PART 2 – IMMEDIATE INDUSTRY RESPONSE

Privacy Leaders' Views

The Impact of COVID-19 on Privacy Priorities, Practices and Programs

By IAPP Research Director Caitlin Fennessy, CIPP/US

During summer 2020, 21 privacy leaders from industry, government and academia graciously shared their views on the impact of COVID-19 on privacy priorities, practices and programs. Each participated in a 30-minute interview to inform the IAPP and EY's joint research project on COVID-19 and privacy. We captured their experiences, challenges and recommendations in a five-part series, introduced previously. In this second piece, we share their insights on companies' immediate COVID-19 response.

Immediate COVID-19 response

The word privacy practitioners most frequently used to describe their experience was "accelerate." As companies sought to operate amid government-mandated quarantines, social-distancing rules and contact-tracing efforts, they introduced new health safety protocols, shifted to remote work, increased virtual engagement, and supported government test and trace efforts. Each of these shifts led to dramatic increases in data processing. Privacy leaders across industry sectors were asked to accelerate digital transformations, privacy and security reviews of new tools to enable remote work and collaboration, and the issuance of guidance regarding COVID-19-related data collection or sharing. In short, they were asked to sprint, and so they did.

Amid the deluge, privacy leaders said employee health data collection and providing a secure and effective virtual work environment for employees and customers were their top priorities.

Employee health data collection

Privacy leaders' views and experiences concerning COVID-19-related employee health data collection highlight the geographic diversity in employee privacy protections. U.S. practitioners pointed to the lack of federal privacy law governing employee data and explained how they have had to look to laws and colleagues in other fields for guidance.

> *WilmerHale Partner Kirk Nahra, CIPP/US, said, “Almost all of the questions that I’ve been asked have been about COVID issues with employees. The answer has either been there isn’t a law or … the answer is driven by a law that really isn’t a privacy law at all.”*

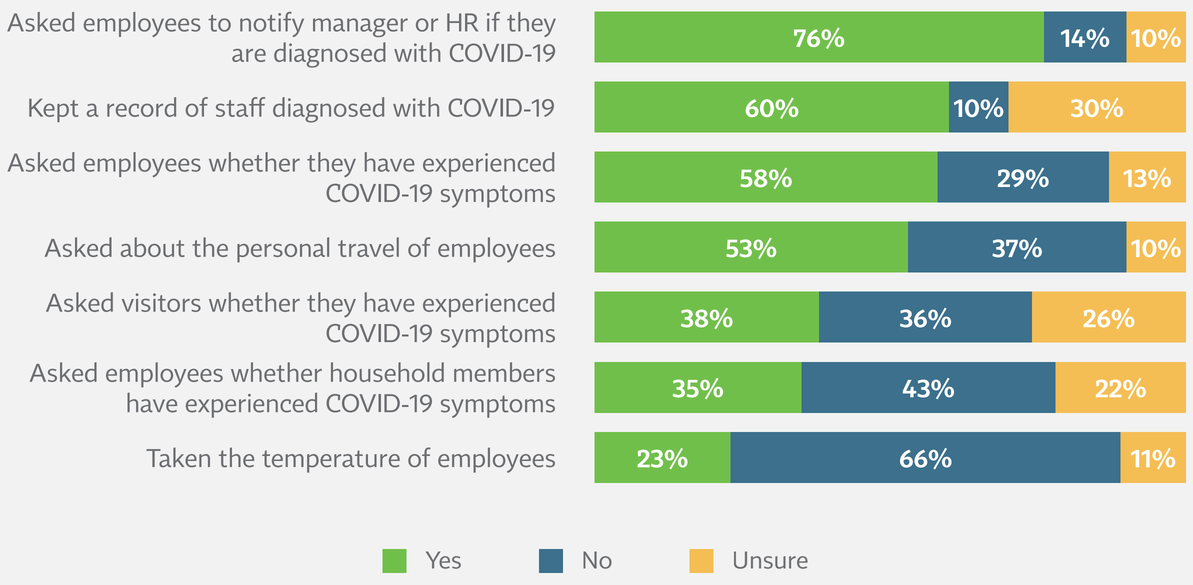
U.S. practitioners turned to Occupational Safety and Health Administration standards and the Americans with Disabilities Act to understand obligations and restrictions on employee data use. While OSHA and ADA standards are instructive, neither provides a comprehensive set of privacy protections or rights. One U.S. Senate staffer noted this legislative gap and said pandemic response is shining a helpful spotlight on the need for employee privacy rights.

