PART 5 – BUILDING TRUST THROUGH INDUSTRY ACTION, LEGISLATION AND ENFORCEMENT

EY Building a better working world

iapp

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, with an introduction, immediate response, new reality and strategic priorities, and surveillance and data sharing for the public good covered previously. In this final piece, we share their insights on how companies, legislators and regulators can build trust in data protection moving forward.

Building trust

Only about half (57%) of consumers globally trust health care organizations collecting data for public health initiatives to use personal data as they have stated and for no other purpose, according to findings in EY's recent survey of more than 1,900 consumers. That percentage is lower for government data collection (53%) and drops precipitously for online retailers (40%), search engines (32%) and social media platforms (28%). U.S. respondents are even less likely to trust the government to use their data only as promised (43%). FIGURE 1

To address this trust deficit during the pandemic and beyond, privacy leaders said industry, policymakers and enforcement authorities must all pitch in.

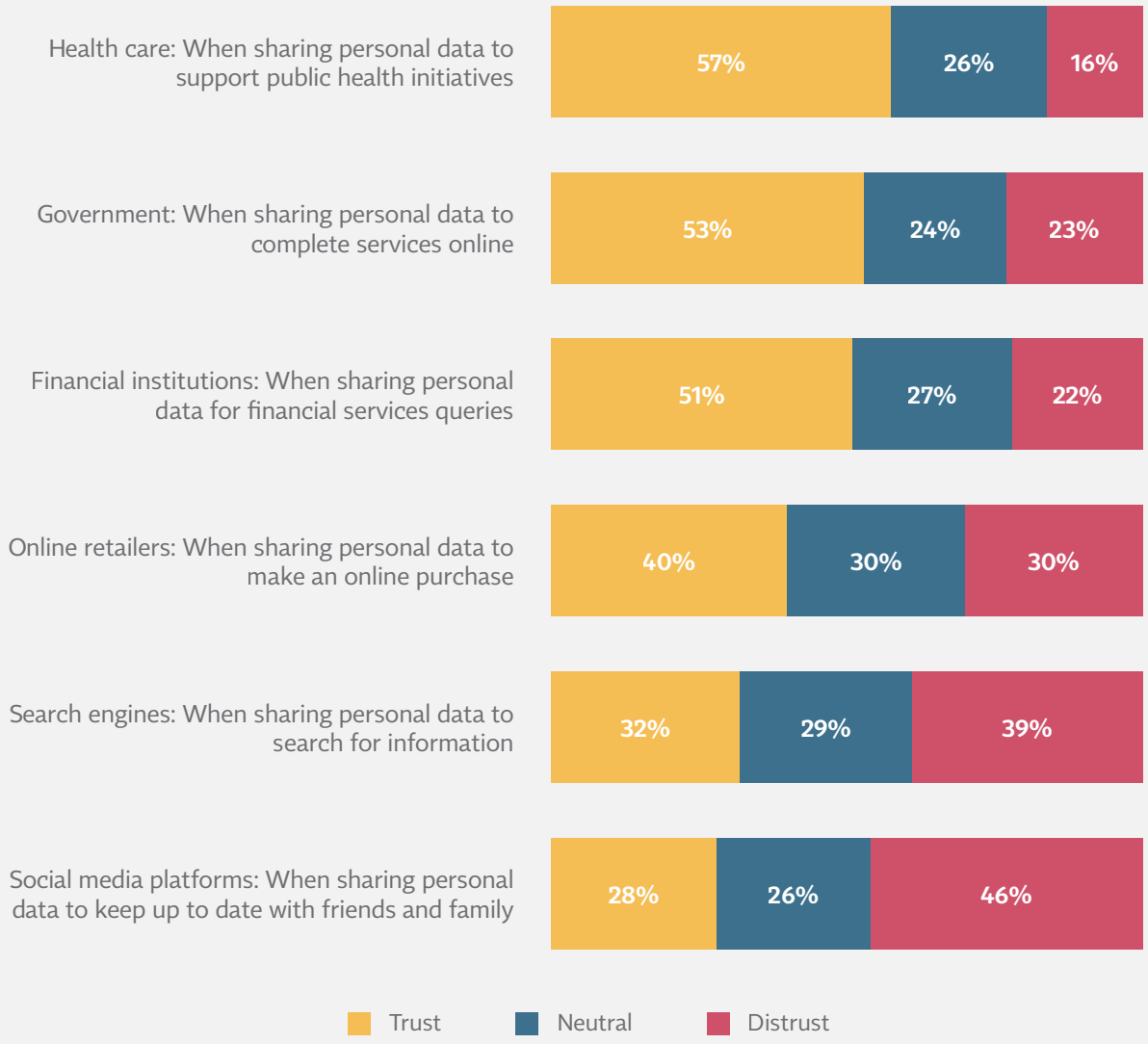
Industry action

In terms of organizations' response, many privacy leaders are leaning in on the old standbys of transparency and communication. Others are more focused on data ethics, purpose limitations, user-centric design and technical controls.

Privacy leaders in industry, academia and government suggested transparency about what personal data is collected and why has been a critical first step to build trust among employees and customers during COVID-19. They also recommended close collaboration and communication with all impacted departments, including HR and tech teams, to ensure everyone understands the what and why surrounding health data collection so they can jointly determine the how. Privacy

