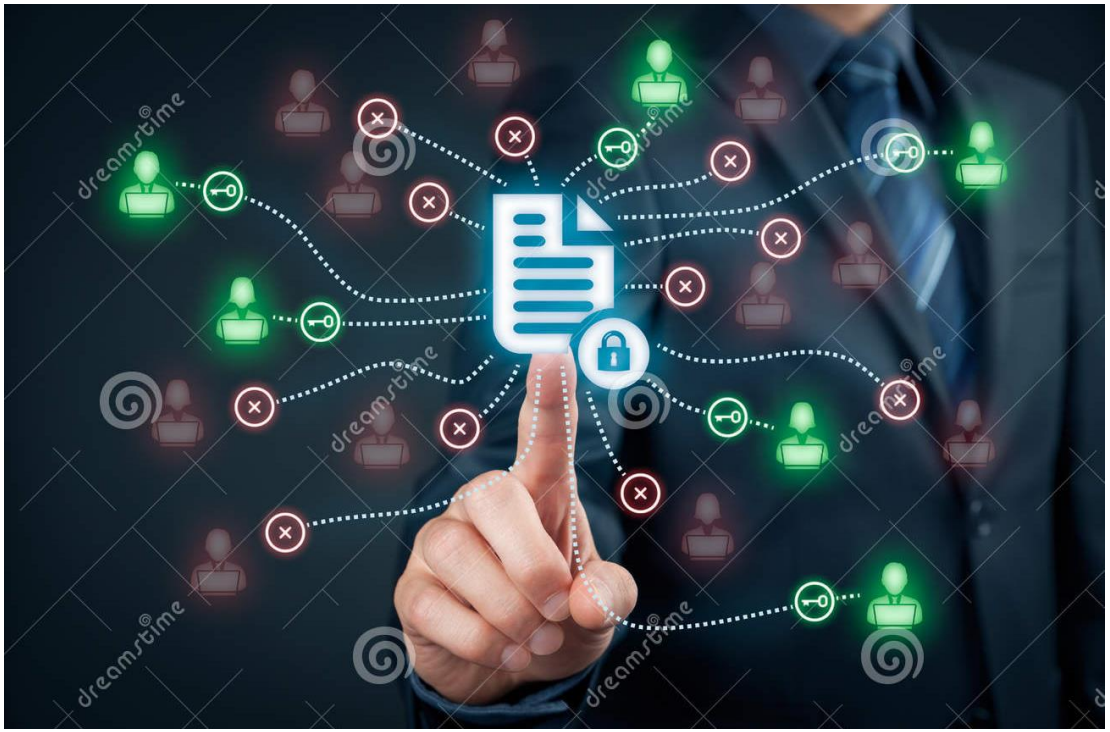
PROGRAM MATERIALS
Program #2997
May 28, 2019

Get Your Privacy House in Order

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

BakerHostetler



Get Your Privacy House in Order

Building an Adaptable Privacy Program in an Uncertain Legal Environment

March 27, 2019

Presenters

Shea Leitch
Seattle
sleitch@bakerlaw.com
206.566.7106

Agenda

I. **Uncertain Legal Landscape**

II. **Overview of Current Legal Terrain**

- US Privacy Law
- Foreign Privacy Law

III. **Covered Information & Key Concepts**

IV. **Laws Applicable to Advertising**

V. **Practical Considerations For Privacy-Complaint Processing**

VI. **Conclusion/Questions**

Uncertain Legal Landscape

State Privacy Legislation

Washington Privacy Act died in Committee in the Washington House of Representatives after nearly unanimous passage in the Senate

…BUT California continues to consider amendments to the CCPA…

California Legislation Still Under Consideration

- AB 25
- AB 874
- SB 561
- AB 846
- AB 873
- AB 981
- AB 1035
- ~~AB 288~~
- ~~AB 1138~~

CCPA Attorney General Regulations

BakerHostetler

- California Attorney General will issue regulations regarding:
  - Whether employees and other individuals who are not customers should be considered "consumers" under the CCPA
  - How the term "household" should be defined and interpreted
  - Whether the $25 million threshold for CCPA application applies to California revenue only, or a company's total revenue
  - The meaning and scope of certain terms
  - How consumer rights should be executed, in practice
  - The scope of the CCPA's exceptions

Other Legislation?

