Q&A with Burns & Levinson Attorneys David Amidon and Brooke Penrose

5/4/21

David Amidon and Brooke Penrose

*We sat down with **David Amidon**, Chair of Burns' Business Media Advisory Group at Burns & Levinson,*

*and IP and cybersecurity attorney **Brooke Penrose**, who will be leading a free webinar **"Privacy & Data Security at Events: What Organizers Need to Know"** on May 6, 2021 at 1:00 pm ET, to get their thoughts on how companies can better manage their organization's collection, dissemination and use of customer and business partner information.*

Q. Do meeting and event organizers have to meet a higher standard of privacy and data security compliance than other businesses?

Amidon: Perhaps the most critical asset of a business that organizes meetings and events is the personal information collected from the "buyers and sellers" that are brought together. In order to monetize that data – which is essentially the business model for most organizers – it's critical that the data be collected, stored and disseminated in a thoughtful, compliant manner. Doing so creates greater trust with stakeholders, making them more willing to share.

Q. What are some best practices that event organizers should follow to ensure they are protecting the personal information of their attendees?

Penrose: First, be transparent with attendees by providing clear notice about the business' personal information handling practices. If personal information will be shared with third-parties, provide attendees with this information as well as notice of what their legal rights are. In addition, only share personal information with reputable third-parties who are contractually bound to use personal information consistent with applicable law and the business' instructions. Finally, adopt thoughtful safeguards against unauthorized access to attendee personal information. For example, if someone at the business does not have a business reason to have access to attendee personal information, it should be technically and physically difficult for that person to access it.

Q. Are there one or two common mistakes that you see event planners regularly make regarding privacy and data security protection?

Amidon: One is not treating privacy and data security protection as a strategic imperative for their business. This means that event planners fall behind in understanding and following current requirements and best practices, which can put them in a challenging position when recipients of their personal information insist on contractual representations and warranties around the lawful collection of this information. Even for companies that do understand best practices, we often see a "one size fits all" mentality instead of trying to identify the "right" privacy and data security policies and practices for that unique organization. For example, data security and privacy laws typically apply based on where the person is physically seated so a business' compliance obligations for collecting information will depend on where the event physically occurs or, if virtual, where its attendees are seated. It's not a cut-and-paste exercise.

Q. What personal information rights under U.S. and international laws do people have?

Penrose: In general, people outside of the U.S. enjoy stronger legal rights regarding their personal information than U.S. residents (particularly those in Europe). Still, at minimum, all U.S. residents have the right to opt-out of receiving marketing e-mails and several state laws provide their residents with the express right to review and correct the personal information a business holds on them. In addition, the FTC has broadly interpreted its ability to enforce against businesses engaging in unfair and deceptive trade practices to extend to a business' privacy and data security practices, making it imperative for businesses to provide clear, advance notice of their personal information handling practices. Under international privacy laws, many individuals enjoy an expanded scope of personal information rights,

including the “right to be forgotten,” meaning they can instruct a business to delete them from a database entirely.

Q. Has the move to virtual conferences made privacy and data security easier, the same or more difficult? Why?

Amidon: The transition to remote conferences has raised management’s awareness of privacy and data security issues, which has made it easier to encourage clients to pay closer attention to the challenges in effectively managing data. We had the same problems and concerns before, when in-person events were prevalent, since the same types of personal information were being collected and used. However, the move to more virtual conferences has introduced some challenges for organizations who focused strictly on in-person events in the U.S. as their compliance typically expands in a virtual environment because they have no control over where attendees are located (and thus, it is harder to ascertain what data security and privacy laws apply to that person’s information).

Q. How are recently enacted data security and privacy laws like GDPR and CCPA affecting the operations of business and event planning?

Penrose: GDPR and CCPA have flipped the presumption businesses need to have with respect to personal information; it used to be that you could presume that any use of personal information was fair unless someone objected. These laws though generally make the use of personal information unfair unless you have some specific lawful basis, such as the consent of the individual.

Q. What are the risks of noncompliance?

Amidon: The most obvious risks are the potential fines imposed by the various regulatory schemes governing personal information collection use, which in some cases can be significant. Less clear, but to me much more concerning, is the lost opportunity in creating greater trust in stakeholders, and in burnishing the event’s brand in its market. Compliance and best practices are being followed with greater ubiquity – if an organizer is behind, it’s noticed and it will have a meaningful effect on the organizer’s standing in the market.

Q. Any parting wisdom you would like to share?

Penrose: Even if you believe your organization is a small enforcement target for regulators, you may work with organizations (like sponsors) who have a high risk of becoming an enforcement target. Many, if not most, privacy laws impart some liability on organizations for sharing personal information with organizations that misbehave, so most reputable organizations will include comprehensive representations and warranties regarding compliance with privacy and data security laws as well as broad indemnification rights if your organization misbehaves in a manner that costs the sponsoring organization.

Amidon: Make privacy and data security protection an integral part of your event or meeting brand and strategy. It’s not simply an IT exercise or a check-the-box compliance matter for legal. It can and should be a powerful tool in developing and building a market-leading platform.

David Amidon *is chair of the Business Media Advisory Group at the law firm of Burns & Levinson in Boston. He has deep expertise in the business media industry as an attorney and former industry executive. Amidon’s clients range from stand-alone event/expo organizers to the vendors and technology providers that support them. He has also helped run two business media companies, including an Orlando, Florida-based tradeshow, conference and event organizer. He can be reached at*

damidon@burnslev.com *or 617-345-3578.*

Brooke Penrose *is a senior associate at the firm, where she focuses her practice on trademark and brand protection, copyright, and privacy and data security. She is an IAPP Certified Information Privacy Professional in U.S. and European law. She has helped many companies develop data collection and compliance programs and is well-versed in data security best practices. She can be reached at* ***bpenrose@burnslev.com*** *or 617-345-5287.*

Posted in Law, People