Data Privacy Bell Ringers

These Situations Should Ring a Bell and Prompt Discussion with Privacy Counsel

By:Faith D. Kasparian
January 30, 2025

Information and data are everywhere. And, as information and data have proliferated, so too have the laws applicable to privacy and data security. Understanding – and complying with – this rapidly changing landscape of laws is critical for any business. The penalties for violation can be significant and may include substantial fines, destruction of unlawfully obtained data, and halting of data flows.

In honor of Data Privacy Week, and to help businesses navigate data privacy issues, I would like to share with you some of the major privacy "bell ringers". These contexts should "ring a bell" – as they may indicate the presence of privacy-related legal issues – and prompt you to consult with privacy counsel.

⍰ Handling any of the following information should ring a bell:

- Medical or Health
- Credit/Debit Card or Bank/Financial Account
- Social Security Numbers
- Biometric data (such as a fingerprint, hand, facial, or retina scan, or voiceprint)
- Insurance information
- Username or email address in combination with a password or security question and answer that would permit access to an online account
- Precise geolocation
- Information from children
- Student education records
- Information from individuals outside the United States (including the EEA or UK)
- Information from consumers in Nebraska or Texas
- Significant amounts of consumer data (such as more than 35,000 consumers in a particular U.S. state)

⍰ Any of the following business attributes should ring a bell:

- Any online presence
- Annual revenues of $25M or more

- Doing business internationally
- A website or online service that is directed to (or may be interesting to) children or minors or used primarily for K-12 school purposes

? Engaging in any of the following types of actions should ring a bell:

- Corporate merger or acquisition or investment transaction (or preparing for such a transaction)
- Transfer of data internationally or receipt of data from outside of the United States
- Service arrangement pursuant to which a service provider may receive, or a service recipient may share, personal data
- Dropping cookies or use of pixels or other online tracking technology
- Use of notetaking or transcription technology (including via AI) in meetings
- Recording meetings
- E-mail or telephone marketing
- Text messaging for marketing or other purposes
- Credit or background checks
- Online advertising (including targeted or behavioral advertising)
- Use of analytics (such as Google Analytics)
- Use of social media login functionality (such as Facebook Login)
- Buying data or use of lead generation services
- Offering an app on the Apple Store or Google
- Sharing data with any third party
- Automatic decision making (*e.g.*, making significant decisions about an individual without human intervention) or profiling (*e.g.*, evaluating or predicting aspects concerning a person such as performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements)
- Inputting personal data to an AI solution or using personal data for machine learning purposes

? Having any of the following types of knowledge should ring a bell:

- Knowledge or reasonable suspicion of any breach of security (including the unauthorized acquisition or use of data or any confidential process or key that is capable of compromising the security, confidentiality, or integrity of data)
- Actual knowledge of use of a website or online service by, or collection of information from, children or minors
- Knowledge of a complaint regarding data privacy or receipt of a request from an individual to exercise rights regarding their data

Finally:

- If your business does not have a privacy policy, or
- The privacy policy of your business has not been reviewed by counsel within the past year, or
- Your business has not audited its information collection and handling practices to ensure compliance with its privacy policy and applicable laws

These facts, too, should ring a bell.

To discuss your specific privacy and data security legal services needs, please contact Faith Kasparian, CIPP-U.S.