mlex
a LexisNexis company

DATA PROTECTION
SPECIAL REPORT
APRIL 15, 2022

Closing the Global Gaps in Data Protection

Comprehensive coverage of the International Association of Privacy Professionals global summit 2022 examining emerging regulatory trends and tensions

INSIGHT | COMMENTARY | ANALYSIS

Editor's Letter

Mike Swift
Chief Global Digital Risk Correspondent

Microsoft President Brad Smith summed it up well. When MLex asked why he decided to air his proposal for a US digital regulator at the International Association of Privacy Professionals Global Privacy Summit, he said: "This is a global conference, and I think this is very much a global question."

From a gathering of a few hundred people in a hotel lobby when MLex began covering the IAPP's annual summit almost a decade ago to the 4,500 in Washington this week, the summit's growth mirrors the growing regulatory importance of data protection. In the three years since the last in-person event, IAPP membership has grown from about 50,000 to nearly 75,000.

Those years obviously spanned the global pandemic, and there were emotional reunions as attendees found familiar faces, even if some were still behind a mask. Over three days, they also discussed next steps in a legal framework for EU-US data transfers, agreed on the critical need to keep children and their data safe online, and heard strategies to avoid regulatory risk from flawed or unfair decisions made by AI algorithms.

The speakers' prominence underscored the growing regulatory importance of privacy and data security. Apple CEO Tim Cook sought to enlist the privacy community to push back against antitrust-fueled efforts in Europe and the US to force Apple to allow apps from outside into its closely curated App Store. Reform-minded US Federal Trade Commission chairwoman Lina Khan, who came to prominence on her antitrust scholarship, delivered her first privacy-focused speech, saying it would continue its quest for innovative enforcement strategies in the digital space. New UK Information Commissioner John Edwards said his office would stick to a risk-based approach, with a focus on enforcing its Children's Code. Christopher Hoff, the lead US negotiator in the effort to replace the EU-US Privacy Shield, saw relief at hand for company lawyers anxious about the legal basis for trans-Atlantic data flows. And Microsoft's Smith predicted that Canberra, Brussels, Seoul or London will likely beat Washington to the idea of creating a specialized digital regulator, but that it is a global regulatory idea whose time would inevitably come.

MLex journalists from bureaux in North America and Europe attended nearly all of the multitude of panels and networking events and revived face-to-face relationships with their broad base of regulatory, competition and legal contacts. We are delighted to present you with our reports, giving you our unrivaled insight, analysis and commentary on key global data protection themes. Tune in also to our podcast wrapping up the week — see page 4.

To inquire about our coverage, including the portfolios that accompany our articles, or to find out more about our subscriber services, see page 3 or visit our website, mlexmarketinsight.com. ■

MLex Insight • Commentary • Analysis

Confidently Navigate and Respond to Regulatory Risk

Stay ahead of key regulatory issues with expert insight, commentary and analysis to ensure you are advising your clients on how to best navigate complex, global enforcement environments. MLex is on the cutting edge of reporting on global regulations, both in effect and proposed. Our exclusive, real-time coverage of probes, enforcement trends, litigation and regulator commentary help ensure you are informed and able to respond immediately to client risks and opportunities.

The MLex Difference

- We have a singular focus on regulatory risk, providing unrivalled expertise across our team of 80+ reporters around the world.
- Through longstanding relationships with regulatory communities we keep you informed of developments ahead of mainstream media.
- We insist on the highest standards of sourcing and accuracy in our editorial process.
- Unbiased and forensic reporting ensures our clients get the information they need.

Our Global Presence

Our journalists cover the world from 14 bureaux in key jurisdictions:
EUROPE: Brussels • London **AMERICAS:** Washington • New York • San Francisco • São Paulo
ASIA-PACIFIC: Hong Kong • Beijing • Shanghai • Seoul • Tokyo • Jakarta • Melbourne • Sydney

mlex
a LexisNexis company

UK +44 800 999 3237
US +1 800 356 6547
EU +32 2 300 8250
HK +852 2965 1424
www.mlexmarketinsight.com
customerservices@mlex.com

Contributors

Ana Paula Candil
Senior Correspondent, Latin America
Ana Paula joined MLex in Brazil in 2014 writing about antitrust investigations and merger reviews. Prior to that, she worked for several trade publications and in TV. She lived in Washington, DC, where she worked for Al Jazeera English in 2010. She studied journalism and holds a postgraduate diploma in International Business Management from the George Brown College in Toronto.

Sam Clark
Correspondent, London
Sam has covered data privacy and security in the UK and Ireland for MLex since November 2021. He previously covered data protection for trade publication Global Data Review, as well as reporting on technology, media and telecoms businesses for S&P Global. He has a bachelor's degree in history and a master's degree in journalism, both from the University of Kent.

Claude Marx
Correspondent
Claude Marx has been a reporter for FTCWatch since February 2013 and has written on a range of subjects such as the implications of certain mergers on consumers, the regulation of advertising and attempts by Congress to overhaul the patent system. He also writes regularly for MLex. Before that, Claude spent four years writing about the impact of legislation and regulations on community banks and credit unions as the Washington reporter for *Credit Union Times*, where he covered the government's rescue of some of the financially troubled wholesale credit unions. He earned his bachelor's degree from Washington University in St. Louis and did graduate work at Georgetown University.

Amy Miller
Senior Correspondent, San Francisco
Amy is responsible for the coverage of an array of regulatory and litigation issues pertaining to the Internet, including privacy, data security and antitrust. Formerly a legal reporter for the ALM media group, Miller has closely followed legal trends in Silicon Valley and covered corporate legal departments for online and print publications including The American Lawyer, Corporate Counsel, and The Recorder. Miller is a graduate of Columbia University Graduate School of Journalism and is an award-winning journalist with expertise ranging from education and legal reporting to computer-assisted reporting.

Matthew Newman
Chief Correspondent, Europe
Matthew wrote about mergers, antitrust and cartel investigations before turning his focus onto digital risk. He began covering competition at the Luxembourg courts in 2004 and then moved to Brussels. After working as a spokesman for the European Commission until April 2012, he spent several months in Washington, DC, writing about mergers for MLex. He spent a year studying French, history and communications in Grenoble, France and is a graduate of Boston University with degrees in history and journalism.

Dave Perera
Senior Correspondent, Washington
Dave joined the Washington, DC, office as a technology reporter as we built that part of our coverage. He is a veteran cybersecurity reporter for Politico and a former editor for FierceMarkets publications. Dave studied Spanish and Italian literature at the University of Colorado, and has a Master's degree from the Columbia University School of International and Public Affairs.

Mike Swift
Chief Global Digital Risk Correspondent
Formerly chief Internet reporter for the San Jose Mercury News and SiliconValley.com, Mike has covered Google, Facebook, Apple and other major Silicon Valley companies closely as he followed trends in search, the mobile web and online social networks. He helps coordinate MLex coverage of privacy and data security worldwide. A former John S. Knight Fellow at Stanford University, he is a graduate of Colby College. He is an award-winning journalist with expertise ranging from the business of professional sports to computer-assisted reporting.

Khushita Vasant
Senior Correspondent, Antitrust
Khushita covers US antitrust enforcement and litigation. Formerly in Brussels writing about antitrust and mergers for PaRR, she has covered the EU's actions against Google, Apple, Facebook and Amazon, to name a few. Khushita specializes in tech and patent policy coverage, which featured in the Concurrences Antitrust Writing Awards. Previously, as a financial journalist for The Wall Street Journal and Dow Jones Newswires, she wrote about monetary policy and the bond and currency markets. Khushita studied journalism at Mumbai University, and received an Erasmus Mundus scholarship for a joint master's degree from universities in Germany and Austria.

Contents

US FTC's Khan vows 'swift and bold' action on privacy

By Dave Perera & Matthew Newman

Published on April 11, 2022

US Federal Trade Commission Chair Lina Khan pledged "swift and bold action" on privacy, telling an audience in Washington, DC, that the agency may reassess the way it evaluates whether particular conduct is unlawful.

Khan's speech — billed as the antitrust-focused chair's first major address on privacy — was short on detailed policy proposals but included a denunciation of notice and consent as likely "outdated and insufficient" for consumers who can't reasonably fail to accept the privacy policies offered by dominant tech companies.

Going forward, the agency should "approach data protection and security protections by considering substantive limits, rather than just procedural protections," she said during her 14-minute speech.

The agency must grapple with "whether certain types of data collection and processing should be permitted in the first place," she added.

The Democratic chair didn't elaborate on how the FTC would accomplish a shift away from privacy enforcement that typically requires a company to be caught in a deception before enforcers act. Khan didn't take questions from reporters.

"Privacy legislation from Congress could also help usher in this type of new paradigm," she allowed.

Earlier in the speech, Khan said the agency may issue rules limiting private sector surveillance and regulating security practices — although fellow Democratic Commissioner Rebecca Slaughter recently appeared to place limits on the scope of FTC privacy rulemaking in stating that FTC regulations aim to clarify existing illegal practices rather than create new rights.

Khan portrayed the fight over privacy in dramatic terms, saying today's granular level of commercial data collection used for individual targeting puts into question "one's freedom, dignity and equal participation in our economy and our society." ■

EU, US still have 'a lot of work' before trans-Atlantic deal on data flows can be finalized this year, Reynders says

By Matthew Newman

Published on April 12, 2022

EU and US officials still have "a lot of work to do" after an EU-US data-flow framework was announced last month, with several important steps needed before the trans-Atlantic data flow agreement can be formally adopted later this year, EU justice chief Didier Reynders said.

