WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

The Intersection of Big Data and New State Privacy Laws

OCTOBER 1, 2021

Arianna Evers
Special Counsel, WilmerHale

Ali Jessani
Associate, WilmerHale

Adam Huff
Managing Counsel, Privacy and Security Legal
Oracle

Overview

- Introduction to Big Data
- Review of California, Virginia, and Colorado privacy laws
- Some challenges for Big Data
- Privacy by design and key questions for building a compliance program
- Parting thoughts

Introduction to Big Data

What is Big Data?

- Big Data refers to “a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions.” (FTC)
- Entities collecting and using big data want as much data as possible to use as the basis for models that can be used to explain, predict, and affect behavior.

Balancing Risks and Benefits

Pros:

- Can be used for good
- Increased efficiencies and insights for businesses and consumers

Cons:

- Use of personal information raises privacy concerns
- Potential to perpetuate existing disparities or exclude consumers from benefits
- Building effective compliance programs can be tricky!

Big Data and State Privacy Laws

- Most big data sets include personal information, which will trigger the requirements of various state laws, including the big three—CCPA/CPRA, Virginia, Colorado
- Requirements are not always consistent with one another
- Large data sets can be difficult to de-identify and even harder to fully anonymize
- Regulations have not yet passed, and more state laws could be on the horizon
- Need to be aware of what the legal issues are, what the risks and opportunities may be, and how best to think about privacy related obligations for your program where the law is in still developing

State Comprehensive Privacy Laws

Overview of Evolving US Privacy Landscape

- Historically, the US has taken a sectoral approach to privacy (e.g., HIPAA for PHI, GLBA for financial information, COPPA for online children's data)
- States are now looking to pass comprehensive privacy legislation (similar to the GDPR in the EU); these laws implicate big data processing
- California was the first of these states in 2018; has since been joined by Virginia and Colorado
- Numerous other states are considering comprehensive privacy legislation during every legislative session, including New York and Washington
- Could inspire Congress to pass a federal privacy bill
  - Current sticking points: federal pre-emption and private right of action

California Consumer Privacy Act

- First comprehensive privacy law in the United States
- Similar to GDPR but different in key ways
- Passed in 2018 and went into effect January 2020
- Mostly enforceable by the California AG for fines up to $7,500 per violation
- Enforcement began in July 2020
- Private right of action for certain data breaches (up to $750 per violation)

California Consumer Privacy Act (cont.)

- Applies to “businesses” and “service providers”
- Protects the “personal information” of California residents
- Does contain broad exemptions for information regulated under federal laws, as well as B2B and employee data
- Creates individual rights (e.g., right to delete, right to access)
- Requires businesses to provide right to opt out of sale
- Creates notice and contractual requirements for businesses
- Businesses have a “right to cure”

Overview of New US State Privacy Laws

- California Privacy Rights Act (CPRA)
  - Passed by ballot initiative in November 2020
  - Most provisions go into effect January 1, 2023
  - Expands and eventually replaces the CCPA
- Virginia's Consumer Data Protection Act (CDPA)
  - Voted into law February of 2021
  - Goes into effect January 1, 2023
- Colorado Privacy Act (CPA)
  - Voted into law June of 2021
  - Most of the law goes into effect July 1, 2023

Overview of CPRA

- Comprehensive privacy law that builds upon the CCPA and brings it more in line with the GDPR
- Passed through ballot initiative in November 2020
- The new requirements for businesses go into effect January 1, 2023 and apply to personal information businesses collect after January 1, 2022
- Creates a new agency (the California Privacy Protection Agency) that will be responsible for rulemaking and enforcement of the law

CPRA (cont.)

- Creates a new category of “sensitive personal information” and new rights associated with this data
- Creates a new “contractor” category
- Consumers now have a right to rectify
- Creates new notice and contractual requirements for businesses
- Implements data retention and data security requirements

Virginia's Consumer Data Protection Act and Colorado Privacy Act

- Passed through the normal legislative process
- Both are modeled more after the GDPR than the CCPA
- Exempt broad categories of data (broader than the CCPA/CPRA)
- Enforceable by AGs (Colorado is also enforceable by district attorneys)

Virginia's Consumer Data Protection Act and Colorado Privacy Act (cont.)

- Require businesses (controllers) to:
  - Provide residents with individual rights (including a right to opt out of certain processing activities)
  - Provide residents with notice of their data processing activities
  - Obtain consent prior to processing sensitive data
  - Implement data processing agreements with processors
  - Conduct data protection impact assessments for certain processing activities (including targeted advertising)
  - Implement privacy by design principles (data minimization, purpose limitation, etc.)

Challenges for Big Data

Personal Information/Data

- Enumerated definition (CPRA) versus conceptual approach (CO/VA)
- “Reasonable basis” to believe personal data is made public
- Limits on use and disclosure of sensitive personal information in CA, versus opt-in
- B2B and employee exemptions expire and are narrow in CA
- Entity-wide exemptions for HIPAA (VA) and GLBA data (VA/CO)
- De-identification requires (1) measures to prevent association, (2) public commitment, and (3) contractual commitments
- Data mapping is critical – what are you getting, where is it coming from, how is it being used, and where is it going?
  - Essential questions for a privacy by design program
- What other laws and regulations – if any – apply to the data?

