach does not fall under the requirements to notify a DPA of the breach, it is still required to inform its data protection officer (DPO) and formally document the breach.
- Prohibition on discrimination against a consumer for exercising a right
  It is implicit in GDPR that organizations cannot discriminate against a data subject that exercises his rights, for example by references prohibiting processing that adversely affects the rights and freedoms of data subjects.
- Purpose limitation
  Personal data can only be used for a new purpose if it is compatible with the original purpose, or for archiving, scientific or historical research, or statistical purposes.
- Processing limitation
  Processing must have a legitimate basis: Consent, Contract, Legal Obligation, Vital Interest, Public Tasks, Legitimate Interests

GDPR: Additional considerations

- Age of Consent

  16. Children must receive an age appropriate privacy notice.

- Security

  Appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

  Children's personal data is subject to heightened security requirements.

- Anonymized, pseudonymous or de-identified, and aggregated data
  - Anonymous and aggregated data are not considered personal data.
  - Pseudonymous data is considered personal data.

- Enforcement

  The fines must be effective, proportionate and dissuasive.

  The authorities have a statutory catalogue of criteria which it must consider for their decision. Among other things, intentional infringement, a failure to take measures to mitigate the damage, or lack of collaboration with authorities can increase the penalties.

  Administrative fines of up to EUR 20 million or 4% of annual global revenue, whichever is highest.

Comprehensive laws - CCPA

- Who is regulated?

  Any for-profit entity doing business in California, that meets one of the following:

  - Has a gross revenue greater than $25 million.
  - Annually buys, receives, sells, or shares the personal information of more than 50,000 consumers, households, or devices for commercial purposes.
  - Derives 50% or more of its annual revenues from selling consumers' personal information.

- Who is protected?

  Consumers, defined as California residents. Consumers also include:

  - Customers of household goods and services.
  - Employees.
  - Business-to-Business transactions.

Comprehensive laws - CCPA

- What Information is protected?

  Personal information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household.

  Includes a non-inclusive list:
  - Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, SSN, driver's license number, passport number, or other similar identifiers.
  - Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
  - Biometric information.
  - Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or ad.
  - Geolocation data.
  - Audio, electronic, visual, thermal, olfactory, or similar information.
  - Professional or employment-related information.
  - Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.
  - Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

  Personal information does not include certain publicly available government records.

  The CCPA also excludes certain personal information covered by other sector-specific laws. It does not exclude GLBA from a private right of action.

CCPA: Consumer Requests

A business must:

- Comply with a verifiable consumer request
- Respond within 45 days after receipt, potentially extendable once for another 45 on customer notification.
- Inform the consumer of the reasons for not taking action.
- Provide the information free of charge, unless the request is manifestly unfounded or excessive.
- Consumers may only make most information requests twice a year and only for a 12-month look-back. There are no limits on deletion and do not sell requests.

CCPA: Major Provisions

- Right to access
  Consumers have a right to request disclosure of their personal information, and to receive additional details regarding the personal information a business collects and its use purposes, including any third parties with which it shares information.
- ~~Right to rectification~~
- Right to deletion
  A consumer has the right to deletion of personal information a business has collected, subject to certain exceptions.
  The business must also instruct its service providers to delete the data.
- ~~Right to restrict processing~~
- Right to data portability
  In response to a request for disclosure, a business must provide personal information in a readily useable format to enable a consumer to transmit the information from one entity to another entity without hindrance.
- Right to opt out of sale
  Businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, subject to certain defenses.
  Must include a "Do Not Sell My Personal Information" link in a clear and conspicuous location on a website homepage.
  Must not request reauthorization to sell a consumer's personal information for at least 12 months after the person opts-out.
  Third parties must also give consumers explicit notice and an opportunity to opt out before re-selling personal information that the third party acquired from another business.

CCPA: Major Provisions (cont.)