On March 25, the two sides announced a successor deal to replace the Privacy Shield, the previous agreement struck down by EU judges in 2020 after they found that the transfer of EU citizens' personal data to the US didn't comply with the bloc's privacy rules.

Reynders, speaking today via video to the IAPP Global Privacy Summit in Washington, DC, said there's a "multi-step process" before the Trans-Atlantic Data Privacy Framework "could be finalized by the end of this year."

"While we still have a lot of work ahead of us, I do believe that this agreement in principle confirms once more how much the European Union and the US can achieve by building on their shared values," Reynders said.

US President Joe Biden and European Commission President Ursula von der Leyen hailed the agreement as a "major breakthrough" that would unblock data flows underpinning $7.1 trillion worth of trade with the EU.

Reynders said the process includes an opinion from the European Data Protection Board — the umbrella group of the national data protection authorities — as well as a vote by EU governments and scrutiny by the European Parliament.

"It is difficult to give a precise timeline at this stage, but we expect that this process could be finalized by the end of this year," Reynders said.

The EU must adopt an "adequacy" decision, in which it declares that the US provides adequate protection to EU citizens' data that is exported to the US.

The draft agreement needs to be translated into legal texts. It also requires an executive order by the US president, as well as an order "implementing regulations," Reynders said. ■

Microsoft's Smith urges compromise on US privacy law, suggests digital regulator

By Sam Clark, Mike Swift & Matthew Newman

Published on April 13, 2022

US lawmakers must find compromise on a federal privacy law to avoid falling further behind the rest of the world, and one way forward might be to create a US digital regulator, Microsoft President Brad Smith said.

Smith, who first called for privacy regulation 17 years ago, again urged the US Congress today to implement federal privacy legislation, criticizing lawmakers' inability to compromise. "Comprehensive privacy legislation for the US is not just needed, it's long overdue," Smith told the IAPP Global Privacy Summit.

The tech sector must "mature" and should collectively "lean in to help make a new era of regulation work," he said.

Microsoft, alongside Apple, has recently sought to position itself as a promoter of fundamental rights, with privacy as a major focus. Smith pushed back on the notion that regulation can become a competitive advantage and will benefit some companies over others.

"We need to recognize that the need to serve the common good vastly outweighs the regulatory

opportunities for competitive advantage," he said. "The reality is regulation applies to everyone, and there will be only … very short periods of time when one company or part of the industry benefits at the expense of another."

Smith noted that 120 jurisdictions globally have passed privacy or data protection laws. "The US increasingly stands alone," he said.

"The fact of the matter is, in my view, there is a critical element that we are failing to think about … that the failure of the US to legislate doesn't stop global regulation. It doesn't even slow it down. It just makes our country less influential in the world," he said.

DIGITAL REGULATOR

The US could benefit from a digital industry-specific regulator, Smith said, noting that many other industries and inventions, such as cars and phones, have specific regulators. He raised the prospect of a "Digital Regulatory Commission," saying such a body could create a more coordinated set of rules than "piecemeal" legislation.

> *"The need to serve the common good vastly outweighs the regulatory opportunities for competitive advantage. The reality is regulation applies to everyone, and there will be only … very short periods of time when one company or part of the industry benefits at the expense of another."*

In an interview with MLex on the sidelines of the conference, Smith said his view is that the digital regulator might take oversight of digital privacy and security issues, artificial intelligence, children's online safety and issues around the lawful access to data by governments. He said he wouldn't favor having the digital commission function as a tech antitrust regulator, however.

"I think it's way too early to actually offer a view of what it would look like or how would it work. But at the end of the day, having a regulator that is deep in the industry I think is pretty much the norm for how complicated industries are regulated," Smith said, noting "sophisticated, well-informed regulators" like the Federal Aviation Administration for air travel and the Food and Drug Administration for food and pharmaceutical issues.

"I think we could well find ourselves in the next couple of years reaching a point where it could make

more sense to give broad regulatory authority to an agency, perhaps a new agency," Smith said. "It wouldn't supplant the antitrust issues" at the Federal Trade Commission or the Department of Justice, "but in many of these other fields, they could go to work."

A dedicated digital regulator "is the natural evolution" in what's happening in the UK in the cooperation there between the national privacy and antitrust regulators, he said. "I think we're going to see one or more governments adopt this. The question is which government will go first. These days it's usually not the United States, but then the question becomes, 'When does the US focus on this as well?'"

Asked if other large tech companies are likely to join his call, Smith said, "I wouldn't hold my breath," but he added that regulatory innovation in the 21st century is more likely in capitals such as Canberra, Brussels, Tokyo, London or Seoul than in Washington, DC.

STATE LAWS

In his remarks to the conference, Smith said that the two issues at the heart of the privacy legislation deadlock in Congress — a private right of action and pre-emption of state laws — "have been part of every consumer protection law in the US for more than a century."

So far, four states have passed comprehensive privacy laws – California, Virginia, Colorado and Utah. Only California's law has taken effect, but the state's voters passed an updated version — the California Privacy Rights Act — in 2020 that will take effect in 2023. Other state legislatures are considering comprehensive legislation as well, and could act as soon as this year.

The laws generally give consumers new privacy rights of access, transparency and deletion, as well as the ability in many cases to restrict the sale of their personal data to third parties.

California's law, which included the creation of the first sole-purpose data protection authority, is generally considered the most strict and prescriptive, while laws passed in Utah and Virginia are considered more business-friendly. ■

Attitudes shifting on prospective federal privacy legislation, congressional staffers say

By Amy Miller

Published on April 12, 2022

Attitudes are shifting on Capitol Hill when it comes to prospective federal privacy legislation, Senate and House committee staffers said today. Now, lawmakers and staffers are more willing to compromise, they said.

Recent testimony from Facebook whistleblower Frances Haugen helped persuade lawmakers to renew serious efforts to compromise on prospective legislation, and abandon "hardline" stances on issues such as a private right of action and preemption of state privacy laws.

"There's been a real, noticeable change in attitude," said John Beezer, a senior advisor to Democrats on the Senate Commerce Subcommittee on Consumer Protection.

State privacy legislation is also having an impact, they said. Four states have enacted consumer privacy laws and more are likely to follow.

"States have really shown us a lot of the options, and we can choose the best," said Timothy Kurth, chief Republican counsel for the House Energy and Commerce Subcommittee on Consumer Protection.

Beezer agreed, saying that "definitely the states are encouraging stakeholders to be more flexible."

At the same time, the weaker state laws are persuading lawmakers to take stronger action, said Syd Terry, chief of staff to Democratic Congresswoman Jan Schakowsky, chair of the House Energy and Commerce Subcommittee on Consumer Protection.

For example, Virginia's state law is "incredibly permissive" and effectively "rubber stamps" current business practices, he said.

"We need to strive a lot higher in terms of what the states have done," he said.

But staffers said that talk of new privacy rules from the US Federal Trade Commission is unlikely to push Congress to act soon. The FTC rulemaking process could take years and would likely result in multiple lawsuits, they said.

And even if the FTC did act, the agency doesn't have authority over all industries, they said.

"It's not an either-or situation," Beezer said. "They need to do their job, and we need to do ours, and hopefully good things will happen." ■

Apple CEO Cook says proposed US, European antitrust rules on 'sideloading' would sacrifice privacy

By Mike Swift, Sam Clark & Matthew Newman

Published on April 12, 2022

Lawmakers in the US and Europe are failing to properly balance the values of privacy and competition, Apple Chief Executive Tim Cook said in a speech today.

Antitrust mandates that would force the iPhone maker to load "unvetted apps" would have "profound" privacy consequences, he said.

In a speech in Washington at the world's largest annual gathering of privacy professionals, Cook reached out beyond his keynote audience — several thousand privacy lawyers in-person and online — to address lawmakers in Washington and Brussels.

"We are deeply concerned about regulations that would undermine privacy and security in service of some other aim," he said. "Here in Washington and elsewhere, policy makers are taking steps in the name of competition that would force Apple to allow apps onto iPhone that would circumvent the App Store."

The practice of "sideloading," Cook said, would mean "data-hungry companies would be able to avoid our privacy rules and once again track our users against their will. It would also potentially give bad actors a way around the comprehensive security protections we put in place, putting them in direct contact with our users."

The Digital Markets Act, which EU negotiators approved last month, establishes a list of obligations with which digital giants labeled as "gatekeepers" must comply in a range of areas including data, default apps, self-preferencing, sideloading, user consent and digital advertising. Similar legislation being considered in the US Congress could also lead to mandates that Apple open its iOS mobile devices to apps from outside the Apple App Store.

Cook said Apple believes in both competition and stronger privacy laws.

"Apple is in favor of privacy regulation," he said today. "We have long been supporters of the GDPR and we applaud the many countries that have enacted privacy laws of their own. We also continue to call for a strong comprehensive privacy law in the United States, and we are grateful for all the global leaders who are working to advance privacy rights, including the rights of children in particular."

But lawmakers are sacrificing user privacy and choice on the altar of competition, he asserted today. "Apple believes in competition. We value its role in driving innovation and pushing us all forward. We appreciate [that] the supporters of these ideas have »»

good intentions. But if we are forced to let unvetted apps on iPhone, the unintended consequences will be profound," Cook said.

Companies such as Epic Games, which challenged Apple's iOS rules in a high-profile antitrust trial in California last year, have criticized the exclusivity of Apple's App Store, contending it allows the company to collect fees that it couldn't otherwise get from developers. Apple's successful deployment of privacy and security as procompetitive defenses in its antitrust trial against Epic, however, was a US judicial first in the view of many.

