SQUIRE PATTON BOGGS

Why Data Privacy, Security and Asset Management is Crucial for Start-ups

Venture Law Meetup Webinar

June 28, 2021

Presenters

Tom Reems
Partner
+1 303 894 6110
thomas.reems@squirepb.com

Alan L. Friel
Partner
+1 213 689 6518
alan.friel@squirepb.com

Glenn Brown
Of Counsel
+1 470 898 4725
glenn.brown@squirepb.com

Special Thanks to Our Co-Sponsors

SQUIRE PATTON BOGGS
Venture Law Meetup

Discussion Topics

SQUIRE PATTON BOGGS
Venture Law Meetup

- Introduction
- Data Privacy & Security Laws in the US
- Data Limitations Require Management
- Data and M&A
- Operating a Data Management Program
- Takeaways
- Q&A


Privacy Laws in the US
squirepattonboggs.com

Historically Sectoral, or About Fair Notice and Reasonable Security

SQUIRE PATTON BOGGS

1. Industries with DPC laws:
   - Healthcare
   - Financial Institutions
   - Communications Providers
2. Specially Protected Activities
   - Collection from children online
   - Cable TV and video/content consumption
   - Communications
- Data Security and Breach Notification
- Deception and Unfair Practices

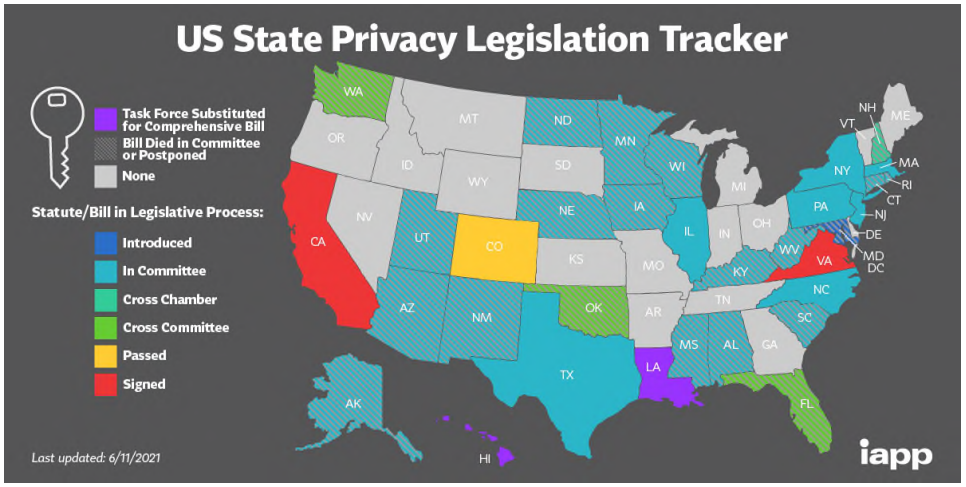
Gen 1 of State Laws – Still in Effect

SQUIRE PATTON BOGGS

1. Online Data Practices Notices
   - CA, NV, DE
   - DE includes B-to-B
- Applied to mobile apps
- Marketing practices:
  - Shine the Light (sharing)
  - CAN-SPAM (e-mail)
  - TCPA/TSR (telemarketing including text)
- Other
  - Wire tapping and non-consented recordings
  - Geo tracking

Overview and Trends

- EU/EEA Privacy Directive becomes the GDPR
- State law trend towards “horizontal” privacy laws
  - California Consumer Privacy Act (CCPA) – Effective since January 2020
  - California Privacy Rights Act (CPRA) – Most provisions effective January 2023
  - Virginia Consumer Data Protection Act (CDPA) – Effective January 2023
  - Colorado Privacy Act (CPA) – Effective July 1, 2023



Graphic from International Association of Privacy Professionals (IAPP)

California Consumer Privacy Act (CCPA)

SQUIRE PATTON BOGGS

- **Effective since January 2020**
- **Very broad definition of *personal information (PI)***
  - Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household
  - This includes not only obvious data like name, SSN, etc., but also pseudonymous identifiers like cookie IDs, IP addresses and mobile ad IDs
- **Expansive consumer rights**
  - Access, data portability, deletion, opt-out of sales, non-discrimination
- **Significant obligations**
  - Notification, vendor management, training, record keeping, etc.
- **Stiff penalties**
  - Up to $7,500 per violation
  - Private right of action and statutory damages for security incidents

