Privacy & Technology Update: Key Issues for the New Year

Speakers:

Michael Young, Partner

Paul Arne, Partner

Austin Mills, Partner

January 25, 2022

Agenda

- Comprehensive Rights-Based Privacy Laws
- EU – US Data Transfer
- Data Breach
- IP Protection for APIs
- Blockchain Legal Update

Comprehensive Rights-Based Privacy Laws

- California
- Virginia
- Colorado
- More on the way?

2022 is last year to prepare for 2023 effective date.

California Privacy Rights Act

Core Scope:

- Businesses that buy, sell, or share info on >100,000 California residents
- Joint ventures "composed" at least 40 percent of businesses
- Those who voluntarily certify
- Data brokers / companies with substantial revenue from data sales

Effective January 1, 2023

California Privacy Rights Act

- Express limitation on data use as “necessary and proportionate”
  - Notice as a *foundation* for data use
  - Limitation on data retention
  - Additional restrictions on sensitive information (SSN, financial account, precise geolocation data, racial/ethnic orientation, labor union affiliation, genetic, biometric, health)

California Privacy Rights Act

- Notice – new content (v. current CCPA standard)
  - Sensitive info practices
  - **Identify retention period**
  - Advertising disclosure

- New rights: correction, restrict sharing (for advertising), limit SPI use
- New twist on old rights: data deletion extended through supply chain

- **New Homepage Links**
  - Right to limit SPI processing
  - Right to opt out of selling *or sharing* of PI.

California Privacy Rights Act

- Process to implement new rights
  - Limit SPI use
  - Restrict sharing for advertising purposes
  - Correction rights (subject to “commercially reasonable” efforts)

- Required Contractual Content
  - Require legal compliance
  - Notice if can’t meet obligations
  - Rights to oversee processors (including right to stop processing)

- Update or Create Process/Procedural Documents

Virginia Consumer Data Protection Act

Core Scope

- "Controls or processes" personal data of 100,000 Virginia consumers
- Data brokers / companies with substantial revenue from data sales

Effective: January 1, 2023

Virginia Consumer Data Protection Act

- Principle of limited collection (limited to notice)
- Notice
  - CCPA-like: collection, processing, sharing, rights
  - (Unusual) “public commitment” regarding de-identified data

Virginia Consumer Data Protection Act

- Rights:
  - Access
  - Correction
  - Deletion
  - Portability
  - *Three kinds of opt-out*
  - *Right to appeal*

- Opt-outs for:
  - Targeted advertising (based on online behavior across sites)
  - (Monetary) sale of data
  - Profiling have legal or “significant effects”

Virginia Consumer Data Protection Act

- Rights to appeal non-action
  - Who decides? How independent? Additional evidence?
  - Response required in 60 days
  - Denied appeals must refer consumer to VA AG

Virginia Consumer Data Protection Act

Specific consent required to process sensitive data

“Sensitive data” includes personal data revealing “racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status”; genetic or biometric data used to identify a natural person; personal data collected from an individual known to be a child under the age of 13; and precise geolocation information identifying a person’s location within 1,750 feet.

Virginia Consumer Data Protection Act

- Required controller-processor contractual terms:
  - Confidentiality
  - Deletion or return
  - Demonstration of compliance and support for assessments
  - Subprocessing

Note: processors have independent obligation to limit processing

Virginia Consumer Data Protection Act

- Data Protection Assessments required to support:
  - Targeted advertising
  - Sales
  - Risky processing
  - Sensitive data processing

Colorado Privacy Act

Core Scope

- Controls or processes personal data of >100,000 Colorado consumers
- Data brokers / companies with substantial revenue from data sales
- Nonprofits in scope?

Effective: July 1, 2023

Colorado Privacy Act

Principle of Limited Data Use (consent for “secondary use”)

Rights: Access, portability, correction, deletion, three kinds of opt-out (similar to Virginia, but broader)

Appeals process must be provided

Notice: Must indicate rights available, make appeals process as easy as submitting a request

Contracting: Similar to Virginia (note express support for “reasonable” audits and inspections)

Consent required to process sensitive data

Data Protection Assessments for “risky” processing of data acquired after July 1, 2023

Recap

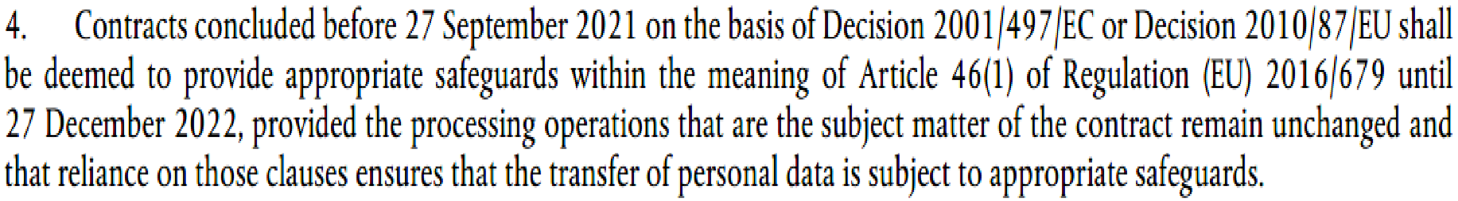
- Essential Tasks List:
  - Notice revision
  - Data mapping
  - Vendor contracts (required content)
  - Customer contracts for B2B
  - Data protection assessments
  - Rights response process
  - Data/process mapping (collection, sensitive info use, sharing, supply chain dependencies, c/p roles)