Cook said today there are already examples of sideloading damaging data security. People using non-Apple devices have downloaded apps that purported to be for Covid-19 tracking, but that in reality were a vehicle for ransomware, he said in an apparent reference to Google's Android devices.

"Proponents of these regulations argue that no harm would be done by simply giving people a choice," Cook said. "But taking away a more secure option will leave users with less choice, not more. And when companies decide to leave the [Apple] App Store because they want to exploit user data, it could put significant pressure on

Cook said today there are already examples of sideloading damaging data security. People using non-Apple devices have downloaded apps that purported to be for Covid-19 tracking, but that in reality were a vehicle for ransomware, he said in an apparent reference to Google's Android devices.

people to engage with alternate app stores, app stores where their privacy and security may not be protected."

Cook sought to enlist privacy professionals to back Apple's push to get policymakers in Washington and Brussels to put more emphasis on privacy as they seek to bolster competition rules.

"We hope all of you in the privacy community will join our effort to make sure that regulations are crafted, interpreted and implemented in a manner that protects people's fundamental rights," Cook said. "Because as much as we all stand to lose in a world without privacy, I know how much we stand to gain if we get this right." ■

US FTC will double down on privacy force multipliers, Khan says

US Federal Trade Commission Chair Lina Khan said the enforcer will continue to select privacy enforcement actions that are force multipliers, confronting not just dominant firms but also middlemen that enable broad harms, executives that engage in harmful conduct and conduct that bridges privacy and antitrust.

"We're seeking to harness our scarce resources to maximize impact, particularly by focusing on firms whose business practices cause widespread harm," Khan said, delivering what was billed as her first pure policy speech on privacy at the IAPP Global Privacy Summit in Washington, DC. "It means tackling practices by dominant firms, as well as intermediaries that may facilitate unlawful conduct on a massive scale."

One example of that kind of enforcement action against a middleman, Khan said, is the FTC's settlement in December with OpenX, which bills itself as the "world's most dynamic ad exchange for data and identity." The ad exchange was hit with FTC allegations that it violated the US Children's Online Privacy Protection Act, using personal data harvested from hundreds of apps directed at children to target ads.

"We intend to hold accountable dominant middlemen for consumer harms they facilitate through unlawful data practices," Khan said.

Second, the FTC has been looking for enforcement actions that straddle the worlds of privacy and antitrust, "assessing data practices through both a consumer protection and competition lens," Khan said. "We are keen to marshal our expertise in both areas to ensure we are grasping the full implications of business conduct and strategies."

The FTC is also focusing on how the agency can handle enforcement actions that feature top executives, as a deterrence. "Where appropriate, our remedies will also seek to foreground executive accountability through prophylactic limits on executives' conduct," Khan said.

An example is the FTC's order last year against SpyFone, in which the FTC banned both the company and its chief executive, Scott Zuckerman, from the surveillance business on allegations they had been secretly harvesting and selling real-time access to personal data.

The FTC is also trying to incorporate the latest privacy and security technology in its orders, such as mandating multifactor authentication in its settlement last month with CafePress.

And the FTC has been focusing on enforcement actions that maximize deterrence by designing remedies that go after the incentives that particularly drive illegal behavior.

One example, Khan said, is the FTC's recent action against Weight Watchers' subsidiary Kurbo, in which the agency forced the company to not only delete personal information it collected without parental consent from children under age 13, but also to destroy any algorithms derived from the data.

"When we encounter law violations, we are focused on designing effective remedies that are directly informed by the various business incentives that various markets favor and reward," Khan said. "This includes pursuing remedies that fully cure the underlying harm and, where necessary, deprive lawbreakers of the fruits of their misconduct." ■

By Mike Swift & Matthew Newman

Published on April 11, 2022

Companies' use of 'legitimate interest' as legal basis for data processing should be resolved this year, Kelber says

Germany's federal data protection commissioner, Ulrich Kelber, said that 2022 will be the year that European regulators or courts will decide whether companies' use of "legitimate interests" as a legal basis for processing data will be upheld under the EU's data protection rules.

Kelber, speaking at the IAPP Global Privacy Summit, said he has doubts about large tech companies' use of legitimate interests for collecting and processing data under the EU's General Data Protection Authority. "The companies collect all the data that they can access on their own apps or they buy it on the market and they tell us that it's all legitimate interest, and it's not," he said.

Under the GDPR, legitimate interests is one of the six lawful bases for processing personal data. It's different from other lawful bases because it's not focused on a particular purpose — performing a contract, complying with a legal obligation, protecting vital interests or carrying out a public task — and it's not processing for which users have specifically given consent.

Companies need to undertake a "balancing test": Is their legitimate interest in processing the data overridden by the user's interests, rights or freedoms?

Some European data protection authorities have been skeptical that a company's interests outweighs a user's interest.

Kelber said that data protection authorities need to resolve this "core issue" that is causing uncertainty in the market. "We have to solve that on certain cases, and 2022 is the year to solve that, and then certainty will go into the market," he said. "You can use these role models for your own business case and for your own technology. You don't have to have a single case decision on that."

Kelber said it will be up to the courts or the data protection authorities to decide on whether the use of legitimate interests complies with GDPR.

He said that a better approach is to have users trust that their personal data isn't abused, such as by having it processed on their devices.

"My experience is if we are involved in a very early stage of creating a business model or introducing new technology to the market, then we can show which cliffs are there, in that deep sea, and which are alternatives to reach the goal you want to have with your business plan," he said.

This is a better alternative than having a court or DPA rule against the data processing, which costs "time, money and trust," he said. ■

By Matthew Newman

Published on April 13, 2022

Compromise on preemption of US state privacy laws possible, privacy experts say

By Amy Miller

Published on April 13, 2022

Each time a new US state enacts privacy legislation, expectations for federal privacy legislation rise, privacy experts said today.

At the same time, ongoing debates over eventually preempting those state privacy laws are making it harder for Congress to enact a federal law, they told the IAPP Global Privacy Summit in Washington, DC.

But there are potential solutions and compromises, and preemption doesn't have to be absolute, they noted.

"It's not a binary thing," said Neil Richards, a professor at Washington University School of Law.

The experts floated several possibilities. Only current state laws could be preempted, and states could still have an option to pass privacy laws in the future, for example, said Kirk Nahra, co-chair of Wilmer Hale's cybersecurity and data practice. Another option is that state laws could be preempted for a limited time period, he said.

"I'm concerned that if we have a federal law that allows unfettered experimentation, we are going to end up with a bunch of bad state laws," Nahra said.

In the meantime, these state laws will continue to build pressure on Congress to act, Nahra said. Whether that results in a privacy law remains to be seen, but next year looks promising, he said.

"I think the sweet spot for federal privacy legislation is going to be next year, he said. ■

US states must coordinate on privacy rules, Colorado AG says

By Amy Miller

Published on April 12, 2022

As more US states roll out new privacy rules and regulations, state regulators will have to coordinate so that businesses don't face a compliance "nightmare," Colorado Attorney General Phil Weiser said today.

Privacy regulators in Colorado, California, Virginia and Utah need to pool their resources and work together to help businesses understand their obligations under each state's consumer privacy law, he said, because if the state privacy laws are too difficult to follow, businesses simply won't comply, Weiser said at the IAPP Global Privacy Summit.

"We want to work hard to get it right, not just in Colorado, but across the nation," Weiser said.

The potential for confusion looms large, he said. The Colorado AG's office is currently soliciting feedback for new rules that will be issued under the Colorado Privacy Act, enacted last year. The California Privacy Protection Agency is also preparing to issue new rules under the California Privacy Rights Act, passed in 2020.

Weiser said he was issuing a roadmap today about how companies and organizations can engage with the AG's office.

"We want your ideas now," Weiser told the standing-room-only crowd.

Differences between California and Colorado's forthcoming rules are to be expected, Weiser said. That means an ongoing dialogue with the California Privacy Protection Agency will be critical if both states hope to succeed, he said. Those difference can't be insurmountable, he said.

"We will learn from what California is doing and engage in a dialogue," Weiser said. "We don't want to make compliance unduly difficult or impossible, and that's going to require coordination."

Working together won't be difficult because that's nothing new for resource-strapped state AGs, who often coordinate on enforcement actions, Weiser said.

"We've done it in other areas, and we'll do it here," he said. ■

US FTC's Phillips touts regulation, not break-ups, as privacy solution

By Dave Perera

Published on April 12, 2022

A US Republican Federal Trade Commission member today said marketplace privacy violations are a negative cost of doing business, not a symptom of monopoly — meaning their solution isn't more antitrust enforcement but regulation.

Agency Chair Lina Khan and others have suggested that dominant tech firms are responsible in large measure for Americans' loss of privacy.

"I think that is wrong, wrong, wrong," Commissioner Noah Phillips said today during the IAPP Global Privacy Summit in Washington, DC.

Rather, Phillips said, today's privacy landscape is a result of a market leading naturally to what economists call an "externality," a situation in which negative outcomes are borne by consumers rather than producers.

Stopping mergers won't necessarily boost privacy, Phillips said. That puts supporters of antitrust as a remedy to privacy violations in the paradoxical position of contending that a corrected marketplace will naturally gravitate toward privacy while also supporting increased regulation, he asserted.

"If you believe that the market is going to solve everything, you shouldn't support privacy law. You certainly shouldn't support privacy rulemaking," he told the Washington audience.

Many small companies perpetuate the worst privacy violations, Phillips added, citing makers of so-called stalkerware apps as an example.

Phillips also took issue with a trend in FTC enforcement to have privacy violators delete algorithms created with data obtained without consumer consent. "What constitutes the algorithm, what constitutes the ill-gotten gain can be hard to spot," he said. ■

EU-US data-flow deal paves the way for a UK version, US Commerce official says

By Sam Clark

Published on April 12, 2022

A data-flow pact between the UK and US has been facilitated by a similar deal between the US and EU, a US Commerce Department official said today.