CCPA Limitations + Repercussions

- **Limits on discrimination and financial incentives**
  - Must be reasonably related to the value of the consumer data
  - Opt-in, with ability to withdraw
  - Advance notice requirements, including valuation statement
- "**Global Privacy Control**"
  - Act grants authority to develop regulations to "facilitate and govern" opt-outs
  - Regulations require "user enabled privacy controls" to be a valid opt-out if:
    - Clearly communicate intent to opt-out;
    - If conflicts with opt-ins, including financial incentive programs, must notify and give choice
  - Attorney General endorses new browser controls
- **Enforcement**
  - Over 200 pending actions, including as to IBA cookies and "do not sell"
  - 30-day cure (for now)
  - Civil penalties, but no consumer lawsuits

California Privacy Rights Act (CPRA)

- **Effective Date = January 1, 2023**
  - Enforcement begins July 1, 2023
  - Certain provisions already effective (mainly related to rulemaking process and the new California Privacy Protection Agency)
- **Significant Changes to the CCPA**
  - Changes in thresholds for applicability
  - B2B and personnel carve outs will expire January 1, 2023
  - New consumer rights and business obligations
  - New obligations on “contractors”/service providers
  - Significantly more rulemaking and establishment of new privacy regulator – the California Privacy Protection Agency

New Rights Under the CPRA

SQUIRE PATTON BOGGS

- **Right to Correct**
  - Consumers have the right to request that a Business that maintains inaccurate PI about the Consumer correct such PI (details TBD in regulations)
- **Right to Opt Out of "Sharing"**
- **Rights Regarding "Automated Decision Making"**
  - New regulations will identify the rules governing access and opt-out rights with respect to automated decision-making technology
- **Right to Limit Disclosure and Use of "Sensitive Personal Information"**
  - What is Sensitive Personal Information (SPI)?
  - Consumers can limit use of SPI to:
    - That "which is necessary to perform the services or provide the goods reasonably expected by an average consumer"
    - To specific business purposes
    - As further authorized by CPRA regulations
  - SPI collected or processed "without the purpose of inferring characteristics about a consumer" is not subject to these rights

Virginia Consumer Data Protection Act (CDPA)

- **CCPA and GDPR inspired, but material differences**
- **Timeline**
  - Passed March 2, 2021
  - Findings of “working group” due November 1, 2021
  - Effective January 1, 2023
- **Data covered**
  - The scope of “personal data” is more narrow than the CPRA
- **More limited definition of “sale”**
- **No processing of “sensitive data” without consent**
- **Right to opt out of sales, “targeted advertising” and “profiling”**
- **No private right of action**
  - Enforced only by the Attorney General

Colorado Privacy Act

- Mishmash of CCPA, CPRA and CDPA
- Timeline
  - Passed June 8, 2021
  - Will become law if not vetoed by July 8
  - Effective July 1, 2023
- Data covered
  - The scope of “personal data” is narrower than the CPRA
- CA-style definition of “sale”
- No processing of “sensitive data” without consent (like VA)
- Right to opt out of sales, “targeted advertising” and “profiling” (like VA)
- No private right of action
  - Enforced only by the Attorney General or District Attorneys

New – Privacy Impact Assessments

CPRA:

- Where processing of ' PI presents "significant risk to consumers' privacy or security," CPRA requires the issuance of regulations requiring:
  - Annual cybersecurity audits; and
  - Privacy impact assessments

CDPA/CPA:

- A controller is required to conduct and document a data protection assessment of certain processing activities:
  - The processing of personal data for purposes of targeted advertising;
  - The sale of personal data;
  - Profiling that presents certain reasonably foreseeable risks;
  - The processing of sensitive data; and
  - Any processing activities involving personal data that present a heightened risk of harm to consumers.


Data Limitations Require Management
squirepattonboggs.com

Data Minimization & Purpose Limitations

- **CPRA introduces data minimization & purpose limitations provisions**
  - Data Minimization: Prohibit collecting additional categories of PI or using PI collected for additional purposes *that are incompatible with disclosed purpose for which the PI was collected*
  - Purpose Limitations: Collection, use, retention, and sharing of PI must be *reasonably necessary and proportionate* to achieve the purposes for which the PI was collected or processed, or for another disclosed purpose that is *compatible with context in which PI was collected*
- **Implications**
  - Limits a business' ability to make new use cases of PI and retain PI longer than necessary for express collection purpose
  - Practically requires PIAs, good data inventories, robust records retention program, and defensible destruction protocol

