Privacy Shakeup: The Double Trouble of the GDPR and the California Consumer Privacy Act

William R. Denny
Secure Delaware Workshop
October 31, 2018
What Is Data Privacy?
Data Privacy – Then and Now

U.S. newspapers regularly shared personal information of individuals up until the:

a) 1920s  
b) 1940s  
c) 1960s  
d) 1980s
Answer: c) 1960s

- Until the 1960s, U.S. newspapers regularly shared personal information about people infected with diseases.

- By the 1970s, the advent of large databases of medical records brought privacy concerns to the forefront, along with new caution about sharing health details.

- Technological advances have introduced novel and more intrusive data collection.
1993 – It’s all about data!

(Originally published on October 18, 1993 in the Seattle Post - by Steve Greenberg)
Every time you pick up the phone, dial a number, write an e-mail, make a purchase, travel on the bus carrying a cell phone, swipe a card somewhere, you leave a trace, and the Government has decided that it's good idea to collect it all, everything, even if you've never been suspected of doing a crime.

– Edward Snowden
Rapid Increase in Data Collection

Technology continues to evolve and develop at a rapid pace

- The volume and type of data collected and developed is dramatically increasing.

- Following are just a few examples of technology developments generating data:
  - The Internet of Things
  - Artificial Intelligence
  - Data Tools and Management
Why is Data Privacy Important?

- We create 2,500,000 terabytes of data per day
  - 90 years of HD video
  - 250,000 Libraries of Congress
- 3.8 billion internet users in 2017
- 90% of all data has been created within the last 2 years
Important Distinction

- **Differing Values of Sensitive Personal Information**
  - **United States**: Social security number, financial information, driver’s license number, medical records
  - **Europe**: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, criminal convictions or offenses
Recent Approach to Data Privacy in the U.S.

- State Law Patchwork
  - Data Breach Notification Laws in 50 states
  - Multiple state data security laws
  - Numerous state laws dealing with privacy

- Federal FTC Enforcement Actions and Sector-specific Laws
  - HIPAA/HITECH (healthcare)
  - GLBA (financial services)
  - COPPA (children’s online privacy)
  - FERPA (student information)
  - TCPA (telecommunications, etc.)
2018 – A Watershed Year in Data Privacy
General Data Protection Regulation (GDPR)

- EU data privacy law became enforceable May 25, 2018
  - Gives control back to citizens and residents over their personal data
  - Addresses the export of personal data from the EU
  - **Data protection** is further established as a fundamental right
  - Much broader definition to **personal data**
  - Heavy penalties for violation
Who Must Comply with the GDPR?

- It applies to companies with a branch, office, subsidiary or other establishment in the EU that collects, receives, transmits, uses, stores or otherwise processes personal data.

- It applies to U.S.-based companies if they process personal data as part of
  - The offering of goods or services to, or
  - The monitoring of the behavior of data subjects in the EU.
Key Concepts under GDPR

- **Personal data** means any information related to an identified or identifiable natural person.
  
  - Name, ID number, location data, online identifiers such as **IP addresses**, **cookie identifiers**, radio frequency identification
  
  - Any factor specific to **physical, physiological, genetic, mental, economic, cultural or social identity** of a natural person.
  
  - **Special categories** include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and data concerning health, sex life, sexual orientation
Key Concepts under GDPR (Cont.)

- **Processing** means any operation that is performed on personal data.

- Different obligations for **Controllers and Processors**
  - **Controller** determines the purposes and means of processing the personal data.
  - **Processor** processes personal data on behalf of the controller.
What Rules Must a Company Follow?

Short answer: Keep a lid on customer data.
Longer Answer:

Complex Series of Rules
Obligations of Controllers under GDPR

- Principles applicable to processing personal data:
  - Lawful Basis for Processing
  - Collected for specified, explicit and legitimate purposes
  - Limited to what is necessary in relation to the purpose
  - Accurate and kept up to date
  - Kept no longer than necessary for purpose
  - Secured against unauthorized disclosure or damage
  - Controller must be able to **demonstrate** compliance
Obligations of Controllers under GDPR (Cont.)