Christopher Hoff, the department's lead negotiator on international data flows, said at the IAPP Global Privacy Summit today that the work done by EU and US negotiators to reach a transatlantic data-flow agreement should make it easier for the UK to get a similar deal.

"There's an opportunity for us to take the work we've done here and build something much quicker … The hard work has been [done]," Hoff said. The UK government, following the country's exit from the EU, has said it will make its own data adequacy agreements to allow data to flow seamlessly across borders.

The UK last year listed the US among six priority countries that it hopes to reach agreements with. A senior UK official said recently that he hopes these agreements will be finalized this year.

EU negotiators have secured commitments by the US to change its surveillance law, including by limiting the data it collects for security purposes and by creating a data protection court. So the EU's counterparts in the UK may have less work to do on securing an adequacy deal that the EU will also consider satisfactory. The UK has been granted its own adequacy decision by the EU.

The US Department of Commerce has been in conversation with the UK government, Hoff said today, as well as with Switzerland, which also had a Privacy Shield agreement before the European Court of Justice "Schrems II" decision in 2020. The US is "looking forward to making announcements" on this topic soon, Hoff said. ■

Data-transfer impact assessments should address US surveillance changes, Commerce official says

By Sam Clark

Published on April 12, 2022

Changes to US surveillance law should be the "first thing" company lawyers mention in their data transfer impact assessments, a senior US government official has said.

Christopher Hoff, the US Department of Commerce's lead negotiator on international data flows, said at the IAPP Global Privacy Summit today that proposed changes to US law announced by US President Joe Biden and European Commission President Ursula von der Leyen in late March are the "epitome of something that would matter in [a transfer risk] assessment."

The pair announced the changes as part of a political agreement on a replacement for the EU-US Privacy Shield, which the European Court of Justice struck down in 2020.

The changes have not yet come into law, but have been approved on a high-level political basis. The US has agreed, as part of the new framework, to create an "independent Data Protection Review Court" and to only collect data for intelligence purposes when it's necessary and proportionate.

Most companies transferring data from the EU to the US use standard contractual clauses — a model contract setting out how companies transferring and receiving data will protect it outside the EU. Once a new transatlantic data pact has been formally agreed, it's expected that many of these companies will shift to using this mechanism rather than the clauses.

But those companies that continue to use standard contractual clauses will also continue to be required to make data transfer impact assessments as part of the contractual processes.

Asked whether lawyers should mention the US surveillance law changes — once in force — in data transfer impact assessments, Hoff said "of course" they should be noted. "It should be perhaps the first thing that you mention in the transfer impact assessment," he said.

"That's the epitome of something that would matter in that assessment. That is such a seismic change to US law that it's something you should note … [the new] very meaningful binding form of redress … and safeguards around US intelligence activities," Hoff said.

The US Department of Commerce will release guidance on this subject, Hoff said. ■

New California privacy rules on employees creating compliance uncertainties, say company lawyers

By Claude Marx

Published on April 12, 2022

Companies are trying to figure out how to handle employee data as they wait for forthcoming regulations to implement new California privacy legislation.

"We are likely to have better training and include a human resources specialist on our data privacy team," Joy Chenault, the associate general counsel of CarMax, said at the IAPP Global Privacy Summit in Washington, DC. "It's not just a legal function but about adding value to your organization."

Stacey Keegan, the chief privacy officer and associate general counsel of Home Depot, said the uncertainty will make it harder for companies to plan how much they will have to spend on compliance costs.

She also said it will be harder to protect employee data than consumer data because employees' data is often spread throughout the company, while consumers usually have just one point of interaction.

The California Privacy Rights Act, which is set to take effect next January, requires companies to protect the data of employees, former employees, independent contractors and directors. It is the only state privacy law passed so far that covers those individuals. The California Privacy Protection Agency is supposed to issue regulations later this year.

The measure is an update of the California Consumer Privacy Act, which took effect in 2020. ■

EU national authorities 'stand ready' to help California set up privacy regulator, Jelinek says

By Matthew Newman & Mike Swift

Published on April 12, 2022

European data protection authorities "stand ready" to help California officials who are setting up a supervisory authority next year, a senior EU official said today.

Andrea Jelinek, chairwoman of the European Data Protection Board — the umbrella group of EU data protection authorities — said at the IAPP Global Privacy Summit today that "we stand ready to support them with our experience as national supervisory authorities in Europe."

"As national supervisory authorities, we can support them," said Jelinek, who is also director of the Austrian Data Protection Authority. "Some of us are small, like the Austrians, but we stand ready."

The California Privacy Protection Agency, created when California voters approved the California Privacy Rights Act (CPRA) in 2020, is the first single-purpose US privacy regulator. The CPPA is charged to not only enforce the CPRA that takes effect in 2023, but to specifically work with privacy regulators elsewhere in the US and other countries on privacy enforcement. »»

The California regulator is already drawing on the experience of European regulators as it develops specific enforcement guidelines for the new privacy law. At a recent hearing, the CPPA took testimony from Gwendal Le Grand, who heads enforcement support for the EDPB, on the EDPB's open-source data privacy assessment software that he said the California regulator could adapt if they wanted to perform similar data assessments.

The requirements of California's new privacy law should be enough for California to be deemed adequate for international data transfers under Europe's General Data Protection Regulation, the CPRA's primary sponsor, Alastair Mactaggart, told MLex in 2020.

Jelinek testified at the US Senate Commerce, Science, and Transportation Committee in October 2018 on the GDPR and the CCPA. When she was asked during the hearing about how the US should shape its privacy laws, she said it's up to US legislators to decide.

"I have the feeling there was a window of opportunity to make a federal law and this opportunity closed. Now I have the impression that again there is a window of opportunity exactly four years later regarding a federal privacy law. I think both sides of the House are speaking with each other very thoroughly."

"I have the feeling there was a window of opportunity to make a federal law and this opportunity closed," she said. "Now I have the impression that again there is a window of opportunity exactly four years later regarding a federal privacy law," she said. "I think both sides of the House are speaking with each other very thoroughly about maybe a privacy law."

She said US companies are concerned about a "fragmentation" of privacy law with four US states having data protection rules. She discussed the issue with Apple chief executive Tim Cook today.

"They are reaching out for federal law. They really want it," she said. ■

European privacy law a poor fit for Latin America, Mexican data-protection official says

By Dave Perera

Published on April 12, 2022

Mexico and other Latin American countries shouldn't be pressured into adopting European privacy law, said an official with the Mexican National Institute of Transparency, Access to Information and Personal Data Protection.

"Our socio-cultural reality is different" than in Europe, where the right to personal data privacy has been recognized for half a century, said Jonathan Mendoza Iserte, secretary for personal data protection at the institute. Better known by its acronym INAI, it is an autonomous government agency charged with overseeing public access to information and personal data protection.

Latin American countries, including Mexico, still find themselves at the stage of consolidating a culture of privacy, Mendoza said on the sidelines of the IAPP Global Privacy Summit today.

Mexico's federal data-protection law covering the private sector dates from 2010 and needs updating since its rules haven't kept pace with technology, Mendoza also said. More than two dozen privacy proposals have been floated in the Mexican congress but none are comprehensive and none are a priority.

The ideal outcome on a global scale, Mendoza said, would be for a convergence of privacy norms that takes into account the different socio-cultural realities of different regions. "That's the big goal, arriving at an international standard," he said. ■

UK government seeks to 'debunk' myth that data localization is justified, official says

The UK government opposes measures that would oblige companies to store data in particular jurisdictions and seeks to convince governments that "data localization" isn't a good approach, a senior UK official said today.

Joe Jones, the deputy director for international data transfers at the Department for Digital, Culture, Media and Sport, told a conference* today that the UK government is "de facto anti data localization."

Jones said that the UK pursues data flow arrangements through bilateral trade agreements as well as multilateral discussions at the Organization for Economic Cooperation and Development, the Group of Seven and the World Trade Organization.

Following Brexit, the UK government expects to reach "adequacy decisions" with countries including Australia, South Korea, Singapore, the US, Colombia and the Dubai International Finance Center — a special economic zone in the UAE.

"Whether through the trade agreements, we sign up to commitments that are opposed to localization … We engage with our partners to discourage them," Jones said.

The UK seeks to "debunk" the myth that data localization is justified for security or law enforcement reasons, he said. "It's not the most secure place, to keep it entirely within territory," he said. "It's not the way you are going to realize the opportunities of responsible data use.

He said that the Covid pandemic has been a paradigm shift in how citizens use data and perceive the value of it.

"It behooves us policy makers, regulators and industry to expose some of the myths about the localization and to tackle them through our bilateral and multilateral arrangements, and among like-minded [countries] to agree on best practices," he said.

Jones said work at the OECD is helpful to convince more countries of the merits of free flow of data.

He said that the UK government, which is considering its approach to making changes to its data protection rules, needs to be "humble" and not assume it has the answers to data protection questions.

"Our experience of revisiting the GDPR and what can be improved, we've learned we've borrowed and copied from all over the world, from Canada and Singapore," he said. ■

By Matthew Newman

Published on April 12, 2022

Data storage, processing on blockchain conflicts with minimization requirement of privacy laws, lawyers say

By Khushita Vasant

Published on April 12, 2022

Storage and processing of personal data on blockchain conflicts with the data-minimization requirement of data privacy rules in Europe and the US, and a solution could be to store data off the chain, privacy practitioners said today.

