September 2021

Privacy Compliance Newsletter

Check out ID's Privacy Compliance webpage, where you can find up-to-date thought leadership and download the most recent version of this newsletter.

SEPTEMBER SPOTLIGHT: IT'S NOT JUST YOUR DATA ANYMORE

In the last two years, there have been over 100 privacy and cyber security laws enacted globally. In the US alone, each of the 50 states has its own data breach law. BUT data breaches and privacy threats continue to grow. It seems any organization that collects and stores personal or sensitive data is inevitably going to experience an "incident." The incident may range from a ransomware attack to an unauthorized person accessing personal or sensitive data without an authorized purpose.

When a privacy incident occurs, the organization is under pressure to notify authorities in a timely manner. The treat of penalties and reputational damage looms large. IT or Security Departments can't be solely responsible. Recently, during a client call, an IT representative made the following analogy: "In IT we prepare and cultivate the land for farming. It's the business that plants and maintains the crops. We can secure the land, but we don't know what's planted."

Privacy departments in many companies are small but growing and maturing. In some companies it's not a department at all but a one-person show. Privacy professionals are working hard to educate the Board and leadership team about incident response requirements and the importance of compliance. They are also training staff on what constitutes a privacy-related incident and how to report them.

The risk of non-compliance is becoming clearer to an organization, but what can be done to take an incident response from a simple reaction to a mature response process? *It's preparation and teamwork among IT/Security, Privacy and Legal.*

CONTINUE READING

UPCOMING IN-PERSON PRIVACY EVENT:

IAPP Privacy. Security. Risk. 2021

WHEN: October 19 – 22 | WHERE: San Diego, CA

P.S.R. is the number-one event focused on the intersection of privacy and technology. Speakers and breakout sessions will dive deeply into maximizing technology as a privacy asset and minimizing it as a privacy threat. **Click here to learn more.**

PRIVACY HAPPENINGS

CPRA's Data Retention Requirements

As we've heard, the CPRA amends the CCPA and enlarges its requirements. In several ways, it bring the CCPA closer to the GDPR. There are many parts of the CPRA that have been well publicized such as its inclusion of sensitive personal information and sharing of personal information for behavioral advertising.

One aspect of the CPRA that hasn't received much attention is its data retention requirements. Again, similar to the GDPR, the CPRA prohibits an organization from, "retain[ing] a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose." The CPRA also requires a business to inform consumers as to the length of time the business intends to keep each category of personal information or describe the criteria it will use to determine this period. Keep in mind the CPRA goes into effect on January 1, 2023.

The CPRA is yet another reason why keeping data "just in case" is no longer viable. **Record retention practices** are a key component of a successful information governance program. The CPRA and GDPR are making retention obligations requirements

Protecting the Information of our Vulnerable Children and Youth Act

It's well-known children and teens are experts when it comes to using mobile phones, gaming platforms and social media. Marketers also know this fact and use many tactics to track and target children. The Children's Online Privacy Protection Act (COPPA) enacted in 1998 imposes certain requirements on operators of websites or online services directed to children under 13. However, times and devices have changed, and many companies have violated the privacy protections in place today. One example of technology outpacing protection is digital tracking technology.

US Representative Kathy Castor introduced the Protecting the Information of Vulnerable Children and Youth Act (PRVCY) to strengthen COPPA. The bill expands COPPA's strengths and incorporates key elements of the UK's Age-Appropriate Design Code. PRIVCY specifically prohibits behavioral ad targeting on all sites children and teens frequent. Its goal is to ban surveillance advertising of children and teens so they can safely use the internet without exposure to data-driven marketing.

Jenny Radesky, MD, FAAP, American Academy of Pediatrics Council on Communications and Media said, "Managing children's relationships with technology has become an increasingly daunting and difficult job for parents. Digital platforms often collect children's data, target them with personalized advertising based on their behaviors online, and generally fail to prioritize the best interests of young people. The Kids PRIVCY Act is a much-needed step toward making digital environments safer for young people by updating the Children's Online Privacy Protection Act for the 21st Century so children—and now teens too—can have control over their data online, just as COPPA intended."

Click here to read the entire press release.

TikTok Changes its United States Privacy Policy

TikTok recently changed its US privacy policy to give itself permission to "collect biometric identifiers and biometric information" from users. The new policy explained this includes "faceprints and voiceprints" although it did not explain what changes it was making to the app or new features being created that necessitated this additional biometric data.

Senators Amy Klobuchar and John Thune sent a letter to TikTok's CEO Shou Zi Chew requesting information about consumer data including facial and voice biometrics the company collects. The Senators wrote, "We were alarmed by reports highlighting TikTok's recent change to its U.S. privacy policy, impacting the application's nearly 130 million users. The updated policy appears to enable TikTok to automatically collect biometric data, including certain physical and behavioral characteristics from video content posted by its users."

Click here to read the entire press release.

Connect with us