Privacy legislation has been proposed in these states just this year!

- **Arizona, Hawaii, Illinois, Maryland, Massachusetts, Mississippi, Nevada, New Jersey, New Mexico, New York, North Dakota, Rhode Island, Texas, and Virginia**

Federal omnibus privacy legislation has been proposed as well.

Overview of the Current Legal Terrain

US and Abroad

US Privacy Law

- **Sectoral approach**
  - No GDPR-style “omnibus” privacy laws (yet)
  - CCPA sparked consideration of federal legislation
- **Federal Law**
  - Sector- or audience-specific laws (TCPA, CAN-SPAM, COPPA, GLBA, HIPAA, ECPA, FCRA, VPPA, etc.)
  - FTC uses Section V authority to regulate privacy and data security
- **State Law**
  - Data security breach notification laws in all 50 states
  - Other state-specific laws
    - NYDFS Cybersecurity Regulation
    - MA security requirements
    - IL biometric laws
    - CA “Shine the Light”
  - 15+ states considering CCPA-style laws

Foreign Privacy Law

- Obligations vary by jurisdiction
  - Scope and extraterritoriality
  - Penalties
  - Breach notification requirements
  - Enforcement risk
- EU
  - General Data Protection Regulation (GDPR)
- Canada
  - Personal Information Protection and Electronic Documents Act (PIPEDA), CASL, etc.
  - Other province-specific obligations

Covered Information & Key Concepts

“Personal Information” or “Personal Data”

BakerHostetler

- All relevant laws protect some form of ***personal data***, ***personal information***, or ***personally identifiable information (PII)***
  - Varying definitions among legal regimes

- Most privacy-related laws have special definitions of and/or protection obligations for ***sensitive data*** or ***special categories*** of data
  - Typically health information, race, religion, sexual orientation, etc.

"Personal Information" or "PII" (US)

- Personal Information
  - Breach law definitions vary by state, in most breach notification laws, name +
    - SSN;
    - Driver's license; or
    - Financial account number if paired with sufficient information to access funds in the account
    - Some states are more expansive
- Personally Identifiable Information (PII)
  - Generally refers to:
    - Information used to distinguish or trace an individual's identity, such as name, SSN, DOB, mother's maiden name, or biometric records
    - Any other information that is linked or linkable to an individual
    - CA AG has stated mobile device identifiers are PII
- Other variations
  - "Personal Information" under COPPA
  - Protected Health Information (PHI) (HIPAA)
  - Nonpublic Personal Information (NPI) (GLBA)

CCPA Personal Information

- The definition of personal information under the CCPA is very broad and includes:
  - Name, alias, unique identifier, IP address, email address, account name, SSN, driver's license number, passport number, or other similar identifiers
  - "personal information" as defined in the California data breach notification statute
  - Protected characteristics under California or federal law
  - Commercial information such as records of property, products or services purchased, obtained, considered, or purchasing or consuming histories or tendencies
  - Biometric information
  - Internet or other electronic network activity information
  - Geolocation data
  - Audio, electronic, visual, thermal, olfactory, or similar information
  - Professional or employment related information
  - Education information
  - Inferences drawn from any of the information above

"Personal Data" (EU)

- GDPR
  - "Personal Data"
    - *"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (Art. 4)
    - ***Broader*** definition than most US laws
      - Includes data elements such as IP address and names alone
  - "Special Categories"
    - *"Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"* (Art. 9)
    - Processing is restricted; may require additional safeguards

Information Not Covered

- In almost all regimes – US and abroad – ***nonpersonal***, ***aggregated***, and/or ***anonymized data*** is not subject to applicable privacy laws and regulations
  - Anonymization vs. pseudonymization
  - Must not be linkable to any individual person
- Examples
  - Aggregate numerical statistics on website visits (10,294 views on X day)
  - Survey results