On a blockchain, data is stored in a decentralized manner, and when it isn't stored in one central place but many times over, this conflicts with the data minimization principle enshrined in the EU's General Data Protection Regulation, Michaela Nebel, partner at Baker McKenzie, said at the IAPP Global Privacy Summit.

A blockchain is a digital ledger of transactions that is duplicated and distributed across a network of computer systems on the blockchain.

Data minimization is the requirement that personal information is "adequate, relevant, and limited to what is necessary in relation to the purposes" for which it is processed, according to the website of the European Data Protection Supervisor.

"Another example of a conflict is that once the transaction has been executed, there is actually no further need to process personal data, but in a blockchain the data will, of course, be stored permanently and it's probably difficult then to say that the purpose does not only include only this one transaction but also the subsequent storage," Nebel said.

"So, there's a conflict with this principle, so one solution may be to store the personal data off chain in a separate database," she said.

This can help meet the minimization principle "because otherwise this multiplication of the ledger would result in probably difficult to defend amount of copy," said Lothar Determann, partner at Baker McKenzie. Even the public key that's stored once or twice, maybe in connection with the centralized ledger, is stored on the blockchain potentially thousands of times, he said. A public key is a cryptographic code that's paired to a private key and allows one to receive cryptocurrency transactions.

The two privacy practitioners were speaking on a panel about compliance challenges and solutions in dealing with privacy on the blockchain, and how organizations and individuals are subject to privacy and data protection law requirements in connection with block chains, non-fungible tokens, crypto currencies and Web 3.0 generally. ■

Transparency needed for algorithms that recommend products, services, say Meta and Nike executives

The host of privacy issues around algorithms that recommend products and services to consumers can be best solved with transparency, executives with Meta and Nike said today.

It may sound like a simple solution, but companies are failing, they said at the IAPP Global Privacy Summit.

"Explaining is not that complicated, and somehow we fumble it," said Pedro Pavlon, global policy director for Facebook parent company Meta, overseeing the monetization team. "We still tend to get it wrong."

Companies have to make clear why people are getting certain recommendations, including what data they're collecting to make them, and give them control to turn them off if they want, they said.

"Direct feedback is the clearest way," said Madeline Zamoyski, chief privacy counsel for Nike.

Adding to the pressure on companies is a new requirement in California that companies must disclose what inferences they make about consumers when they exercise their rights under the California Consumer Privacy Act, she said.

The privacy issues around recommenders are the same as with any machine-learning technology, said Jessica Rich, former director of the US Federal Trade Commission's Bureau of Consumer Protection. Are companies delivering harmful, addictive content to children? Are they making misleading or false claims about products or services? Are they discriminating against any groups or individuals?

Companies have to test their systems for bias, and measure their impact, Rich said. "Consider human oversight to check the inputs and outputs. If it's a black box you can't figure out, don't use it."

Companies have to come up with better ways to measure the output and impact of recommenders to make sure they are not creating negative side effects while trying to drive engagement, Pavlon said.

"The tricky part is when there's friction, there's heat, and there's damage, and it's not always possible to predict the harm you are going to create," he said.

There's nothing inherently wrong with monetizing data, and companies have been doing it "forever," Pavlon said.

But Zamoyski disagreed, saying that data isn't always collected to be monetized. It's also used to create meaningful experiences for consumers, she said.

"I think there are plenty of data strategies that do not involve selling data," she said. ■

By Amy Miller

Published on April 13, 2022

UK, Ireland set to ramp up children's data enforcement

UK and Irish data protection authorities are set to ramp up their enforcement on children's data protection, officials from both have said.

Jacob Ohrvik-Stott, head of regulatory futures at the UK Information Commissioner's Office, and Dale Sunderland, deputy commissioner at the Irish Data Protection Commission, said at the IAPP Global Privacy Summit today that they will begin enforcing codes on the processing of children's data that they recently released.

The ICO's Age Appropriate Design Code, or AADC, came into force in September last year and contains 15 principles, including on default settings, geolocation, parental controls and profiling. The Irish children's "fundamentals" guidelines took effect in December last year. It has less legal heft than the AADC but will be used as a guide by the regulator when enforcing.

The ICO sent letters to more than 40 companies, including Apple and Google, last November, asking for information about their compliance with the code.

Ohrvik-Stott said that while the ICO is "pleased" with some of the changes made by the larger tech platforms, such as stopping personalized ads for children, the regulator plans to move from the information-gathering stage to formal investigations soon. He did not identify the organizations against which the ICO will step up its enforcement.

Sunderland said the Irish regulator is looking at "supervision and enforcement measures" that it may start taking this year. The aim of these measures is to encourage organizations to "embed" the authority's recommendations in their data protection compliance considerations, he said.

The Irish authority also sent a draft enforcement decision against Instagram over its processing of children's data to EU data protection authorities in December last year. It did not say what decision it has reached.

Helen Dixon, the head of the regulator, told MLex in February that the other regulators have raised objections to the decision and that these concerns are unlikely to be resolved, meaning the case will likely go to the General Data Protection Regulation's dispute resolution mechanism. ■

By Sam Clark

Published on April 12, 2022

New UK ICO chief clarifies enforcement approach, says children are priority

By Sam Clark

Published on April 13, 2022

The new head of the UK's data protection authority has provided more details on how his risk-based approach to enforcement will work in practice.

John Edwards, who took over as head of the UK Information Commissioner's Office, or ICO, in January, has said several times since he started that he plans to allocate resources "judiciously" and in a way that targets issues that could carry the most risk. He reiterated his intention to take that approach at the IAPP Global Privacy Summit today, and said his office will use a "matrix" to make these decisions. The regulator will take input data, such as complaints or media reports, and analyze it to decide the level of potential risk.

Considerations in this analysis include how many people are affected and how moderate or severe the harm is, Edwards said. He said he doesn't believe in privacy "absolutism" and argued that most people would agree that every breach of data-protection legal obligations isn't the same.

Once this decision has been made, he said, the ICO must make an "appropriate regulatory response."

Enforcement and fines are "not the only tool in the toolbox," he said. Fines can be used, but the best way to achieve compliance is to make it easy to comply, he said. Any fines he does issue "should not come as a surprise to anyone," he said, arguing that predictability is important.

Edwards said he also will take this fundamental rights-based approach to his analysis of the UK's proposed reform of its data-protection laws.

"We need to focus on what is important for ensuring that fundamental rights are not reduced," he said. If existing provisions are not "making a material contribution to rights," and they add compliance burden, it is a "good thing" to remove them, he said.

The processing of children's data is a top priority for the ICO, Edwards said. The Age Appropriate Design Code became legally enforceable from September last year, and an ICO official said yesterday that enforcement will soon ramp up in that area. ■

Japanese official says more policy coordination among governments needed on privacy, global data framework

No single global data-governance framework exists, and governments around the world have never been more in need of policy coordination in bridging this gap, a Japanese government official said today.

Japan's government is working closely with its partners in the private and public sector to develop a global data framework, Koji Ouchi, counsellor at the Embassy of Japan at the US Ministry of Foreign Affairs, said during the IAPP Global Privacy Summit.

"We are facing an increasing amount of risks on privacy and security" that have led to concerns over cross border data transfer among governments, he said.

Ouchi spoke on a panel about OECD countries' efforts to develop trusted government access to private sector data.

The background to the discussion was the way EU member states realized that there were significant exceptions to national security practices when it came to data and privacy, which led to a desire among other member countries to probe what other governments were doing in terms of national security laws and practices. The EU's General Data Protection Regulation hasn't created any standards for national security, which has led OECD member countries to embark on a serious effort to remedy the gap.

"We have never needed more policy coordination in bridging those gaps among government," he said.

"We understand that legal framework of data protection or information security is heavily dependent on the political context and cultural profiles in respective countries, including OECD members," according to Ouchi.

Japan first proposed the prospect of common high-level principles and policy guidance on the subject at a Group of 20 summit in Osaka, he said. The government developed a few pillars that include data organization, regulatory cooperation among data protection authorities — including with European states — and prioritizing potential areas of data sharing. ■

By Khushita Vasant

Published on April 13, 2022

Experts in privacy, national security must engage in dialogue as global data framework emerges, US official says

By Khushita Vasant

Published on April 13, 2022

Experts in national security law and privacy law need to start a dialogue as governments around the world try to develop a global data and privacy framework where national security concerns play a role, a senior US government official said today.

Lauren Bernick, principal deputy chief of the Office of Civil Liberties, Privacy, and Transparency for the Office of the Director of National Intelligence, said a sophisticated conversation has been ongoing among privacy experts.

"It's a robust conversation. There have been debates, and it's been recently [the case] that the national security part has come into that conversation. Yet we haven't seen the national security experts [get] into that conversation as well," she said at a conference.*

Bernick was speaking on a panel about the OECD countries' efforts to develop trusted government access to private sector data. She said there has been an effort focused on identifying common practices among OECD members.

"We want to identify those shared principles, but we need the national security experts in the room. We need the law enforcement experts in the room," she said.

But it has also been a "challenge to get national security experts there because how do you talk about national security [and] authorities' constraints in an open setting, in an unclassified setting?" she said.

Conversations on a global data privacy framework need to be had "multi-nationally, globally," Bernick said.

The OECD has 37 members which "leaves a whole lot of the rest of the world. So how do we start taking this conversation and identifying the safeguards that like-minded democracies have?" she said. The focus right now is just getting different sets of experts talking to each other, Bernick said. ■

Brazil needs to follow its own path to develop new data protection law, experts say

By Mike Swift & Ana Paula Candil

Published on April 13, 2022

In the less than two years since Brazil's national privacy law came into force, its national data protection authority is focusing on education — of consumers as well as for judges and prosecutors — and is making progress across the massive country, a group of experts said at a global privacy conference today.