Most non-U.S. stakeholders saw the dynamic reversed. They pointed to heightened protections for employee data compared to consumer data, including due to requirements to work through employee works councils. Some noted virus response efforts like contact tracing have made clear that protections for consumers and employees should be equalized.

While protections might vary by jurisdiction, the need to collect employee health data to ensure safe work environments during the pandemic has been fairly universal. In IAPP and EY’s April survey, 58% of respondents from around the world reported their organizations were asking employees whether they had experienced any COVID-19 symptoms. Almost a quarter (23%) had also taken their employees’ temperatures. FIGURE 1

FIGURE 1

Most organizations have collected data from employees about COVID-19 symptoms and kept diagnostic records



Originally published in “Privacy in the Wake of COVID-19” report.

Industry privacy leaders said they were asked to weigh in on these new data collection efforts and noted the questions they faced went well beyond whether or not to collect. They were asked about recording, retaining, sharing, disposing and, importantly, how such data should or could be used.

Nahra mentioned some of the many questions he is being asked: Do you record employees' temperatures? How do you use the data? If someone's temperature is high one day and low the next, are they then fine? Do you bar certain people from entry based on a temperature? If so, for how long? How do you effectuate that? As a result, privacy practitioners are working more closely with HR colleagues to document employee privacy protections and data uses.

Even when questions are universal, the answers frequently are not.

Multinationals have had to decide whether to localize or globalize approaches to employee health data collection. Given the geographic diversity in employee privacy rules and in COVID-19 incidence, this was a tough call for many. Data protection authorities have provided extensive guidance on how some of the above questions can be addressed in compliance with local data protection laws and that guidance is far from universal. Several practitioners said their companies have sought uniformity in their approaches across cities, states and countries, achieving this through "acknowledgement" of individual compliance with local rules concerning individual health and gathering. However, operationally, with offices closed in some locales and open in others, local nuances or completely different approaches have been necessary in some places.

Privacy practitioners also raised more sector-specific employee privacy challenges, where they were often less able to draw on regulator guidance or the best practices of their peers. Unique challenges arose for in-person service providers, essential workers and logistics companies, among others.

Practitioners discussed how they addressed data protection challenges related to enforcing mask mandates, providing COVID-19-related financial assistance, conducting health screenings and vetting in-person service providers. In each case, they focused on necessity of collection, minimizing data retention and transparency.

> ***Uber Chief Privacy Officer Ruby Zefo, CIPP/US, CIPM, FIP, for example, said they decided to use an object identifier to enforce Uber's mask mandate for drivers rather than collect biometric information to help preserve their privacy principles.***

Merck Chief Privacy Officer Scott Taylor spoke about health screenings for essential workers at Merck, as well as the vendors with which they work. "We've got essential workers that are producing lifesaving medicines every day, so we have to protect that environment from an outbreak. We've had to modify a bit how we approach who can come into the facility and do some basic health screening," he said. Taylor said essential workers at Merck understand the rationale behind the health screening and so are fairly comfortable with it. Transparency has helped. He added that Merck has approached screening differently for outside suppliers, such as FedEx and UPS, delivering the base products necessary for vaccine development. Rather than duplicative screening, Taylor said, “We’ve worked with those companies to ensure that their practices for health and safety of their employees actually have been attested to so that we have more trust with those folks coming into the facility.”

