

# ALSTON & BIRD



## Data Disposal: You Really Can Delete It

Privacy + Security Forum  
Washington, DC  
May 11, 2023

# Speakers



**Kate Hanniford**  
*Partner,*  
*Privacy, Cyber & Data*  
*Strategy*  
Alston & Bird



**Alison Atkins**  
*Assistant General Counsel and*  
*Vice President, Chief Cyber*  
*Counsel*  
U.S. Bank



**Matt McClelland**  
*Senior Director, Data Privacy &*  
*Cybersecurity; Information Risk*  
*& Governance*  
Ankura



# Agenda

- Introduction
- Legal Framework
- Spotlight: Ransomware
- Cultural Hurdles to Secure Disposal
- The Business Case for Secure Disposal
- Governance
- Looking Ahead



# Legal Framework



# Who Cares about Data Disposal?

**Cyber**

**eDiscovery**

**Privacy**

**Business Continuity &  
Disaster Recovery (BC/DR)**



# U.S. Legal and Regulatory Landscape

## State Data Security Laws

- NY SHIELD Act (GBL § 899-BB (b)(ii)(C)(4)) – Companies must maintain appropriate safeguards, such as to dispose of “private information” (i.e., sensitive information that could trigger a breach notification obligation) within a “reasonable amount of time” after the information is “no longer needed for business purposes.”
- Similarly, Colorado (Colo. Rev. Stat. § 6-1-713(1)) and Oregon’s laws (ORS § 646A.622(2)(d)(C)(i) and (iv)) require that companies securely destroy or dispose of documents when they are no longer needed, unless otherwise required by state or federal law or regulation.

## NYDFS Cybersecurity Regulations (23 NYCRR 500.13)

- Covered entities must implement a cybersecurity program that includes policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes of the covered entity.

## FTC guidance and enforcement actions

- FTC requires companies to implement policies and procedures identifying and securely disposing of customer information once no longer needed for legitimate business purposes.

## Federal laws


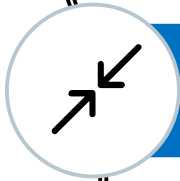


- GLBA, HIPAA, FACTA





# Privacy Laws – the California Privacy Rights Act



-  Publicize Retention Periods at Point of Collection
-  Data Minimization
-  Reasonable Security
-  Secure Disposal or Pseudonymization



# Exemplar Privacy Law Requirements Specific to Data Disposal

<p><b>General Data Protection Regulation (GDPR)</b></p>	<p><u>Compliance</u></p> <p>Art. 5: Personal Data may be retained “<u>no longer</u> than is necessary for the purposes for which the personal data are processed.” AKA the Storage Limitation Principle</p> <p>Art. 13: Data Controllers shall provide the individual with information including “the <u>period</u> for which the personal data will be <u>stored</u>.”</p> <p><u>Enforcement</u></p> <p>Danish DPA fines business 2.8% of revenue for failure to delete personal data.</p>
<p><b>California Privacy Rights Act (CCPA 2.0)</b></p>	<p><u>Compliance</u></p> <ul style="list-style-type: none"><li>At or prior to the time when personal information is collected, the business must disclose “the <u>length of time</u> the business intends to retain each category of personal information . . . provided that a business <u>shall not retain</u> a consumer's personal Information or sensitive personal information for each disclosed purpose for which the personal information was collected <u>for longer than is reasonably necessary</u> for that disclosed purpose”</li></ul>
<p><b>Colorado Privacy Act</b></p>	<p><u>Compliance</u></p> <p>Companies’ “collection of personal data must be adequate, relevant, and <u>limited to what is reasonably necessary</u> in relation to the specified purpose for which the data are processed.” Violations subject to fines up to \$20,000 per violation.</p>





# Exemplar Statutory Requirements Specific to Information Management

<p><b>Virginia Consumer Data Protection Act (CDPA) – Compliance</b></p>	<p><u>Compliance</u>  <b>Personal Data collected should be “Adequate, relevant, and <u>limited</u> to what is necessary in relation to the specific purposes.”</b></p>
<p><b>Utah Consumer Privacy Act</b></p>	<p><u>Compliance</u>          Anticipated effective date December 21, 2023. Consumer rights around access, deletion, portability, opt-out of targeted advertising and sale of personal data are similar to the VCDPA. Up to \$7,500 per violation.</p>
<p><b>Brazil – Lei Geral de Protecao de Dados, or “LGPD”</b></p>	<p><u>Compliance</u>          Consumer rights around access, deletion and data transfers similar to GDPR. Sanctions became effective August 2021.</p>
<p><b>Australia – Privacy Act 1998; Fair Work Act 2008</b></p>	<p><u>Compliance</u>          Rights around collection, use, storage and disclosure of personal information in private and federal sector.</p>
<p><b>China – Personal Information Protection Law “PIPL”</b></p>	<p><u>Compliance:</u> Effective November 1, 2021          Defined by “strong data subject rights” and stringent requirements on data sharing, data transfers (including data localization), data minimization and storage limitations as well as serious corrective actions for those organizations that fail to adhere to the legal regime, including penalties and fines (up to 50 million RMB or 5% of an entity’s annual revenue), confiscation of illegal income and suspension of services.</p>

# Cybersecurity Risks: Spotlight on Ransomware

- **Corporate repositories** present the most significant risk of being susceptible to ransomware due to the potentially significant quantities and highly sensitive nature of data they may hold.
- **Reduce the potential attack surface** by reducing the amount of records containing sensitive data. This can minimize an organization's risk of a data leakage/exposure.





# Cultural Hurdles to Secure Disposition



# The Business Case for Secure Disposal of Data



# Governance



# Looking Ahead

# Thank you!



**Kate Hanniford**  
*Partner,*  
*Privacy, Cyber & Data*  
*Strategy*  
Alston & Bird



**Alison Atkins**  
*Assistant General Counsel and*  
*Vice President, Chief Cyber*  
*Counsel*  
U.S. Bank



**Matt McClelland**  
*Senior Director, Data Privacy &*  
*Cybersecurity; Information Risk*  
*& Governance*  
Ankura