In the less than two years since Brazil's national privacy law came into force, its data protection authority is focusing on education — of consumers as well as for judges and prosecutors — and is making progress across the massive country, a group of experts said at the IAPP Global Privacy Summit today.

The conference panel was kind of a milestone, in that it was the first session on Brazil's LGPD in the history of the IAPP conference. It was attended by Miriam Wimmer, director of the ANPD — the Autoridade Nacional de Proteção de Dados — the Brazilian national privacy regulator. Although she didn't speak on the panel, Wimmer told MLex on the sidelines that she agreed with the views she heard.

While there are still many substantial enforcement and operational questions for companies and the ANDP to resolve, including working on a legislative proposal to turn the agency into an independent body, speakers said it was important to be patient with the development of the law and the regulator, rather than Brazil measuring itself to Europe's more advanced state of privacy law.

"We always look to Europe to see what's happening there, since the [LGPD] was inspired by the GDPR. But the Brazilian reality has a lot of differences from the European reality, in terms of awareness, in terms of the maturity of the market," said Gabriela Garcia de Paiva Morette, Johnson & Johnson's director of privacy for Latin America. "So, I don't know if 'proud' is the best word, but I really admire the work that has been done by the Brazilian authorities so far. They have such a short staff and they have done so much in such a short time."

ANPD's establishment was delayed in Brazil. The General Law for Data Protection, or LGPD, ended up taking effect in August 2020, three months before the agency was established.

"We always look to Europe to see what's happening there, since the [LGPD] was inspired by the GDPR. But the Brazilian reality has a lot of differences from the European reality, in terms of awareness, in terms of the maturity of the market."

"Brazil is a huge country, 230 million people from north to south — so many different contexts, so many different cultures. And privacy is a new topic, and such a technical topic," said Philippe Sundfeld, the data protection officer for Wildlife Studios, a video game developer. "So how do you reach those folks?" That doesn't mean, he said, that his company and others aren't anxious to get more specific legal guidance from the ANPD on enforcement questions. He said one pressing question for Wildlife Studios was whether the age of consent under the LGPD should be 13 or 16.

Brazil also needs to decide which enforcement model it will follow for children's privacy, he said.

Two choices would be to follow the model of the United States' Children's Online Privacy Protection Act, which focuses on companies obtaining parental consent before collecting and using children's data; or the UK's "Children's Code," which directs companies to consider the best interests of children in offering digital services. The code contains 15 principles, including on default settings, geolocation, parental controls and profiling.

"It would be brilliant" to have that sort of guidance from the ANPD, Sundfeld said, although he and others acknowledged that type of specific guidance will likely have to wait.

"I think we're at a very early stage in development of the law and in the awareness of it," Morette said. ■

White House official says administration won't reignite crypto wars

By Dave Perera

Published on April 12, 2022

Encryption ought to be viewed as a means to an end rather than an intrinsic good, a top White House cybersecurity official said today.

Governments across the world typically have, at best, an ambivalent attitude toward end-to-end encryption, since it makes it considerably harder for authorities to intercept digital communications. In the US, various presidential administrations have pressured the private sector to include flaws in encryption schemes to enable backdoor access by authorities.

Unlike its predecessor, the Biden administration has not rekindled the so-called crypto wars. "That is not something the US is actively considering," Chris Inglis, the national cyber director, told the IAPP Global Privacy Summit when asked about US policy on backdoors.

Private sector providers of operating systems have root access to devices but have said they're unwilling to turn over their privileged access to the government. "I don't know anyone in government who wants to challenge that," said Inglis, a former deputy director of the National Security Agency.

Inglis nonetheless appeared unwilling to give a full-throated endorsement of encryption, calling the phrase "backdoor" access to encryption a potential "pejorative." He told the Washington audience that encryption should be viewed as "a means to a larger end, as opposed to an objective in of itself."

Computer systems ought to be designed with objectives such as privacy or collective security in mind, he said, making encryption an attribute rather than a goal, Inglis said. ■

Data transfers are increasingly a material risk for international investors in M&A transactions, investment firm exec says

International data transfers are a material risk subject for investors looking to invest in US companies, and privacy professionals ought to flag related concerns at the outset of any transaction they are involved in, an executive at a multinational technology investment firm said today.

"More recently, in particular with US transactions, I would say that the international data transfer issue has become quite material for digital and Internet companies," Justin B. Weiss, global head of data privacy at Naspers & Prosus, said at the IAPP Global Privacy Summit.

This is particularly the case with investors outside of the United States looking to invest in US-based companies that have expansion plans or are multinational, he said.

Weiss was speaking about "risks and materiality" on a panel about privacy risks in mergers and acquisitions. He said the M&A and privacy worlds are growing closer and requiring more and more collaboration.

"Just because of the headlines and the regulatory focus on international data transfers and the gray areas associated, it's something that's very useful to elevate to the attention of the deal team so that they are not surprised if there's a challenge in that area," Weiss said. "Even if you can't solve it for them, you've flagged it for the deal team."

Security and data breach readiness, as well as data subject rights and consents, are two areas that Weiss said he tends to focus on in every new transaction.

"And I'll tell you why those two buckets. I call them Day One risks. So, if you buy a company that doesn't have a plan in place to call the regulator within 72 hours if something happens, and doesn't quite know how they're going to deal with a data emergency on Day One, you have a pretty significant risk," Weiss said.

A regulator will immediately expect to be notified, and failure by a company to do so is indicative of broader issues that are likely to lead to a broader investigation, he said.

"So, I see a data breach as a kind of a gateway incident, so the better security controls, the better incident response planning they have on Day One post-transaction, the more comfortable I am with that category of risks," Weiss said.

The other area of focus is data subjects' rights, Weiss said. A "data subject" is any individual whose personal data is collected, held or processed by a company and who has the right to request and receive confirmation of whether a company holds their personal data.

Weiss said data subjects are the ones who complain to the regulator if, for instance, a company is going to take a year to put automation in place to comply with data protection regulations. ■

By Khushita Vasant

Published on April 12, 2022

Privacy lawyers need 'actionable' intervention when voicing concerns that disrupt M&A deals, tech exec says

Privacy executives and lawyers need skills — and confidence — in raising concerns that may affect the valuation of a merger or acquisition because the deal team would likely view their intervention as disruptive, an executive at a multinational technology investment firm said.

"There's a huge desire — it's like a giant rock rolling down the hill — that [the deal team] wants to do the deal," said Justin B. Weiss, global head of data privacy at Naspers & Prosus. Privacy lawyers are faced with a bias toward participating in the deal and not blocking the deal, he told the IAPP Global Privacy Summit.

"So, anybody who steps forward and says, 'I've come up with a reason not to do this deal' or has come up with a concern or an issue that may affect the price or the valuation or whatever cost us to integrate that company is a very disruptive intervention," Weiss said.

By Khushita Vasant

Published on April 12, 2022

He was speaking about "risks and materiality" on a panel about privacy risks in mergers and acquisitions.

When making such an intervention, which privacy lawyers may have to do with increasing frequency, one needs to be "very confident," he said. "You need to be able to back up what you say. It's not an FYI. It needs to be actionable," according to Weiss.

Privacy lawyers will often be asked whether a specific concern or privacy requirement is "material or not," Weiss said. He recommended embracing the word and trying to get comfortable with it.

SKILL SETS

The European General Data Protection Regulation was an "accelerator" for making privacy a big part of the M&A process.

As data is increasingly seen as a pure asset, or acquisitions for the purpose of getting data, or antitrust reviews for data, deal teams are going to want a privacy lawyer to help them with processes that didn't used to involve questions about privacy. Weiss said that in the US, a review by the Committee on Foreign Investment in the United States (CFIUS) historically didn't have a very active privacy lawyer on the team, but that has changed now.

While some privacy officers have been very effective in the M&A context, others haven't, Weiss said.

"The deal teams are so occupied with speed, efficiency, brevity and the sort of tightness of intervention in the communications that if your topic isn't immediately obvious that it is material, it can be tough to get a seat at the table or be very relevant in the transaction," he said.

According to Weiss, "privacy folks have to earn their stripes with the M&A team" and show that they can "run with the pack and not be perceived as obstructionists."

A skillset where a privacy lawyer identifies, for instance, several issues but picks only a handful to talk about requires a "certain maturity and experience" that not everyone has, Weiss said.

"More and more privacy people are starting to get involved and are gaining experience in this space and I think that will continue," he said. ■

Privacy risks are causing companies to walk away from M&A transactions and divest risky assets

By Khushita Vasant

Published on April 12, 2022

Privacy-related concerns are increasingly making companies walk away from acquisitions because of the risks associated with purchasing a new asset, practitioners said today.

"I've seen a couple of things happen. Organizations not wanting to have assets, which carries significant risks because it's non-core to their business ... and divesting those [acquisitions] because they are not comfortable with the privacy risks associated with that entity," Mark Thompson, research director at the International Association of Privacy Professionals, or IAPP, said at the IAPP Global Privacy Summit.

He was responding to a question about the prevalence of companies choosing tactical divestments — as opposed to the purchase of an asset — because of privacy concerns. He spoke at a panel on privacy risks in mergers and acquisitions.

Another phenomenon Thompson said he has witnessed —a flipside — is companies' choosing not to acquire an asset because of privacy risks.

"When I talk about not acquiring, it's not because of the privacy issues in the entity, but actually taking the risk they've currently got and bolting on this other entity, they deem that to be too great of a collective risk," he said.