Data Subject Access Rights

- Certain rights (e.g., know and access, deletion, portability, correction) appear across the state laws, suggesting they may represent a new baseline
- Rights to opt out for:
  - CA: (1) sale or sharing, and (2) sensitive personal information
  - CO/VA: (1) targeted advertising, (2) sale of personal data, and (3) profiling that produces legal or similarly significant effects
- Children – under 13 (CO/VA) versus under 16 (CA)
- How do you approach rights for data of individuals residing in other jurisdictions?
- User friendly interfaces and packaging for rights administration are important and reduce regulatory risk
- Balancing look back periods and data minimization

Data Protection Assessments

- Colorado and VA introduce Data Protection Assessments (DPAs)
- Required for processing that "presents a heightened risk of harm to a consumer"
  - Targeted advertising or profiling that presents reasonably foreseeable risks
  - Selling personal data
  - Processing sensitive data
- Balancing of risks and benefits, as mitigated by safeguards
- Must make available to Attorney General upon request
- DPAs can help reduce risks and identify opportunities, including through data minimization
- Consider conducting DPAs more broadly

Service Provider Relationships

- California, Virginia, and Colorado all require contracts with service providers/processors
  - CPRA also creates a new contractor category
- Understanding your data flow will help you assess your various relationships with other businesses in relation to these laws
- Questions to ask:
  - Does this contract implicate data regulated by these laws?
  - Is any data being transferred from one party to another (such that it could constitute a sale)?
  - Does the contract limit what my businesses or a third-party can do with the data?
  - Am I meeting the relevant DPA requirements?

Privacy By Design

Privacy By Design

Potential Components (no one size fits all approach)

- Cross-functional comprehensive information-security and privacy review
  - Understand what data is involved and what security features are present to protect the data
    - Are they commensurate?
- Review of data flows and data use for new products and services
  - Understand business objective and ask some key questions
    - Can the data be de-identified (if not already)?
    - Can less data be used?
    - Is the data ”sensitive”?
    - Is the use in-line with the privacy policy?

Privacy By Design

Potential Components (no one size fits all approach)

- Global Privacy Program
  - Lines of business provide at least yearly updates on data use, products and services
  - Embedded privacy professionals in each LOB
  - Reviews conducted by privacy legal teams
- Audit
  - Dedicated neutral audit professionals
  - Review data use and areas of greatest risk
  - Make suggestions for improvements

Key Questions

Data format and type

- Is the data structured or unstructured?
- Does the data set include any personal information? If yes, what kinds of personal information are included in the data set?
- Does the data set contain sensitive personal information, for example, health information, financial information, or precise location?
- Does the data set include demographic information, such as gender, age, or race?
- Does the data set include information collected from children under 13? Children under 16?
- Does the data set include any information that relates to creditworthiness, credit standing, or credit capacity, such as defaults, income, credit scores, etc.?

Key Questions

Data collection

- How was the data set obtained? Is it all first party day, or does some of it come from third-party sources?
- Does the entity compiling the data and doing the analytics have a direct relationship with the consumer?
- Were APIs or web scraping used to obtain any of the information?

Key Questions

Contractual and Other Restrictions

- Is the data use consistent with material promises made to consumers?
- Were consumers provided sufficient information about relevant data practices?
- Are reasonable measures being undertaken to know the purposes for which downstream users are using the data?
- If a third party is providing the data, does the agreement with the third party place any restrictions on the use of the data?

Key Questions

Other Questions

- Do you have reasonable safeguards in place to protect consumer information that are commensurate with the amount and sensitivity of the data at issue, the size and complexity of the company's operations, and the cost of available security measures?
- Have you reviewed your data sets and algorithms to ensure that hidden biases are not having an unintended impact on certain populations?

Key Questions

Other Questions

- Have you confirmed the accuracy of your predictions based on big data
- Have you considered whether fairness and ethical considerations advise against using big data in certain circumstances?
- Is there a corporate policy/position on the data use, and is the proposed use consistent with that policy/position?
  - Should there be one?

Parting Thoughts

Parting Thoughts

- Shifting regulatory environment requires thoughtful analysis of evolving legal structures
- Being proactive and anticipating where the law is going can help reduce necessary changes down the road
- Need to think beyond formal structures and pay attention to ethics and best practices—especially true for companies in industries where the risks to consumers are particularly high
  - Try not to be an outlier with data practices
- Think about potential oversight; not just regulators, but media, plaintiffs' attorneys, consumers
- Transparency and accountability are important
- Make sure you understand your company's data program: what data do you have, what do you actually need, what are you doing with it, and how are you using it, who are you sharing it with, what controls do you have on third party use of the data

Questions + Contact

Arianna Evers
Arianna.Evers@wilmerhale.com

Adam Huff
Adam.huff@oracle.com

Ali Jessani
Ali.Jessani@wilmerhale.com