- **Individuals’ rights**
  - Transparent information and modalities for exercising rights
  - Information and access to personal data
  - Rectification and erasure
  - Data portability

- **Accountability**
  - Records of processing activities
  - Data protection officer
  - Data protection impact assessment
  - Data protection by design and by default
  - Designated representatives
Obligations of Processors under GDPR

- Direct obligations
  - Data security
  - Data breach notification
  - Following controller’s instructions
  - Contractual relationships
  - Sub-processing
  - Designated representatives
  - Record-keeping
  - Data protection officer
Transfer of EU Personal Data Out of EU

- Significant restrictions on countries, like the U.S., that are deemed not to have an **adequate level of protection**.

- Options for U.S. companies to demonstrate adequate assurances of data protection:
  - EU-U.S. Privacy Shield
  - Standard Contractual Clauses
  - Binding Corporate Rules
  - Codes of Conduct and Certification
How can Organizations Prepare for the GDPR?

- Understand **what** data you collect, process and store.
  - The purpose for the collection
  - Whether the collection is minimized to meet only that purpose
  - Whether you are collecting any of the various types of sensitive data

- Understand **how** the data is being processed and stored.
  - Lawful basis
  - Data protection measures
  - Location of stored data
  - Period of retention
  - How and where records of processing and storage are kept
How can Organizations Prepare for the GDPR?

- Evaluate how you transfer and share data
- Review contractual relationships with processors
- Put together a plan to bring yourself into compliance
  - Specific training needs
  - Data management procedures (storage, processing, data breaches)
  - Responding to requests from data subjects
  - Record-keeping
  - Revise privacy notices
California Consumer Privacy Act of 2018

- Signed into law on June 28, 2018, a few days after it was introduced to the California legislature.

- Why so fast?
  - To head off a ballot initiative
  - Public attention on privacy issues
    - Cambridge Analytica
    - Data Breaches (Equifax, Yahoo, Under Armour, Facebook)
    - GDPR

- Effective earlier of 6 months after AG rules or July 1, 2020.
Who Must Comply With the CCPA?

- Applies to any **business** that **collects or sells personal information** from or about **consumers**.

- **Business**: “A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners” that:
  - Has gross annual revenues in excess of $25 Million; or
  - Annually buys, sells, receives or shares for commercial purposes personal information of 50K or more consumers, households or devices; or
  - Derives 50% or more of its annual income from selling consumers’ personal information.
Broad Definition of Personal Information

- **Personal Information**: Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - **The Basics**: Name, contact information, IP address, biometric information, geolocation data, financial information, health information
  - **Also includes**:
    - Commercial information, including consuming history or tendencies
    - Internet and other electronic network activity information
    - Audio, electronic, visual, thermal, olfactory or similar information
    - Professional or employment-related information
    - Inferences drawn from any personal information
Who is a Consumer?

- Any California resident

- Includes:
  - Information collected inside or outside California unless every aspect of the commercial conduct relating to the consumer’s personal information takes place wholly outside of California.
  - Employees, students, tenants, customers
  - California residents who are temporarily living outside of California
Major Obligations of Businesses under the CCPA

1. To track consumer information from collection through disclosure or deletion

2. To create a system to promptly respond to and honor consumer requests
Consumer Rights

- CCPA establishes the following rights for consumers:
  - Right to know what is being collected
  - Right to know what is being sold or disclosed and to whom
  - Right to say no to the sale of personal information
  - Right to access
  - Right to delete
  - Right to equal service and price even if they exercise their rights

- 45 days to respond to consumer requests
  - Must be free of charge
  - Must cover the preceding 12-month period
Transparency and Disclosure

- CCPA requires disclosures and consumer-facing privacy policies to:
  - Inform consumers about rights
  - Identify categories of personal information collected and sold
  - Identify categories of third parties with whom personal information is shared
  - Identify financial incentives offered by the company
Liability for Violating CCPA

- Private Right of Action
  - Statutory remedy up to $7,500 per incident for intentional violation, up to $2,500 per incident for non-intentional.
  - Requirement of 30 day notice and cure period.
  - Expect Class Action Lawsuits

- Action by California Attorney General
2020 – What comes next?

- A National Privacy Law?
- CCPA in force along with a patchwork of state laws & sectorial regulations?
- Impact of GDPR enforcement?
- Impact of BREXIT?
- Cross border mechanisms?
A Federal Data Privacy Law?