"So, it's not a divestment, but they've chosen not to make a decision [about a new acquisition] because the collective entity would have carried too much of a privacy risk for their risk tolerance levels," Thompson said. ■

Privacy-enhancing technologies will take time and experimentation, experts say

New advances in privacy enhancing technologies could help ease the friction between the digital ads ecosystem and consumers who don't want to be tracked across the Internet, regulators and online advertising experts said today.

But it's going to take time and experimentation to get there, they told the IAPP Global Privacy Summit.

Marketing to potential customers will never disappear, said Yeong Zee Kin, deputy commissioner with the Personal Data Protection Commission of Singapore. The task now is to find a better way to advertise online that doesn't "creep out" consumers by tracking them everywhere they go on the internet, and that also serves the needs of advertisers and publishers, he said.

"Now is the best time for us to get all the right people in the room together, including policymakers and technologists," Kin said. "Let's focus on this question: How do we make it better?"

The World Wide Web Consortium, or WC3, is looking at several new technologies that can be built onto the basic technologies already underpinning the internet, lead counsel Wendy Seltzer said.

One example is federated learning, a technique that trains algorithms across multiple decentralized devices or servers that hold local data. Another is secure multiparty computation, a cryptographic tool that safeguards confidential data when it is shared from multiple parties.

Figuring out what approach works best will require lots of testing and analysis, she said.

"We need solutions that work for all the participants in the ecosystem," Seltzer said.

But these potential changes shouldn't be implemented in a way that will destroy the online ecosystem, said Lartease Tiffith, executive vice president for public policy at the Interactive Advertising Bureau (IAB). Personalized advertising works because it gives consumers what they want to see, he said, and the online advertising industry is collaborating to solve these privacy issues.

"I definitely think it's possible, and I'm optimistic," Tiffith said. ■

By Amy Miller

Published on April 12, 2022

Clearview AI and adtech ecosystem are focus of growing global data protection cooperation

By Mike Swift

Published on April 12, 2022

Facial recognition firm Clearview AI and the ad-tech ecosystem are two key areas of focus for a 29-nation group of international privacy enforcers that has substantially grown in membership and activity during the pandemic

The International Enforcement Cooperation Working Group, or IEWG, currently led by data protection officials from Norway, Hong Kong, Colombia and Canada, is part of the Global Privacy Assembly — an association of the world's privacy regulators.

Two members of the working group said at a global privacy event today in Washington that the IEWG has provided significant assistance to global privacy regulators, helping them pool resources to learn about emerging technologies, to discuss how best to cooperate on privacy investigations, to learn how to prioritize the most important probes to pursue, and to assign responsibilities for investigations.

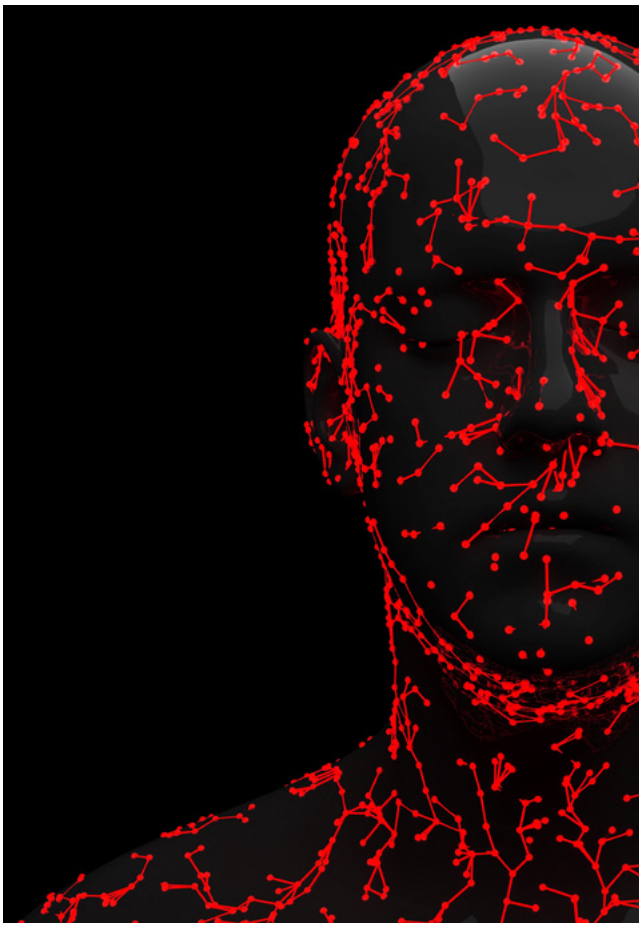
In the early days of the global pandemic, the IEWG wrote to four companies with global video chat platforms — Microsoft, Cisco Systems, Google and Zoom Video Communications — to insist on standards for privacy and security for video chat. The companies responded rapidly and positively, demonstrating the efficacy of the IEWG approach, said Brent Homan, a deputy commissioner in the Office of the Privacy Commissioner of Canada,.

"By joining forces to adopt and communicate positions on issues that have a significant impact on privacy, we're not only able to expand our collective enforcement capacity and influence, but we're able to effect an expedient and positive global privacy impact," Homan said. "What was key was that there was authentic and unguarded dialogue between the regulators and the organization."

The IEWG has also helped to coordinate the multinational joint investigation of Clearview AI, the US company that has scraped billions of facial images from online platforms to create a global facial recognition database.

In Canada, the UK, France, Italy and other countries, regulators have found a significant benefit in using the IEWG as "a gateway to international enforcement cooperation" to confront Clearview, said a representative of the UK's Information Commissioner Office.

"Working within the working group has helped achieve a pretty convergent outcome [on Clearview] if »»



The International Enforcement Cooperation Working Group has helped to coordinate the multinational joint investigation of Clearview AI, the US company that has scraped billions of facial images from online platforms to create a global facial recognition database.

you're looking across the globe," said Claudia Berg, the general counsel of the ICO. National authorities agreed that they each had legal jurisdiction when Clearview scraped the facial images of their citizens, and in the substance of investigations, she said.

Australia and Canada have forced the company to shutter its local operations; Italy and the UK have imposed final or provisional fines.

"International cooperation has never been more important than now, because we all live our lives increasingly online, and our personal data in principle flows freely across international borders," Berg said. "So, when we've got an international global issue, we need a global international response to that issue."

The fact that different countries have different privacy laws has, perhaps surprisingly, not been an impediment as much as an opportunity, Canada's Homan said, allowing countries to tailor their approach given the legal tools they have.

Quoting John Edwards, the new chief of the ICO, Homan said the IEWG has proven to be "one of those situations where something that appears impossible in theory works very well in practice." That, he added, "has been a bit of an 'a-ha' moment."

Because it became a permanent body in 2019 on the eve of the Coronavirus pandemic, the IEWG has yet to meet in person, holding its non-public sessions over video chat programs.

Meanwhile, another international working group within the Global Privacy Assembly, the Digital Citizen and Consumer Working Group, for the last four years has been analyzing the growing connections and tensions between privacy and antitrust enforcement.

With adtech, the IEWG is functioning as a kind of information clearinghouse, helping both privacy and antitrust regulators to better understand technological complexity of digital advertising platforms of companies such as Google and Meta Platforms, the Canadian and UK regulators said today.

"The objectives are really to share information and to understand properly the ad-tech ecosystem," Berg said. "The aim is … to work toward a much more consistent and effective regulatory approach in this area across borders." ■

Companies deploying AI must consider accountability, transparency in deploying algorithms, experts say

With regulators from Brussels to Washington to California poised to issue artificial intelligence enforcement rules, companies that use AI must focus on developing procedures to ensure the fairness, transparency and accountability of their algorithms, experts said today.

Speaking at the IAPP Global Privacy Summit, lawyers for Google, Autodesk and in private practice said rules proposed by the European Commission, the US Federal Trade Commission and the California Privacy Protection Agency could trigger fines or injunctive regulatory action. Senior FTC officials have recently said, for example, the agency will continue to seek "forward-leaning" business changes such as requiring companies to destroy algorithms based on flawed or discriminatory data.

Unless companies can show they've built in robust, thoughtful procedures to ensure algorithms aren't driving discriminatory outcomes, and they continue to check that those AI systems are behaving as they should, companies run the risk of significant regulatory problems.

By Mike Swift

Published on April 13, 2022

"It's important to get this right on the front end," said Bret Cohen, a partner in the privacy and cybersecurity group at the firm Hogan Lovells. And for companies that don't, "there are penalties where you might have to give up the end results."

Companies can't just rely on lawyers to vet the fairness of algorithms; they need to develop cross-functional teams that also include policy specialists and people with a focus on ethics, said Britanie Hall, a product counsel for Google who works on its Google Assistant and speech recognition product. Companies, Hall said, need to be willing to have "difficult conversations" before deploying AI products.

"'Why are we doing this?' — I can't tell you how often people forget to ask this question," Hall said. "Does [the use of an AI algorithm] really give us something we can't get some other way?" With an AI product, she said, companies should also consider the question: "What's the absolute worst thing you can imagine happening" if things go wrong with the algorithm?

Based on the crowd of well over 600 people who crammed into the standing-room-only session, the regulatory risk of deploying AI is a common problem for many companies. Hall, Cohen, Rob van Eijk of the Future of Privacy Forum, and Alexandra Ross, the senior data protection, use and ethics counsel for Autodesk, urged companies to consider a range of issues in building AI products, but particularly accountability for how an algorithm works, fairness in regard to how it might discriminate against groups, and transparency for the workings of the algorithm.

Companies need to be able to say, when confronted by a regulator, "we understood the implications when we started this process," Cohen said.