Data Governance has 3 Components

SQUIRE PATTON BOGGS

1. PRIVACY
2. Information Management
3. Data Security

Data Management has 5 elements

SQUIRE PATTON BOGGS

1. Governance
2. Transparency and Choice
3. Security and Control
4. Third Party Risk
5. Accountability

Operational Benefits

SQUIRE PATTON BOGGS

1. Improved confidence in the quality of the organization's data.
   - Information that is out-of-date, redundant or incomplete can result in faulty strategy and damage to customer relations;
2. Better, more comprehensive analysis from consistent, uniform data across the organization;
3. Clear rules for change management that help the business and IT become more agile and scalable;
4. Reduced data management costs through the implementation of centralized controls and processes; and
5. Increased efficiency through the ability to use and processes data.


Data Privacy and M&A
squirepattonboggs.com

Privacy-Related Issues in M&A

SQUIRE PATTON BOGGS

- **Data Privacy is a Key Deal Issue Where:**
  - Personal information is a major asset of Target
  - Target is in data-driven industry
  - Target “sells” personal information
  - The Target processes personal information about minors
  - The Target has experienced data incidents in the past
- **Business/Controller Obligations Relevant for M&A**
  - Privacy policies
  - Ability to process consumer requests to exercise privacy rights
  - Notices at point of collection
- **Service Providers/Processors**

Planning and Valuation

SQUIRE PATTON BOGGS

- **Sellers**
  - Performing a privacy gap assessment well in advance of a sale
  - Remediate “low-hanging fruit” issues
  - Create a compelling compliance narrative and key documentation for longer-term remediation projects
- **Buyers:** when creating financial deal models and assumptions, legal and business teams should not forget to consider:
  - The impact of possible privacy law-related use restrictions on the valuation model
  - The impact of consumers’ exercise of their consumer rights on the Target’s data assets
  - Data breach and cybersecurity vulnerabilities/potential liability and
  - Estimated costs of remediation of privacy issues, including headcount needed for any technology development or ongoing management of privacy program.

Privacy-Related Diligence

In addition to reviewing Target's data privacy practices generally, a thorough review of the following is recommended:

- The maturity of Target's data mapping and data governance program
- Target's loyalty programs or financial incentives for consumers to provide personal information
- Target's vendor/customer contracts
- Target's ability to operationalize rights requests; *e.g.*:
  - To block the sale of personal information upon request
  - To delete or correct personal information throughout the organization and
  - To limit the uses of sensitive personal information upon request
- Record of past data breaches and Incident Response Plan

Negotiating Definitive Agreements

SQUIRE PATTON BOGGS

- Ensure merger or purchase agreements contain appropriate data privacy representations, covenants and indemnities
  - Don’t limit compliance representations to compliance with law; include compliance with Target’s external and internal privacy policies and contractual obligations
  - Consider including privacy-specific pre-closing covenants
  - Consider specific indemnities for privacy issues
  - For data-rich Targets, consider including privacy representations as fundamental representations
  - Cyber Insurance cover
- Many deals will include a Transition Services Agreement or Hosting Agreements that will govern the use of systems containing personal information – data protection provisions should be included

Privacy Compliance in the M&A Process Itself

SQUIRE PATTON BOGGS

- Making available to Buyer diligence material containing personal information
- Transferring personal information to Buyer at closing
- Consideration of post-closing uses of personal information


Operating a Data Management Program
squirepattonboggs.com

Stakeholder Participation

Info Tech	Risk Management / Insurance	Internal Audit
Info Security	Marketing	Compliance/Ethics
Product	Records	Human Resources
Privacy	Finance	Security
Legal	Procurement	PR / Communications

Understanding Company Data and Data Obligations and Practices

SQUIRE PATTON BOGGS

- An organization must understand what data it has, how it is collected, where it resides, its appropriate purposes and life cycle, what third parties have what interest in it, access to and involvement with it, how the company ensures appropriate protection and compliance with legal and other obligations, and that it is not inappropriately accessed, used or transferred.

- This is accomplished initially through inventories and assessments of data, data practices, and data obligations, and then application of appropriate controls on various data.

