Data Privacy Bell Ringers

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

January 08, 2018

Information and data are everywhere. Indeed, as of 2010, it was noted that "every two days, we create as much information as we did from the dawn of civilization up until 2003."[1] 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, because the penalties for violation can be significant and may include substantial fines plus destruction of unlawfully obtained data.[2]

The privacy team at Morse would like to share with you some of the major privacy "bell ringers" – the contexts that should "ring a bell" indicating the presence of privacy-related legal issues and prompt you to consult with privacy counsel.

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

- Medical or Health
- Credit/Debit Card or Bank/Financial Account
- Social Security Numbers
- Student education records or information from children or minors
- "Personal Information" within the meaning of the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. § 17.00 *et seq.* (Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account).
- Information about individuals from jurisdictions outside the United States (particularly the European Union)

The following business attributes should ring a bell:

- A website or online service featuring any advertising, conducting analytics, or using social media plugins
- A website or online service that is directed to (or may be interesting to) children or minors
- A website or online service that is used primarily for K-12 school purposes
- Any online presence

Having the following types of knowledge should ring a bell:

- Actual knowledge of use of a website or online service by children or minors

- Actual knowledge of collection of information from children through a website or online service
- 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)

Engaging in the following types of action should ring a bell:

- Corporate merger or acquisition transaction[3]
- Transfer of data overseas or receipt of data from overseas
- Service arrangement pursuant to which a service provider may receive, or a service recipient may share, data (including customer data)
- E-mail, telephone, or text marketing
- Conducting credit or other background checks

Finally…

- If your business does not have a privacy policy or a written information security program, 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 D. Kasparian**, **Michael J. Cavaretta**, **Amanda E. Schreyer**, or **Howard G. Zaharoff**.

Footnotes.

1. See MG Siegler, Eric Schmidt: Every Two Days We Create as Much Information as We Did up to 2003, Tech Crunch (Aug. 4, 2010) (quoting Google CEO Eric Schmidt).
2. See, e.g., *United States v. Playdom, Inc.*, Case No. SACV 11-0724-AG(ANx), Consent Decree and Order for Civil Penalties, Injunction and Other Relief (C.D. Cal. 2011) (Playdom fined $3 million by the FTC for violating the Children's Online Privacy Protection Act, 15 U.S.C. § 6501, et seq.); Resolution Agreement Between U.S. Dept. of Health and Human Services and Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (Sept. 13, 2012) ($1.5 million fine for failure to adequately assess data security risks or adequately adopt or implement security procedures to protect private data); Press Release, Major Boston Restaurant Group That Failed to Secure Personal Data to Pay $110,000 Under Settlement with AG Coakley (March 28, 2011) (Restaurant group paid a $110,000 fine for failing to put in place adequate safeguards to protect customer credit card data and failing to adequately secure its wireless network); see also, In the Matter of Sears Holding Mgmt. Corp., Docket No. C-4264 (Aug. 31, 2009) Decision and Order (Sears ordered to destroy all data collected through tracking software after failing to adequately notify consumers that the software collected data from consumers' secure browsing sessions and third-party website visits).
3. For further information on privacy and data security issues associated with merger and acquisition transactions, see Faith Kasparian, M&A Privacy and Compliance with

Applicable Privacy Laws and Sharing of Customer Information (Jan. 5, 2015).