"I think accountability means determining that the algorithm continues doing what you think it's doing," Hall said. But companies need to have a system to set up "smoke signals" that indicate the algorithm isn't behaving the way it's supposed to. "What is your mitigation plan when that happens? These are really important things to think about," she said.

Ross said companies should never think of algorithms as a finished, static thing: "You want it to be flexible; you want it to be accurate and forward-looking, and you might want to iterate on it." Disclosure rules with AI are also likely to evolve: "I think this is going to develop over time, just like a lot of the transparency over privacy has developed over time," Ross said. ■

Targeted-ads industry faces unprecedented regulatory scrutiny and uncertainty, experts say

The combination of privacy technology changes to platforms such as Apple's iOS and Google's Chrome, coupled with a proliferation of regulatory changes from China and South Korea to Brazil the EU and the US, has left the global targeted-advertising business in a place of unprecedented uncertainty.

"I think it's fair to say that tracking and targeting have never been under so much scrutiny in so many places and has never been subject to as much uncertainty as it is right now," Reed Hastings, a partner at the firm Venable, said at the IAPP Global Privacy Summit.

In the US, comments just last night at the same conference by Lina Khan, chair of the US Federal Trade Commission, suggest the traditional "notice and choice" model is giving way to a regulatory framework where companies will have to follow a series of rules about what data they collect and how they can use it.

Khan said during a conference keynote address yesterday in Washington that there needs to be a reassessment in how regulators "assess unlawful conduct" in privacy, and that reassessment may "render notice and consent paradigm outdated."

Questions on whether consent is still an appropriate tool for people to control their personal data is also an issue in Europe, said Colin O'Malley, founder of Lucid Privacy Group, a privacy consulting group. "We are seeing this movement toward consent globally, but also questions about whether consent is broken, particularly as you look at how consent is modeled in Europe," he said.

A recent decision by the Belgian data protection watchdog is yet another source of uncertainty, O'Malley said. Last month, the APD found that IAB Europe acts as a joint controller for profiling and other data-processing done by companies using its Transparency and Consent Framework. The tool identifies and records web users' consent to data processing, an important compliance measure for the digital ad industry.

The Belgian authority fined IAB Europe 250,000 euros ($270,000), and gave the body two months to submit an "action plan" on changes to the TCF. A hearing on IAB Europe's appeal has been postponed until mid-May, MLex has learned.

There are significant regulatory changes in Asia, too, where China's new Personal Information Protection Law, while drawn in many respects from the GDPR, has unique elements such as a ban on price discrimination or any other unreasonable data-driven special treatment in automatic algorithmic systems, said Danda Zhao, head of the Asia-Pacific data protection laws section at Continental.

But experts said those regulatory changes don't have the impact of the uncertainty driven by changes such as Google's decision to phase out third-party cookies on its Chrome browser, and Apple's decision to allow users of its iOS devices to block third-party tracking in all apps on that platform. "The impacts are profound. We're looking at a migration from third-party cookies to first-party data" as companies seek to collect data directly from consumers instead of through third-party trackers, O'Malley said.

The changes in Chrome and iOS "are changing the marketplace more comprehensively than any of the legal regimes around the world, including GDPR," he said. ■

By Mike Swift

Published on April 12, 2022

US government will act quickly on cyber incident reporting mandate, official says

By Dave Perera

Published on April 13, 2022

The US government will fast-track a rulemaking process to implement a new statute requiring American companies to disclose cybersecurity incidents, an official said.

Congress in March approved a law mandating companies vital to the normal functioning of the country to report hacks and ransomware payments to the Department of Homeland Security.

Legislators left it up to the department to decide through a formal rulemaking process how broadly the reporting requirement should apply, since the official definition of critical US infrastructure encompasses broad swathes of the economy — in all, 16 separate sectors encompassing everything from transportation to information technology.

"I am trying to accelerate this as much as I can," said Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, while at the IAPP Global Privacy Summit today. Her agency, more commonly known as CISA, is the Homeland Security organization charged with receiving the private sector reports.

The rulemaking process will begin with a request for information, to be followed by listening sessions, she added.

The reporting requirement aside, CISA lacks regulatory authority — a fact Easterly portrayed as a feature rather than a bug. The agency is "here to help," she said, not "to shame, to blame, to kill anyone's reputation, to stab the wounded."

Private sector cyber incident reports will be protected from disclosure and from triggering liability.

Easterly nonetheless advised the conference audience to follow the "binding operational directives" the agency issues to federal agencies, which must follow the agency's mandates on cybersecurity measures. The directives "are not binding on critical infrastructure, but they're an incredible signaling mechanism" for matters requiring high-level attention by the marketplace, she said. ■

Palantir, Wejo say connected-car data can drive key transportation decisions while protecting privacy

Connected cars can be a rich source of data that helps governments make better investments in roads and vehicle infrastructure, while still preserving the privacy of drivers, representatives of Palantir and Wejo say.

Speaking today at the IAPP Global Privacy Summit, representatives of the two companies said they're already drawing data from nearly 12 million cars, including about 500,000 in the EU, which feeds databases that local governments can query for a long list of public safety or infrastructure decisions. By 2030, Wejo, a UK-based connected-vehicle-data startup, believes there will be 600 million connected vehicles on the road globally.

"That projection is significantly on the lower end because China has significantly advanced in relation to their connectivity, and in the US, we are seeing a significant advancement and progression in connected vehicle data," said Taiwo Idowu, privacy operations officer for Wejo. "And all of this data has provided insights: How is the car working? How is the road working? How is the weather and the road functioning for drivers? ... How can the data be used in an environment that can better society?"

One key application, the companies said, is developing the best evacuation routes in case a disaster requires authorities to move as many people over roads as quickly as possible. One conclusion: "The route that most people think is the best route to get out if there's an evacuation is actually the worst route," Idowu said.

A second application Wejo and Palantir are working on together is using data to determine the best location for electric vehicle charging stations. Data is particularly important because there is large disparity across the US in EV trips — California had 6.5 million EV journeys in April 2019, while New York had fewer than 400,000.

Good data is crucial in areas where there are fewer EV journeys. "This is part of the insight we're providing to different state localities," Idowu said.

Alice Yu, privacy and civil liberty commercial lead for Palantir, said Wejo takes steps to anonymize the car data it collects to ensure it can't be tied to an individual driver before the data is delivered to Palantir for application, such as location of charging stations.

"Prior to any of the Wejo data coming in the Palantir system, they have already done their own processing privacy techniques on top of the data, to really minimize the re-identification risk for that data," Yu said. "They are doing their own modeling to make sure that data is appropriately de-identified prior to coming into the model."

Wejo has different classifications based on the consent level for its collection and use by drivers, ranging from data that is deemed to be personal data to data classified as fully anonymous that can never be tied to an individual.

"If a data set is deemed to be de-identified, we have controls that are automatically embedded in the data set ... to make sure it meets our internal classification for de-identification and anonymization," Idowu said. ■

By Mike Swift

Published on April 13, 2022

Cloud providers drafting update to code of conduct for global data transfers under EU's GDPR

Cloud service providers are drafting an update to an EU-approved "code of conduct" to include international data transfers that would provide companies with an extra tool for transatlantic data flows as EU and US negotiators continue talks to finalize a successor to the Privacy Shield, industry representatives said today.

Adding data transfers to the code of conduct would be a "powerful tool that removes extra negotiations," Mark Webber, US managing partner at Fieldfisher, said at the IAPP Global Privacy Summit today.

Codes of conduct have been seen as a potentially useful alternative for European companies needing to transfer data. They are listed as potential transfer tools in the EU's General Data Protection Regulation, but are often overlooked as they need pre-approval.

Webber said even though companies may still have to do a transfer impact assessment — in which they assess the risk of government access to the data — a code of conduct for global transfers "really removes that friction."

Jörn Wittmann, managing director of SCOPE Europe, a Brussels-based monitoring body for codes of conduct, said during a panel discussion that talks on the draft update to the code will be held with European data protection authorities in the coming weeks.

In May 2021, privacy regulators approved the first EU-wide codes of conduct — the Cloud Code of Conduct and the Cloud Infrastructure Service Providers in Europe's (CISPE) code of conduct for cloud infrastructure providers — allowing cloud businesses to show compliance with EU data protection rules. The Belgian and French privacy regulators, respectively, acted as the lead data protection authorities for the codes.

In February, CISPE — an industry association representing cloud companies such as Amazon Web Services and Aruba — agreed on the code of conduct.

The code defines requirements for cloud service providers for data-processing activities under the EU's General Data Protection Regulation. It allows these providers to show GDPR compliance as processors and is overseen by an accredited monitoring body.

The move to update the EU code of conduct comes after a senior official at the UK's Information Commissioner's Office said that UK businesses could see codes of conduct recognized in the future as a legal underpinning for international data transfers.

The European Data Protection Board — the umbrella body of the EU's privacy authorities — is also working on guidance on certification for cloud service providers.

The impetus for another tool for global transfers follows a 2020 ruling by the EU Court of Justice that invalidated the EU-US Privacy Shield data-transfer agreement and at the same time backed the use in principle of "standard contractual clauses," or SCCs — sets of template contract clauses that comply with the EU's strict data-protection rules.

On March 25, EU and US leaders announced an agreement in principle on revamping the Privacy Shield, though a final agreement won't be adopted until the end of this year, EU justice chief Didier Reynders said yesterday. ■

By Matthew Newman

Published on April 13, 2022

mlex
a LexisNexis company

UK +44 800 999 3237
US +1 800 356 6547
EU +32 2 300 8250
HK +852 2965 1424
www.mlexmarketinsight.com
customerservices@mlex.com