- **Pressure points**
  - Multiple, inconsistent state and sectorial federal laws in the U.S.
  - GDPR’s broad reach changing business practices
  - CCPA forcing a radically different approach to privacy in the U.S.

- **Challenges**
  - Meeting the GDPR adequacy standard
  - Overcoming U.S. sectorial approach
  - Multiple congressional committees with overlapping jurisdiction
  - Substantive policy issues: private right of action, federal preemption
  - Conflicting interests between consumer groups and industry
  - Conflicting interests within the business community
First Steps to Compliance

- Focus on **outward-facing actions** that show intent to comply
  - Amend your privacy notice
  - Carefully select and monitor vendors
  - Use Data Transfer Agreement for cross-border transfers
  - Adequately respond to requests from individuals
  - Report data breaches to regulators within 72 hours

- Then turn to **internal steps** to compliance
Amend your Privacy Notice

- GDPR requires that companies provide detailed disclosures:
  - Identity and contact details of controller
  - Purposes of the processing
  - Legal basis for the processing
  - Legitimate interests
  - Recipients or categories of recipients
  - Cross border transfers
Amend your Privacy Notice

- **GDPR** requires that companies:
  - Be *transparent* about how they handle data
  - Provide *detailed disclosures*
  - Use the right "*legal basis*" for processing the data

- **CCPA** requires that companies provide even more rights!
  - More specific disclosure and communication requirements
  - Broader definition of personal information
  - Greater rights to restrict sale of personal information
  - Opt out v. opt in
Amend your Privacy Notice

– Detailed disclosures required under GDPR:
  • Identity and contact details of controller
  • Purposes of the processing
  • Legal basis for the processing
  • Legitimate interests
  • Recipients or categories of recipients
  • Cross border transfers
  • Term of data retention
  • Existence of data subject rights (access, rectification, erasure)
  • Existence of automated decision making or profiling
  • Whether it is mandatory to provide information
  • Rights to withdraw consent and to lodge complaint with regulator
Amend your Privacy Notice

- Strict requirements for consent
  - Freely given
  - Specific
  - Informed
  - Unambiguous
  - Can be withdrawn at any time

- You must be able to prove that you got consent
Amend your Privacy Notice

- Create a Competitive Advantage!
  - Demonstrate competence in handling customer data
  - Provide clear policies that give control to customers
  - Build trust – create a positive value proposition
Carefully Select and Oversee Your Vendors

- GDPR requires that companies
  - Ensure that any third party provider that handles their personal data comply with GDPR requirements, and
  - Enter into a written agreement with them, containing specific provisions.

- How to start?
  - Collect and review all written agreements with providers that handle personal data of EU residents.
GDPR Requirements for Vendor Agreements

- Use only processors providing sufficient guarantees
- Specify:
  - subject matter and duration of processing,
  - nature and purpose of processing,
  - types of personal data and categories of data subjects,
  - Rights and obligations of the company
GDPR Requirements for Vendor Agreements

- Agreements must require:
  - Processing only per documented instructions
  - Confidentiality obligations
  - Appropriate technical and organizational measures
  - Assist controllers in complying with obligations
  - No subcontracting without authorization
  - Delete or return data at end of engagement
  - Provide information to demonstrate compliance
  - Approved mechanisms for transferring personal data from the EU
Resources

- FTC Protecting Small Businesses [https://www.ftc.gov/tips-advice/business-center/small-businesses](https://www.ftc.gov/tips-advice/business-center/small-businesses)
- Delaware Small Business Development Center - Datassured [https://delawaresbdc.org/special-programs/datassured/](https://delawaresbdc.org/special-programs/datassured/)
- Computer Incident Readiness Team (US-CERT) Resources for Small and Midsized Businesses [https://www.us-cert.gov/ccubedvp/smb](https://www.us-cert.gov/ccubedvp/smb)
To Contact Us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
P.O. Box 951
Wilmington, DE 19899-0951
www.potteranderson.com
Presenter: William R. Denny

- Partner and Chair of the Cybersecurity, Privacy and Data Governance Practice at Potter Anderson & Corroon LLP
- Certified Information Privacy Professional (CIPP/US)
- Member of the ABA Cyber Security Legal Task Force
- Licensed in Delaware