Other issues: “Reasonable” information security, other affirmative duties

EU-US Data Transfer

- *Schrems II* invalidated Privacy Shield
- EC approved new model clauses in June
- New clauses needed for (a) all new contracts and (b) existing contracts started December 27, 2022

From EC decision:



4. Contracts concluded before 27 September 2021 on the basis of Decision 2001/497/EC or Decision 2010/87/EU shall be deemed to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

Breach Risks

1. Direct / Indirect Business Interruption
2. Reputational
3. *<u>Class Actions / Statutory Damages</u>*
4. Other Financial Risks (recovery, mitigation, new procurement)

Average Monetary Cost of a Data Breach

$4,240,000	Average Cost of a Data Breach (↑10%)
$180	Average Cost per Record of PII (↑11%)
$4,620,000	Average Cost of a Ransomware Breach
$5,010,000	Average Cost of an Inbox Compromise
$5,650,000	Average Cost of a Data Breach at an Organization with High-Level Compliance Failures
$5,540,000	Average Cost of a Data Breach at an Organization with more than 80% of Employees Working Remotely
$401,000,000	Average Cost of a “Mega Breach” Impacting 50-65MM Records

Strategies for a Breach

1. **Limit data collection and retention**
2. Real data security (technical *and* administrative)
3. Contract strategy
4. Incident response plan
5. Retained professionals
6. Training / Tabletop
7. Cyberinsurance

IP Protection for APIs

- Two EHR systems can't talk to each other. If patient agrees, **can an EHR provider use APIs of the other EHR provider** to obtain patient data?
- Healthcare startup wants to use data from very large EHR provider. **Can the EHR provider require the startup to disclose its source code** as a condition to using the EHR provider's APIs?
- Open source software: Under the GPL, **does dynamic linking create a "combined work," requiring the whole combination to be licensed under the GPL?**
- FinTech startup wants to provide services to customers; needs customer data from bank account. **If customer agrees, can FinTech use bank's APIs**?

IP Protection for APIs

- Idea / Expression
  - Expression (§102(a)): Copyright subsists in original works of authorship fixed in a tangible medium of **expression**
  - Idea (§ 102(b)): Copyright protection does not extend to “any idea, procedure, process, system, **method of operation**, concept, principle, or discovery….”
- What happens if you have a **method of operation** that is **expressive**?
  - 1ST Cir. Lotus v. Borland: If both: not protected
  - 9th Cir. Oracle v. Google: If both: protected

IP Protection for APIs

- Fair Use
  - Standard
    - "[T]he fair use of a copyrighted work, … for purposes such as ***criticism, comment, news reporting, teaching …, scholarship, or research***, is not an infringement of copyright."
    - Four factors
    - Fact intensive
  - However:
    - "[E]very commercial use of copyrighted material is presumptively an unfair exploitation of the monopoly privilege that belongs to the owner of the copyright." *Sony Corp. v. Universal City Studios*, Inc., 646 U.S. 417, 451 (1984).

IP Protection for APIs

- Google v. Oracle: the perfect case
  - Only involved APIs
  - Both Idea/Expression and Fair Use were at issue
- Ruling:

Google’s use of APIs were FAIR USE

IP Protection for APIs

Case	On Appeal
Sony v. Universal–Fed. Dist.	Reversed
Sony v. Universal–Ct. App.	Reversed
Harper & Row–Fed. Dist.	Reversed
Harper & Row–Ct. App.	Reversed
Campbell–Fed. Dist.	Reversed
Campbell–Ct. App.	Reversed
Google v. Oracle–Fed. Dist.	Reversed
Google v. Oracle–Ct. App.	Reversed

Blockchain & Cryptocurrency

- U.S. Federal Law Updates
  - Infrastructure Investment and Jobs Act (Infrastructure Bill)
  - Sanctions Compliance Guidance for the Virtual Currency Industry (OFAC)
- General Uncertainty

Infrastructure Bill

- Infrastructure Investment and Jobs Act (Infrastructure Bill)
  - Brokers who deal in digital assets to report personal information of counterparties
    - Applies to both transactions and transfers
  - Broad definition of Broker

Sanctions Compliance Guidance

- Sanctions Compliance Guidance for the Virtual Currency Industry from The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)
  - Companies and providers (e.g. exchangers, administrators, miners, and wallet providers) to meet same standards as other tech providers
  - Screen transaction/identifying data to prevent transactions with sanctioned parties/jurisdictions

Thank you!

Michael Young
myoung@mmmlaw.com
404.495.8481

Paul Arne
pha@mmmlaw.com
404.504.7784

Austin Mills
amills@mmmlaw.com
404.495.8490