

Privacy Leaders' Views

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

By IAPP Research Director Caitlin Fennessy, CIPP/US

Privacy Leaders' Views

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

By IAPP Research Director Caitlin Fennessy, CIPP/US

“Everything has changed. Nothing has changed.” U.K. Information Commissioner Elizabeth Denham’s sentiments on the impact of COVID-19 on data protection encapsulate well those voiced by privacy leaders around the world.

During the summer of 2020, the IAPP and EY launched the second phase of a research initiative aimed at understanding the implications of COVID-19 on privacy priorities, practices and programs by conducting interviews with 21 privacy leaders from around the world. The first phase of the joint research initiative featured [a survey of more than 900 privacy practitioners](#), exploring data protection issues related to working from home, monitoring employee health, and sharing data with governments, researchers and public health authorities to combat the pandemic.

Building on the initial survey findings in this second phase, the IAPP and EY sought privacy leaders’ views on the top privacy challenges stemming from COVID-19, the privacy implications of potentially permanent changes in our way of working, the impact of the pandemic on privacy programs and budgets, how to increase consumer and employee trust amid an increase in data processing, necessary legislative changes, and regulators’ enforcement priorities.

We captured privacy leaders’ thoughts, experiences, challenges and recommendations in a five-part series on COVID-19, introduced here. Four additional pieces will follow, offering privacy leaders’ insights on companies’ immediate COVID-19 response; the new reality and strategic priorities; surveillance and data sharing for the public good; and the actions needed by companies, legislators and regulators to build trust moving forward.

Introduction

Privacy leaders across disciplines and around the world agree principles-based data protection laws and mature privacy programs have proven resilient in the face of innumerable data protection challenges brought on by COVID-19. They agree that as data processing to track and trace ramps up and our lives and identities are digitized, privacy is transcendent.

But, their views on the top privacy priorities and challenges stemming from COVID-19 diverged. Their perspectives reflect their vantage points and the role each plays in shaping and responding to the new reality brought on by the pandemic.

Practitioners implementing privacy on the ground across business sectors focused on the most immediate challenges, highlighting employee privacy protections and virtualization challenges as the top priorities as they prepared for work-from-home and return-to-work transitions. They expressed gratitude that privacy remains a strategic business

priority and that their teams have not been disproportionately impacted by budget cuts.

Policymakers, regulators and academics focused on bigger-picture societal concerns and cited the increase and normalization of surveillance — by governments and commercial actors — as their top priority. Still, they acknowledged the myriad practical challenges organizations face as a result of the pandemic and discussed the flexibility and guidance they have provided to assist in their data protection efforts.

The narratives of both groups intersected when discussing one type of “surveillance,” specifically, “data sharing for the public good” and the role companies have played in sharing commercial data or developing applications to help governments fight the pandemic. These shared responsibilities then teed up questions and ideas about how privacy leaders in government and industry should respond and legislative and enforcement priorities should shift to enhance individual trust in how personal data is processed in times of crisis and in the new more virtual reality.

Privacy leaders' views on the top privacy priorities and challenges stemming from COVID-19 diverged



Practitioners implementing privacy on the ground across business sectors focused on the most immediate challenges, highlighting employee privacy protections and virtualization challenges as the top priorities as they prepared for work-from-home and return-to-work transitions.

Policymakers, regulators and academics focused on bigger-picture societal concerns and cited the increase and normalization of surveillance — by governments and commercial actors — as their top priority.

The IAPP and EY are grateful to the following privacy leaders for sharing their thoughts, experiences and expertise with the privacy community on these critical issues. Following is a glimpse of the key takeaways they shared, with more details to come in the pieces ahead. Thank you, as well, to Nathan Kanter, IAPP's legal extern, for his invaluable research assistance.