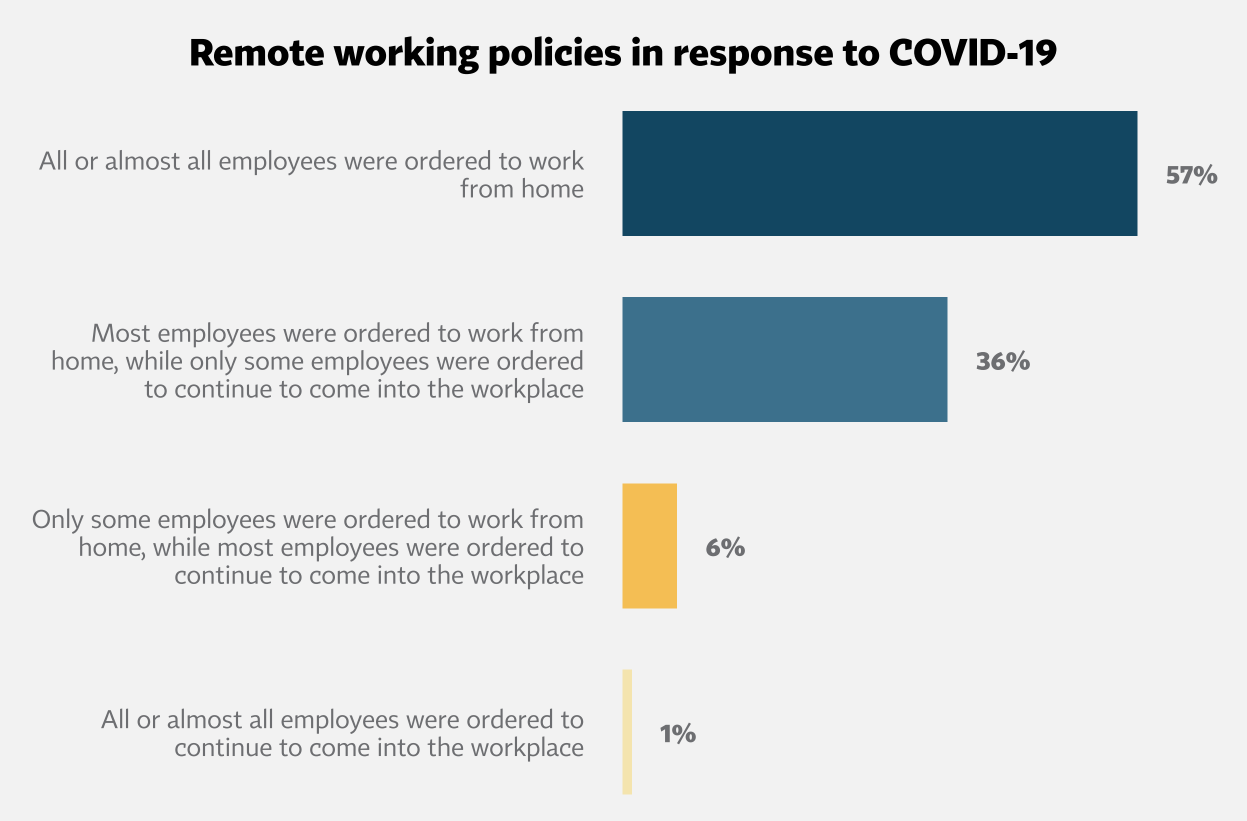
For privacy professionals in companies whose mission does not require workers to be on site or to come into daily contact with others, the focus has instead been on virtualization.

Virtualization

Practitioners spoke of the privacy implications of rapid transitions to a virtual environment for both employees and customers. In April, IAPP and EY found that more than 90% of survey respondents had put in place a policy requiring most or all employees to work from home. FIGURE 2 This exceptionally high percentage may reflect the data-driven and digitally oriented nature of much of the privacy profession. Many privacy leaders expressed gratitude that virtualization projects were already under way and that they did not need to start from scratch.

> ***Vivienne Artz described her experience at Refinitiv in London, where she serves as chief privacy officer. “We were already on a digital journey. What [COVID-19] has done is to accelerate that,” she said.***

FIGURE 2



Originally published in “Privacy in the Wake of COVID-19” report.

As practitioners helped their companies transition to virtual environments, they said security, efficiency and speed were their top areas of focus.

On the security front, they pointed to the added concerns related to home networks, increased attacks on organizations' systems and heightened scrutiny of security protocols, particularly for cloud service providers.

> ***Citrix Chief Privacy and Digital Risk Officer Peter Lefkowitz, CIPP/US, said they have seen "a lot more attempts at malware, hacking, intrusion, theft of credentials, crypto mining and the like" during this pandemic. This has led Citrix's internal audit function to take a "tremendous interest in security."***

