Top Takeaways From the International Association of Privacy Professionals Global Privacy Summit

By: Kevin D. Pomfret

04.25.2022

On April 12 and 13, the International Association of Privacy Professionals (IAPP) hosted their 2022 Global Privacy Summit in Washington, DC. It was another jam-packed event, with fantastic speakers discussing a wide range of issues associated with privacy, data protection and cybersecurity.

The top three takeaways from the Summit that resonated most with me are:

- Privacy Law in the U.S. Continues to Move Forward on Three Distinct Tracks

  Privacy law in the U.S. continues to move forward along three paths. First, a growing number of states are expected to enact privacy legislation over the next year. One speaker suggested that he believes upwards of 30 states will have some sort of comprehensive data protection law in place by the end of 2023. Second, a panel that included Congressional staffers suggested that significant progress was being made on two major sticking points to a comprehensive federal privacy law-federal preemption of state laws and private right action-and suggested a law could be passed by the end of the year. Finally, Federal Trade Commission (FTC) Chair Lina Khan suggested the FTC is exploring using its rulemaking authority to address privacy and data protection from both a consumer protection and an anti-competition standpoint. While it is difficult to predict how it will all turn out, the amount of laws and regulations around privacy and data protection are going to continue to grow over the next few years.

- The U.S. Government?s Cybersecurity Effort Remains Fragmented

  National Cyber Director Chris Inglis spoke on the important role that the federal government can and should play in working with both the private sector and state and local governments to address the growing cybersecurity threats to our nation. However, it remains unclear whether there is agreement within the federal government on which agencies will take the lead on this critical issue. In addition to Director Inglis, there are currently a number of other individuals and agencies within

the U.S. Government responsible for some aspect of cybersecurity, including the Cybersecurity and Infrastructure Security Agency (CISA), headed by Jen Easterly, the National Security Council (NSC), the National Institutes of Standards and Technology (NIST) and the National Security Agency (NSA). In addition, sector-specific regulatory agencies, such as the Departments of Energy and Transportation, also have regulatory authority pertaining to cybersecurity.

Perhaps in an effort to address this uncertainty, on the Friday before the event, the Federal Interagency Cybersecurity Forum-a group of 30 regulatory and advisory agencies within the federal government-met. According to the group?s charter, its mission is to ?align, leverage and deconflict cross-sector regulatory authorities? approaches and promote cybersecurity protection.? In her opening remarks to the Forum, FCC Chairwoman Jessica Rosenworcel stated that ?[r]ight now, there?s a lot of fragmentation across sectors and jurisdictions in what information gets reported, when and how it is reported, and how that information can be used. So, we?ll discuss using this Forum as a place to work toward greater convergence on these matters.?

Author?s Note: In April CISA published a Fact Sheet on the type of information that a company should report if it suffers a cyber event.

- Data Transfers from the E.U. to the U.S. Should Become Easier (Again) for Small and Medium Size Enterprises (SMEs).

  A panel discussion on the recently announced Trans-Atlantic Data Privacy Framework discussed the key changes that will be put in place to address the issues raised with Privacy Shield under the Schrems II decision. The panelists stated that the changes will primarily involve the U.S. Government?s access to personal data and ensuring European citizens having a right to redress under U.S. law if they think they have been unlawfully targeted by the U.S. Government. As a result, the speakers suggested, the obligations for businesses should not significantly differ from Privacy Shield?s requirements. This should come as a relief for the many SME?s that relied upon Privacy Shield for data transfers to the U.S.

In Case You Missed It: Amendments to the Virginia Consumer Data Protection Act

Also, of note last week, Virginia?s Governor Glen Youngkin signed into law several amendments to the Virginia Consumer Data Protection Act (the ?Act?) which will come into force in January 2023 The two most significant amendments were:

1. Clarifying Requirements for Responding to Right to Deletion Requests for Certain Personal Data.

   Under the first amendment, a business that has obtained personal data about a consumer from a source other than the consumer will be able to lawfully respond to a consumer's request to delete such data by either:

   (i) retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring the consumer's personal data remains deleted from the business?s records and

not using such retained data for any other purpose, or
(ii) opting the consumer out of the processing of such personal data for any purpose except for those exempted under the Act.

2. Expanding Definition of ?Nonprofits?

The second amendment expands the definition of nonprofits-which are exempt from the Act-to include ?any party, committee, association, fund, or other organization, whether or not incorporated, organized and operated primarily for the purpose of influencing or attempting to influence the selection, nomination, election, or appointment of any individual to any federal, state, or local public office or office in a political organization or the election of a presidential/vice-presidential elector, whether or not such individual or elector is selected, nominated, elected, or appointed? that is exempt from taxation under § 501(c)(4) of the Internal Revenue Code.

Stay tuned for more legal developments related to data management, including privacy and data protection, cybersecurity, intellectual property rights and data quality. Please contact**Kevin Pomfret** (703.760.5204 | kpomfret@williamsmullen.com) with any questions.

Related People

- Kevin D. Pomfret ? 703.760.5204 ? kpomfret@williamsmullen.com

Related Services

- Data Protection & Cybersecurity
- Intellectual Property