FIGURE 1

Percentage of respondents that trust the following organizations to use their personal data as stated and not for anything else



leaders also urged creativity in communications, noting that short and snappy is more effective in a virtual environment. FTC Commissioner Noah Phillips pointed to the creativity employed in marketing efforts, recommending as much ingenuity should go into communicating about privacy.

Others felt it was important to go further, that the same suite of fair information practice principles must be deployed to build trust during a pandemic and more normal times. Policymakers and practitioners recommended greater attention be paid to data ethics and user-centric design processes that provide individuals actionable notice and choice. They pointed to the need for clear and necessity-based use limitations when collecting COVID-19-related data. In speaking of data ethics, they focused on benefits for individuals, bias avoidance, reputable data sources, respect, fairness and accountability. They

also suggested considering the alignment of individual and business incentives, noting it is more difficult to build individual trust in data collection for "the public good" by companies whose business model relies on data monetization. These insights align with those shared by consumers themselves — in response to EY's recent consumer survey — that user control, security, reputation, transparency and personal benefits all factor into individuals' trust. FIGURE 2

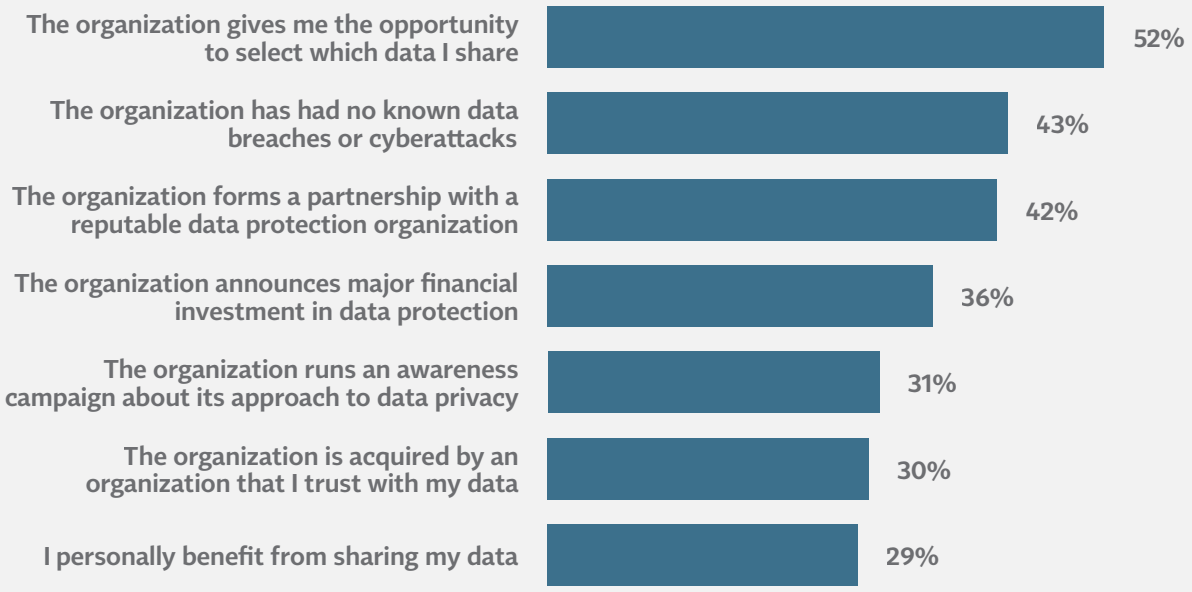
Finally, some privacy leaders argued companies cannot overcome the trust deficit independently. They spoke of the need for technological solutions to make personal data elements inaccessible to those who do not need them or for unapproved purposes. They also argued that a legal backstop is paramount.