Privacy Laws Applicable to Advertising

US Laws and Regulations

Telephone Consumer Protection Act (TCPA)

- Companies that contact consumers via telephone, text, or fax must comply with the Telephone Consumer Protection Act (TCPA)
- The TCPA places a number of detailed restrictions on the following types of communications
  - Autodialed calls and text messages
  - Telemarketing calls and text messages
  - Artificial or prerecorded calls
  - Unsolicited fax advertisements
- Individuals who receive unwanted calls/texts/faxes may file lawsuits, including class actions, for TCPA violations
  - May recover damages of $500 per violating call or text (and up to $1,500 per willful or knowing violation)

CAN-SPAM Act

- Sets out rules and requirements for commercial emails
  - Provide means for opting out and honor opt-out requests within 10 days
  - No false or misleading headers or subject lines
  - Other requirements
- US has opt-out regime; Canada's CASL is opt-in
- ***Takeaway:*** check email promotions and solicitations against CAN-SPAM requirements and ensure adequate opt-out mechanisms

Children's Online Privacy Protection Act (COPPA)

BakerHostetler

- Imposes requirements on websites or online services directed to children under 13
  - Parental notice explaining data practices
  - Requires parental consent to collect children's PI (with limited exceptions)
- Applies to operators that have actual knowledge that they are collecting PI from a child under 13
- Enforcement bodies
  - FTC
  - State AGs
- ***Takeaway:*** Consider whether the company may have knowledge that children are providing personal information on a website (for example, if full DOB is collected, company will be deemed to have actual knowledge)

California-Specific Laws

- ***"Shine the Light"***
  - Applies if sharing PI with third parties for their own marketing purposes
- ***CalOPPA***
  - Key requirement: commercial websites or online services must post privacy policy
- ***CCPA***
  - Comprehensive privacy law similar to GDPR, set to take effect January 1, 2020
- California laws often set the floor
  - May apply only to CA residents, but can be difficult to segregate by state

FTC Oversight

- Primary federal agency for oversight of privacy and data security issues
  - Enforces pursuant to Section V authority to regulate unfair or deceptive trade practices
- Issues reports and guidance for industry
- May link Section V authority to statutory violations with civil penalties
  - Ex: COPPA, FCRA, CAN-SPAM all have statutory penalties

Industry Standards

- Industry standards and best practices may apply
  - Payment Card Industry Data Security Standard (PCI-DSS)
    - Security standard applicable to processing of payment card data
  - ISO/IEC 27000 Standards
    - Information security program certification
  - NAI/DAA Requirements

Privacy Laws Applicable to Advertising

Foreign Laws and Regulations

General Data Protection Regulation (GDPR)

BakerHostetler

- Broad jurisdictional scope, applies to organizations that:
  - Are “established” in the EU;
  - Process personal data of EU “data subjects” when offering them goods or services (whether or not for payment); or
  - Monitor behavior occurring in the EU
- Numerous consumer-focused obligations
  - Broad definition of personal data
  - Transparency in collection and use of data
  - Assurances of security and transparency with third parties
  - Data subject rights over personal data held by organizations
- Max fine: greater of €20 million or 4% of worldwide annual turnover

Other Non-US Regimes

- PIPEDA
  - Broad privacy legislation, similar to GDPR
  - Definition of “personal information” is broadly defined as information about an identifiable information
  - Sets notice standards and rules for when consent is required
  - Imposes individual and regulatory data breach requirement
- Varied international landscape
  - Privacy laws already in force elsewhere, in many forms
    - Including breach notification laws
  - Many slated to implement regimes similar to GDPR
    - Ex: Brazil’s LGPD
- Data localization laws may impact business practices

Practical Considerations for Privacy-Compliant Processing

Data Flows

- Foundation of a good privacy program is knowing:
  - What personal information you are ***collecting***, and how you're collecting it
  - How you are ***using*** it
  - How you are ***sharing*** it
  - How long you are ***retaining*** it
- Some organizations engage vendors to "map" data flows, especially if complex
- Identify privacy laws and regulations applicable to relevant data flows