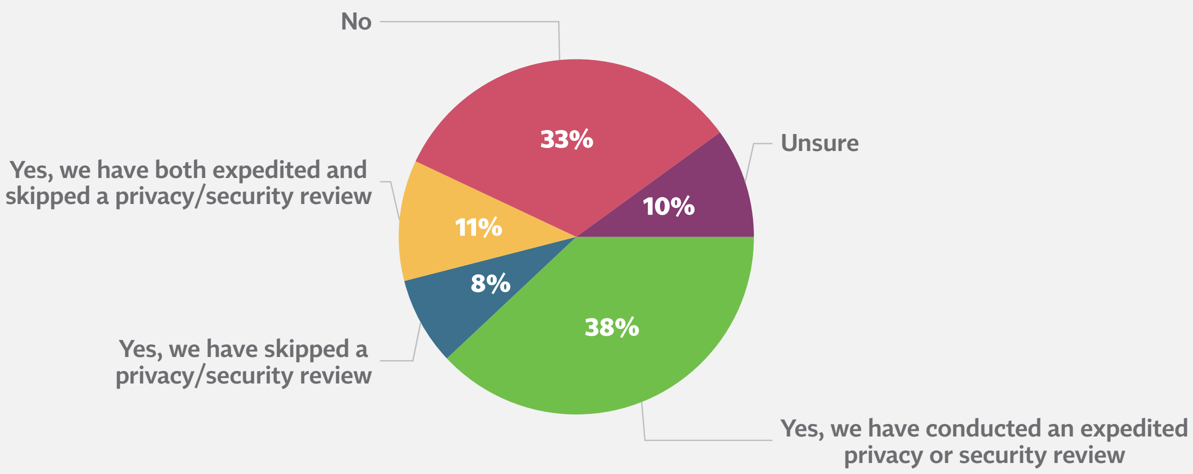
Numerous practitioners said this made it more important than ever to ensure employees' security updates are completed and patches installed. Caroline Louveaux, CIPP/E, CIPM, chief privacy officer at Mastercard in Brussels, said it has increased the "need to monitor what employees are doing and also monitor for fraud and for cybersecurity." She felt it "made the case for those data breach exercises (for employees and the board) stronger."

In terms of efficiency and speed of digital transformations, virtual collaboration tools were top of mind.

Many practitioners spoke of the need to fast-track privacy and security reviews of new communications platforms. In our April survey, nearly half of organizations (45%) had adopted a new technology or contracted with a new vendor to enable remote work due to COVID-19. Sixty percent of those that adopted new technologies had accelerated or bypassed the privacy and/or security review. FIGURE 3 Meanwhile, highly publicized privacy and security challenges have plagued some of the companies providing these tools.

FIGURE 3

Expedited or skipped privacy/security review as a result of COVID-19



Originally published in "Privacy in the Wake of COVID-19" report.

To address these challenges and increase employee and customer confidence in virtual communication, several privacy leaders said they provided employees with a list of trusted communications platforms. Others supported collaborative efforts to identify key questions to ask when vetting new vendors. Privacy practitioners felt this increased scrutiny would push platform providers to improve their privacy and security practices.

On the more personal front, privacy leaders discussed data protection challenges associated with working from home during a pandemic. With spouses and children often sharing workspaces, it has been more difficult for employees to keep personal lives private. Virtual backgrounds help and practitioners welcomed the humanizing appearances of kids and pets, but these new dynamics have created some privacy challenges (and amusement on social media) that will need to be addressed, particularly if the intermingling of home and work life continues longer term.

Privacy leaders also highlighted more sector-specific virtualization challenges. In regulated industries, such as health care, virtualizing certain activities has required extra engagement with government authorities.