Eric Goldman, a privacy professor at Santa Clara University, suggested technologies that prevent data misuse are the only viable solution at this stage. "I think we've reached a world in which we no longer trust entities that need our trust to function properly," he said. "What we need is industrial-grade technology that can't be abused even if the laws and workflows fail."

U.S. Federal Trade Commissioner Rohit Chopra agreed organizations are incapable of overcoming the trust deficit independently, but like other government officials around the world, suggested that privacy laws and enforcement have a critical role to play. "I think post–Cambridge Analytica, consumers or the public essentially feels powerless," he said. "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."

FIGURE 2

Factors most likely to increase the level of trust consumers place in organizations to collect, store and use their data



Legislation

Policymakers and regulators shared their thoughts on the efficacy of current laws and enforcement regimes and the changes needed to protect privacy and combat the current or future pandemics. In general, they agreed that a legal backstop is necessary to ensure that abuse of personal data by industry or government actors is identified and punished. They made clear this need is not driven by the pandemic, but that the current crisis has exposed gaps in data protection laws and laid bare how crucial trust in that protection is to efforts to stop the spread of the virus. In some jurisdictions, policymakers and regulators felt the existing legal regime provided the necessary protections and flexibility, while in others, they recommended adjustments both small and big.

U.S. privacy leaders were more likely to suggest the need for legislative action than their counterparts overseas.

U.S. policymakers and regulators pointed to three specific areas in need of scrutiny. First, U.S. officials acknowledged the limited nature of the Health Insurance Portability and Accountability Act and the demand for a regulatory framework to protect the sensitive information flowing through health apps. Timothy Noonan, deputy director for health information privacy at the U.S. Department of Health and Human Services, said this has been an area of "growing concern," including as pandemic-related health data collection has ramped up.

Second, some U.S. policymakers raised the need for specific legislation to build trust in contact-tracing apps. Jared Bomberg, with the U.S. Senate, explained "the biggest barrier to adoption (of contact-tracing apps) is privacy concerns," which is why, he said, Sens. Maria Cantwell, D-Wash., Bill Cassidy, R-La., and Amy Klobuchar, D-Minn., introduced the bipartisan Exposure Notification Privacy Act.

Third, U.S. privacy leaders recognized the current health privacy debate is an offshoot of the broader legislative debate about the need for an omnibus federal privacy law. They suggested the adoption of a broad-based federal privacy law would help remedy the trust deficit evident during the pandemic but also noted the politics surrounding the adoption of such a law have hindered progress of more targeted legislative efforts.

Policymakers and regulators outside of the U.S. spoke more about the flexibility that existing principles-based laws provide to address a public health crisis and more minor recommendations for change.

> ***Europe-based officials suggested the EU General Data Protection Regulation provides both strong protections and needed flexibility. "We have the best law in the world," EU Parliamentarian Sophie in't Veld said. "The idea that the GDPR or privacy rules are in the way of measures is complete and utter nonsense."***

While citing some legislative gaps, policymakers and regulators in the U.S., EU and Asia all agreed that greater enforcement of existing laws and enforcement resources are also needed.

Enforcement priorities

Privacy regulators recognized laws are only as strong as their enforcement and readily discussed their enforcement efforts and priorities in the time of COVID-19. Here they demonstrated less geographic diversity.

Regulators in the U.S., U.K. and Hong Kong expressed similar views about the need for investigatory and prosecutorial discretion where organizations are making good faith attempts to protect individuals' and societies' health and safety and might unintentionally make some privacy missteps along the way.

For example, FTC Commissioner Phillips said a high school principal shouldn't spend too much time worrying about compliance. "If you're saying, there's just so much going on that no one's going to notice if I break the law, that's different," he said. This was the motivating sentiment behind the "notification of enforcement discretion" the U.S. Department of Health and Human Services announced in targeted areas, including the good faith provision of telehealth, the disclosure of protected health information by business associates for public health, and the good faith operation of COVID-19 testing sites, as Timothy Noonan at HHS explained. A major question privacy professionals are raising now is how long such discretion might last. Noonan said HHS is considering whether anything should be made permanent. He expects to receive a significant amount of public feedback on both sides of that question.