- Implement Privacy-by-Design

Risk-Based Compliance: From Remediation Priorities to program Maturity

SQUIRE PATTON BOGGS

1. Assess
2. Protect
3. Sustain
4. Respond


Takeaways
squirepattonboggs.com

Next Steps …

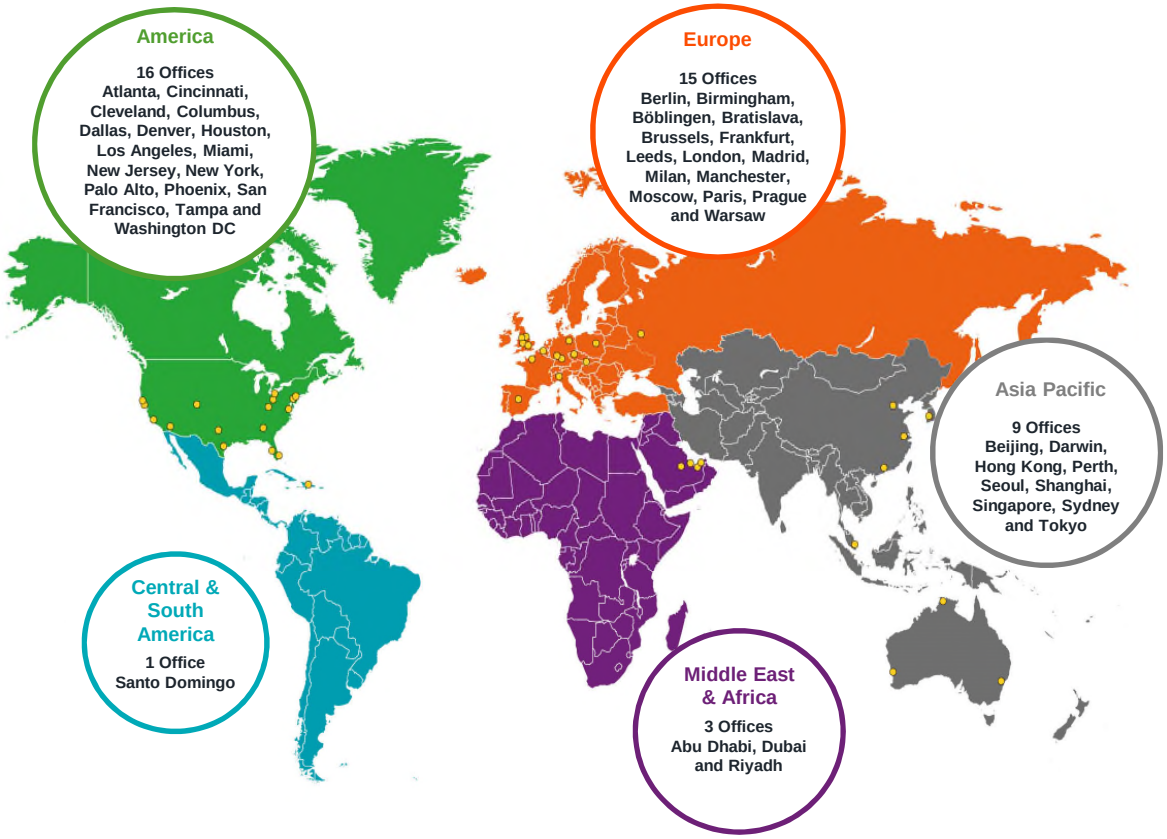
- Assess Your Data Program Now
- Prioritize of Remediating Compliance Gaps
- Develop Governance and Accountability
- Concentrate on Security and Incident Readiness
- Obtain Cyber Coverage
- Ensure Proper Notice and Consent to Ensure Ability to Meet Data Use Goals
- Make P-by-D part of product development and maintain good data inventories and hygiene
- Manage data processing vendors


Questions &
Answers
squirepattonboggs.com

Squire Patton Boggs

- More than 2,600 employees
- 500 partners, 1,500 lawyers, 45 offices in 20 countries
- A seamlessly connected service that operates on any scale – locally or globally
- Top 35 firm globally by lawyer headcount
- Practice law in 140 jurisdictions speaking more than 40 languages
- Selected as a “go-to law” firm by in-house law departments at Fortune 500 companies
- Advise a diverse mix of clients, from long-established FTSE 100/Fortune 500 corporations to emerging businesses, start-ups and sovereign nations
- Recognising the impact of regulation/politics on business, we have a unique mix of highly experienced lobbying/political capabilities in the US, Europe and beyond

Regional Desks & Alliances
Africa
Brazil
Caribbean/Central America
India
Israel
Mexico
Turkey
Ukraine



SQUIRE
PATTON BOGGS

squirepattonboggs.com
mcpc.com