Consumer-Facing Notices

- Ensure consumers are given appropriate notice ***before*** they provide information
  - Website privacy policies
  - Just-in-time notices (e.g. geolocation)
- GDPR generally requires more robust notice
- CCPA adds notice requirements as well
- Identify populations requiring special notice
  - EU or other countries
  - Children (also teenagers between 13 and 16)
  - CA residents
- Key principle: transparency

Consumer Consent

- Often, notices and/or requests for consent must be framed in a particular way
  - Ex: GDPR requires specific, informed, uncoerced, unambiguous consent
- Opt-in vs. Opt-out
  - US: generally consumers opt out of marketing communications, but business must provide opportunities to do so
    - Exceptions: TCPA, CCPA requirements
  - EU: GDPR generally requires opt-in consent to use personal data for marketing activities
- Processing of sensitive and/or “special categories” of data may trigger heightened requirements
  - FTC released guidance defining data sensitivity
  - GDPR: “explicit consent”
- Key principle: (also) transparency

Uses of Consumer Data

- Best practices
  - Only use personal information for purpose(s) ***reasonably anticipated*** by the consumer
  - ***Data minimization***
- Under GDPR, more narrow interpretation
  - Generally must state each purpose explicitly before collecting/processing
  - Counterexample: Facebook providing user data to Cambridge Analytica
- Ensure each use of data has a definite purpose and/or legal basis
  - GDPR sets out 6 “lawful bases” for processing
    - Ex: legal obligation, consent, legitimate interest
- CCPA do not sell ELABORATE

Third-Party Relationships

- In general, laws apply based upon activities
  1. Entities determining "purposes and means" of processing
     - GDPR: "***controllers***"
  2. Vendors/service providers following instructions
     - GDPR: "***processors***"
- Some laws require certain security and conduct assurances between parties sharing personal information
  - GDPR Article 28
  - CCPA (when effective)
  - May also be contractual obligations
- Overseas transfers may trigger further obligations
  - Consider service providers located in foreign countries

Information Security

- Best practices
  - Adherence to ***industry standard*** (e.g. ISO 27000)
  - Implement measures proportional to ***sensitivity*** of data

- Many privacy laws contain vague requirements for adequate security
  - GDPR: Must take into account *"the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" and "ensure a level of security appropriate to the risk"*
  - CCPA: Businesses can be penalized for not maintaining *"reasonable security procedures and practices appropriate to the nature of the [nonencrypted or nonredacted personal] information"*

Data Retention

- Best practice
  - Do not retain data for longer than needed to ***achieve purpose for which it was collected***
  - Implement ***data retention policy*** addressing types of data collected
- Currently, GDPR has most stringent requirements
  - Do not retain identifiable data for longer than needed for purpose(s) for which data was processed (Art. 5)

Recordkeeping and Privacy Impact Assessments

BakerHostetler

- Best practices
  - Ensure regular recordkeeping and documentation
    - Data flows
    - Third-party obligations
    - Security incidents
    - Data subject communications and opt-outs
  - Conduct privacy impact assessments
- GDPR-specific obligations
  - Comprehensive Article 30 recordkeeping
  - Data protection impact assessments (DPIA)
  - “Privacy by Design” for new processing activities

Children's Privacy

- Identify activities or services that may involve the collection of children's personal information
- Often, special notices and consents required
  - COPPA (13 or younger)
  - GDPR (tiered approach, thresholds between 13 and 16 years)
  - Consider necessity of parental consent
  - CCPA ages – bill in congress that would raise the age for coppa

Consumer Rights

- CCPA is the first statute to require broad consumer rights
  - Notice
  - Access
  - Deletion
  - Do-Not-Sell
- EU's GDPR gives data subjects numerous rights
  - Access/disclosure
  - Deletion ("right to be forgotten")
  - Objection
  - Rectification
  - Restriction
  - Portability

Questions?

BakerHostetler

Atlanta
Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Philadelphia
Seattle
Washington, DC

bakerlaw.com