Regulators indicated that, in addition to these "proportional" approaches to enforcement, they are shifting their priorities. Regulators in the U.S. and Europe said they will focus considerable attention on those who are taking advantage of vulnerable groups during the pandemic. They also expect to focus more on digital service providers, social media and those collecting children's data, given that many individuals' lives and children's education has moved online. FTC Commissioner Chopra stressed the importance of monitoring the shift in engagement to the online world. "There's an expectation that this is going to be a huge boon … to traditional social media. Engagement is going up. … So you will certainly see greater interest from all of them in taking advantage of this moment to harvest more data, to combine more companies into their empires. A strong focus on the dominant players — I think it's just going to have to increase," he said. Regulators also plan to monitor health data services, biometric data collection and the use of artificial intelligence closely and are increasing their technical capacity accordingly.

Some regulators made clear their preferred approach is more carrot than stick. They are prioritizing early engagement to avoid later harms and working to support organizations engaged in new data collection to help combat the pandemic, as well as smaller companies launching during a challenging moment but pivotal to economic recovery.

In many instances, this has led to a significant amount of bespoke guidance. That guidance has focused in large measure on the necessity and proportionality of data collection, use and sharing. In other instances, it has led to early engagement between regulators and companies prior to the launch of new technologies. Such engagement, regulators said, allows them to offer guidance during application development stages and reassure the public after the fact that apps are safe and work as advertised.

Several countries have sought engagement from authorities prior to launching contact-tracing apps, in particular. U.K. Information Commissioner Elizabeth Denham advocated for such an approach. "Invite the ICO into the tent. … Getting the ICO involved is a badge

of public trust," she said. "It has never been about enforcement and compliance. It is about catching the issues further upstream before something goes wrong."

These collaborative and guidance-driven regulatory approaches are not limited to times of crisis but can be particularly reassuring to the public in such instances.

Conclusion

As policymakers, regulators, academics and practitioners work to respond to COVID-19, the landscape of privacy challenges, data needs and regulatory guidance continues to shift. Kirk Nahra, CIPP/US, a partner at WilmerHale and privacy professor, pointed to the evolution of regulator guidance that he and privacy practitioners across industry have watched and reacted to in real time. "Originally, we wouldn't have let you do X, but now we know you need to do X, so that's OK as long as you don't do it badly," he said. Spoken with a touch of humor, Nahra's comments capture the proportional approaches and support authorities have tried to offer those working hard to keep their footing in the whirlwind brought on by the pandemic.

As we conclude this series on privacy leaders' views on the impact of COVID-19 on privacy priorities, practices and programs, we are struck, once again, by the resilience of privacy principles and practitioners. Privacy professionals in industry, government and academia made clear the data protection principles that underpin hundreds of laws and thousands of privacy programs have served us well during the pandemic. Privacy leaders said continued application of those principles, within companies and by public authorities, is a must to build trust in industry and governments efforts to combat the virus. But, they also said changes brought on by the pandemic demand creativity and evolution in how those principles are applied, by companies and regulators. The virus forced them to focus less on process and protocol and more on providing actionable protections that instill confidence in necessary services and data processing.

Privacy leaders said they have been able to "pivot" and "accelerate" to provide "flexibility" and "discretion." These somewhat euphemistic terms repeated by many seem to belie the complete transformation of our lives and economies, the shifts to virtual, digital and quarantined with huge implications for data use and sharing and for commercial and governmental surveillance. And yet, perhaps, as a profession in which change has long been the defining features, the privacy profession was better prepared than most to weather the storm. European Parliamentarian Sophie i'nt Veld put it well when she said, "Privacy rules weren't designed for sunny weather. They were designed for bad weather, turbulence." Privacy leaders across disciplines agreed.

As our societies continue to ramp up data processing to enable work from home, return to work, remote schooling, virtual connection and a host of efforts to combat the pandemic, we can and must find new and creative ways to maintain our core privacy principles. Those principles will be equally important as our societies consider what data processing to dismantle and which elements of our new reality we wish to retain.

EY Building a better working world

iapp

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