Vivienne Artz, chief privacy officer, Refinitiv



Peter Lefkowitz, CIPP/US, chief privacy and digital risk officer, Citrix



Amit Ashkenazi, head of the Legal Department, Israel National Cyber Directorate



Caroline Louveaux, CIPP/E, CIPM, chief privacy officer, Mastercard



Andy Bloom, CIPP/E, CIPP/US, CIPM, CIPT, FIP, vice president and chief privacy officer, McGraw Hill



Kirk Nahra, CIPP/US, partner and co-chair of the Privacy and Cybersecurity Practice at WilmerHale, adjunct professor at Washington College of Law



Jared Bomberg, senior counsel, U.S. Senate Committee on Commerce, Science, and Transportation



Timothy Noonan, deputy director for health information privacy, Office for Civil Rights, U.S. Department of Health and Human Services



Rohit Chopra, commissioner, U.S. Federal Trade Commission



Noah Phillips, commissioner, U.S. Federal Trade Commission



Lorrie Cranor, CIPT, professor of Computer Science, Engineering & Public Policy and CyLab director, Carnegie Mellon University



JoAnn Stonier, CIPM, chief data officer, Mastercard



Elizabeth Denham, commissioner, U.K. Information Commissioner Office



Scott Taylor, vice president of privacy and global functions compliance, chief privacy officer, Merck



Patrice Ettinger, CIPP/US, chief privacy officer, Pfizer



Eduardo Ustaran, CIPP/E, partner, Hogan Lovells



Eric Goldman, professor of law, Santa Clara University



Sophie i'nt Veld, European Parliamentarian



Tony Lam, Deputy privacy commissioner for personal data, Hong Kong, China



Ruby Zefo, CIPP/US, CIPM, FIP, chief privacy officer, Uber

Key takeaways

- > With increased data collection to track, trace and digitize, COVID-19 mainstreamed privacy and ensured it will remain a strategic priority for organizations moving forward.

Citrix Chief Privacy and Digital Risk Officer Peter Lefkowitz, CIPP/US, said, "If you go back 15 years in privacy, boards had a member who knew how to spell privacy Today, I get out in front of the board and usually within about 10 minutes of the start of the discussion some board member will say, 'Well, is that legal under privacy laws?'...You sort of want to get up and hug them, but you can't because of COVID."

- > The pandemic shone a spotlight on employee and health privacy rules and exposed some gaps in legal protection and trust, particularly in the United States.

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."

- > Organizations fast-tracked virtualization efforts to maintain engagement with customers and employees, requiring greater attention to communications platforms' and cloud providers' privacy and security protections.

Refinitiv Chief Privacy Officer Vivienne Artz said, "We were already on a digital journey. What (COVID-19) has done is to accelerate that."

- > The new, more virtual reality will impact all aspects of the business, requiring careful consideration of how we maintain privacy values and avoid biased uses of the troves of new data generated.

Uber Chief Privacy Officer Ruby Zefo, CIPP/US, CIPM, FIP, expects "more profiling, more

attempts to predict people's behavior[T]hat's all good-natured in the sense that we want to satisfy more needs, but it brings privacy challenges with it, to make sure that people are not doing things in a biased way or all the other problems that can come along with profiling people."

- > Surveillance has been normalized across all aspects of our lives, while its efficacy is being questioned.

Hong Kong Acting Privacy Commissioner Tony Lam said, "During the pandemic, people are scared so they are more willing to provide such data ... in the end, people will want to know if you produced results."

- > Regulators have doubled down on providing organizations a guiding hand, focusing enforcement resources on those taking advantage of vulnerable populations.

U.K. Information Commissioner Elizabeth Denham said, "Invite the ICO into the tent ... Getting ICO involved is a badge of public trust It has never been about enforcement and compliance. It is about catching the issues further upstream before something goes wrong."

- > Building trust in data protection during a pandemic is no different than during normal times, requiring organizational commitment to privacy principles, technical protections and a strong legal backstop.

U.S. Federal Trade Commissioner Rohit Chopra said, "I think post-Cambridge Analytica, consumers or the public essentially feel powerless They feel that wherever they go, online especially, their data is going to be extracted from them, and many have simply given up. So, I'm not really sure organizations can do much to increase trust. Ultimately, we're going to need laws to be passed and those laws to be enforced."

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