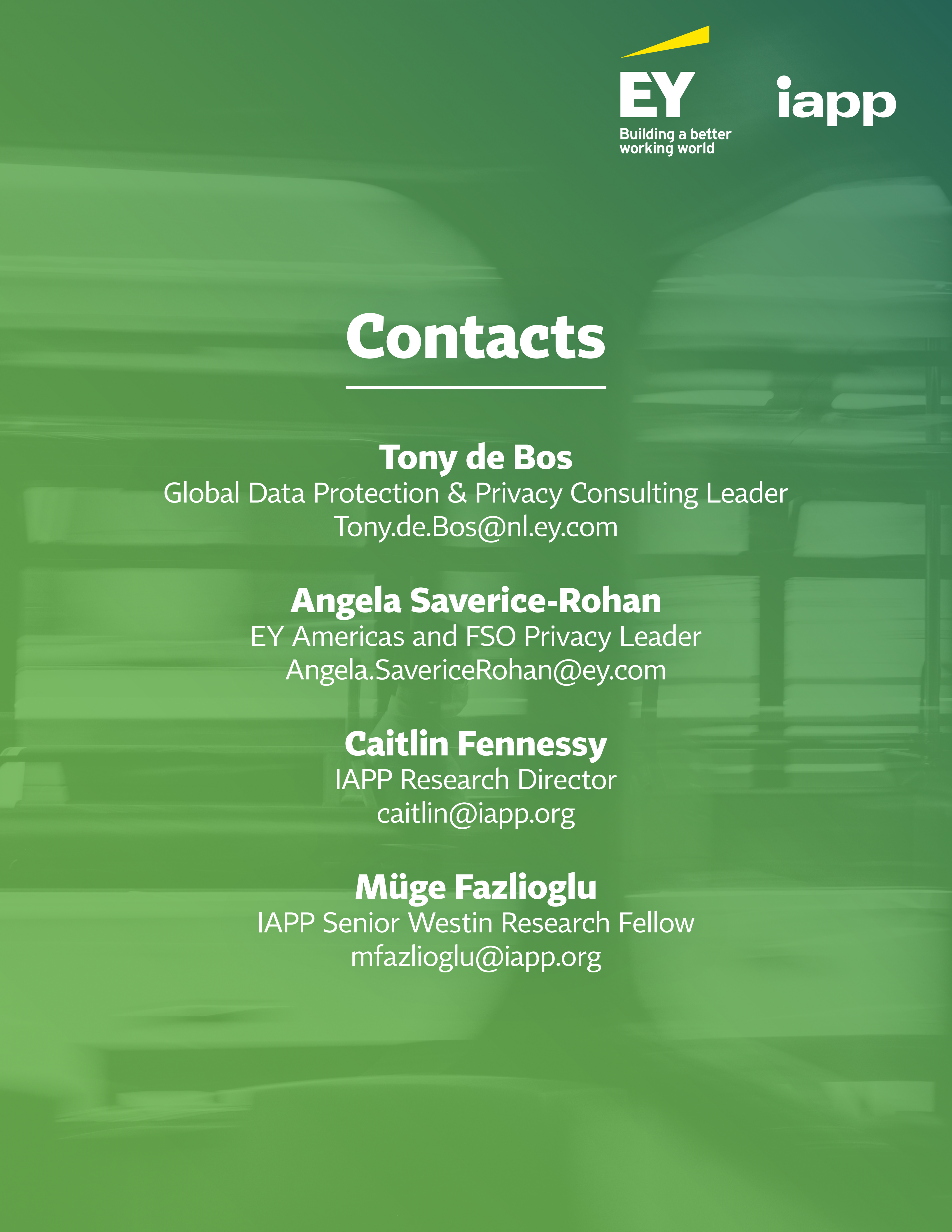
> ***Pfizer Chief Privacy Officer Patrice Ettinger, CIPP/US, said the pharmaceutical company is increasingly monitoring clinical trials remotely. This requires coordinating with regulators, who have shown flexibility once we demonstrated it can be done properly in a new way, she said.***

In the education sector, companies must abide by sector-specific laws and provide more stringent protections for the data of minors.

> ***McGraw Hill Chief Privacy Officer Andy Bloom, CIPP/E, CIPP/US, CIPM, CIPT, FIP, said they have provided thousands of professors and instructors with training on how to use digital tools and have gone from more than 50% to nearly 80% digital in the higher ed space.***

As part of these rapid transitions, Bloom said they have focused on reassuring parents "that using a platform will protect the privacy of their children and that the teacher is still ... in control of the education." McGraw Hill signed the student privacy pledge introduced by the Future of Privacy Forum and the Software & Information Industry Association as part of this confidence-building effort.

Privacy leaders across industry sectors felt these commercial changes brought on by the pandemic would be long lasting, if not permanent, though some acknowledged that their crystal balls were a bit blurry at the moment. In part three of this series, we'll discuss privacy leaders' thoughts on what the new reality might look like and its implications for privacy practices and programs.



Contacts

Tony de Bos
Global Data Protection & Privacy Consulting Leader
Tony.de.Bos@nl.ey.com

Angela Saverice-Rohan
EY Americas and FSO Privacy Leader
Angela.SavericeRohan@ey.com

Caitlin Fennessy
IAPP Research Director
caitlin@iapp.org

Müge Fazlioglu
IAPP Senior Westin Research Fellow
mfazlioglu@iapp.org