- ~~Right to opt out of automated decision making~~
- Private right of action
  The CCPA establishes a narrow private right of action for certain data breaches involving a sub-set of personal information. However, the CPPA grants companies a 30-day period to cure violations, if possible.
- Notice
  Businesses must inform consumers about the personal information categories collected and the intended use purposes for each category.
  Further notice is required to collect additional personal information categories or use collected personal information for unrelated purposes.
- Notification
  Covered under prior California law.
  AB-1130 just passed Senate Appropriations Committee to add additional fields, including passport number and biometric data.
- ~~Risk assessment~~
- Prohibition on discrimination against a consumer for exercising a right
  A business must not discriminate against a consumer because they exercised their rights. However, a business may charge differently if that difference reasonably relates to the value provided by the consumer's data.
  Businesses may also offer financial incentives if they are disclosed in terms or online privacy policy, and require opt-in consent.
- ~~Purpose limitation~~
- ~~Processing limitation~~

CCPA: Additional considerations

- Age of Consent

  13.

- Security

  CCPA does not directly impose data security requirements. However, it does establish a right of action for certain data breaches that result from violations of a business's duty to implement and maintain reasonable security practices and procedures appropriate to the risk arising from existing California law

- Anonymized, pseudonymous or de-identified, and aggregated data
  - Anonymous data is not considered personal data.
  - The CCPA does not restrict the ability to collect, use, retain, sell, or disclose a information that is de-identified or aggregated. However, it establishes a high bar for claiming data is de-identified.
  - CCPA does not clearly categorize or exclude pseudonymous data.

- Enforcement

  Consumers may seek the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Courts may also impose injunctive or declaratory relief.

  The California AG may bring actions for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional.

  However, the CCPA also grants businesses a 30-day cure period for noticed violations

CCPA - Amendments

- 17 amendments submitted
- 7 amendments passed California Senate Committee on the Judiciary.
  - EMPLOYEE EXEMPTION: AB 25 changes the CCPA so that the law does not cover collection of personal information from job applicants, employees, business owners, directors, officers, medical staff, or contractors.

    What's New? The Senate Committee weakened the employee exception by sun-setting the exemption on January 1, 2021, and negating the exemption with regard to the CCPA's notice and data breach liability provisions.
  - DATA BROKER REGISTRATION: AB 1202 requires data brokers to register with the California Attorney General.

    What's New? The amendment dropped language that would have provided consumers the right to opt-out of the sale of their personal information by data brokers.
  - PUBLICLY AVAILABLE INFORMATION: AB 874 streamlines the definition of "publicly available" to mean information that is lawfully made available from federal, state, or local government records. The bill also seeks to amend the definition of "personal information" to explicitly exclude de-identified or aggregate consumer information.
- Included in the amendments that failed to pass out of committee
  - SB 561, a bill that would have expanded the private right of action to permit consumers to sue for any violations of the CCPA. It also eliminated the 30-day cure period.

Trending privacy issues

- Facial recognition
  - Bans in San Francisco, Oakland, and Somerville MA
  - San Francisco banned the use of facial recognition by police and city agencies. Somerville is modelled after SF.
  - City of Oakland – banned from "acquiring, obtaining, retaining, requesting, or accessing" facial recognition technology
- Geolocation data
  - HB 702
  - New York City – bill in committee

    Prohibits telecommunications carriers and mobile applications from sharing a user's location data with another person, if the location is within NYC. Penalty of $1,000 per violation, with a maximum penalty of $10,000 per day per person. The Dept. of Information Technology and Telecommunications would enforce. This bill also creates a private right of action against telecommunications carriers and mobile application developers.
  - California AB 523 – Passed Assembly, passed Senate Judiciary Committee

    Requires telecoms to receive express consent from their customers before sharing real-time data to third parties.
  - Federal S. 142 proposed American Data Dissemination (ADD) Act by Mark Rubio. Requires FTC to extends Privacy Act requirements to ISPs.
- Data Brokers

  Vermont - requires all businesses that trade data on Vermont residents to register publicly and share basic information about how they operate.

  California - AB 1202 requires data brokers to register with the California Attorney General.
- Internet of Things

  Proposed S. 734 - IoT Cybersecurity Improvement Act of 2019
  Directs NIST to establish standards for "covered devices". Directs OMB to reflect the standards in procurement.