
iapp25
25 leaders, 25 moments at 25 years

Contents

Introduction

In 2025, the IAPP celebrated its 25th anniversary. Over those two-and-a-half decades, privacy evolved from a niche compliance task handled by a small cadre of professionals into a core business function for organizations around the world. In many ways, the profession's origins trace back to the rise of the internet in the late 1990s and early 2000s. From there, it only grew in significance as technology evolved, and laws emerged globally.

With massive developments like the advent of smartphones, the invalidation of multiple trans-Atlantic data transfer agreements, the sweeping impact and influence of the EU General Data Protection Regulation, and the rapid proliferation of artificial intelligence, data professionals have had to constantly adapt to changes taking place almost daily.

To reflect on the dramatic rise of the privacy and digital responsibility profession — and the parallel growth of the IAPP — we highlighted 25 leaders and 25 moments from the last 25 years. Beginning in January and running through December 2025, we published a new LinkedIn post each Friday that looked back at notable leaders and moments during the IAPP's history.

While this collection is not exhaustive, it was curated to demonstrate the wide array of voices and developments across the field — from industry, advocacy, academia, government and journalism — and to capture key developments in privacy, AI governance and cybersecurity, as well as the IAPP's own evolution.

Each week's post alternated between leaders and moments, often aligning with the timing of when those milestones took place. Here, we bring them together in two sections within a single volume.

The project was a truly collaborative effort, involving contributions from many individuals — far too many to name here — within the IAPP and beyond. You know who you are, and we are grateful.

Jedidiah Bracy
IAPP Editorial Director


iapp25
LEADERS

Alan Westin

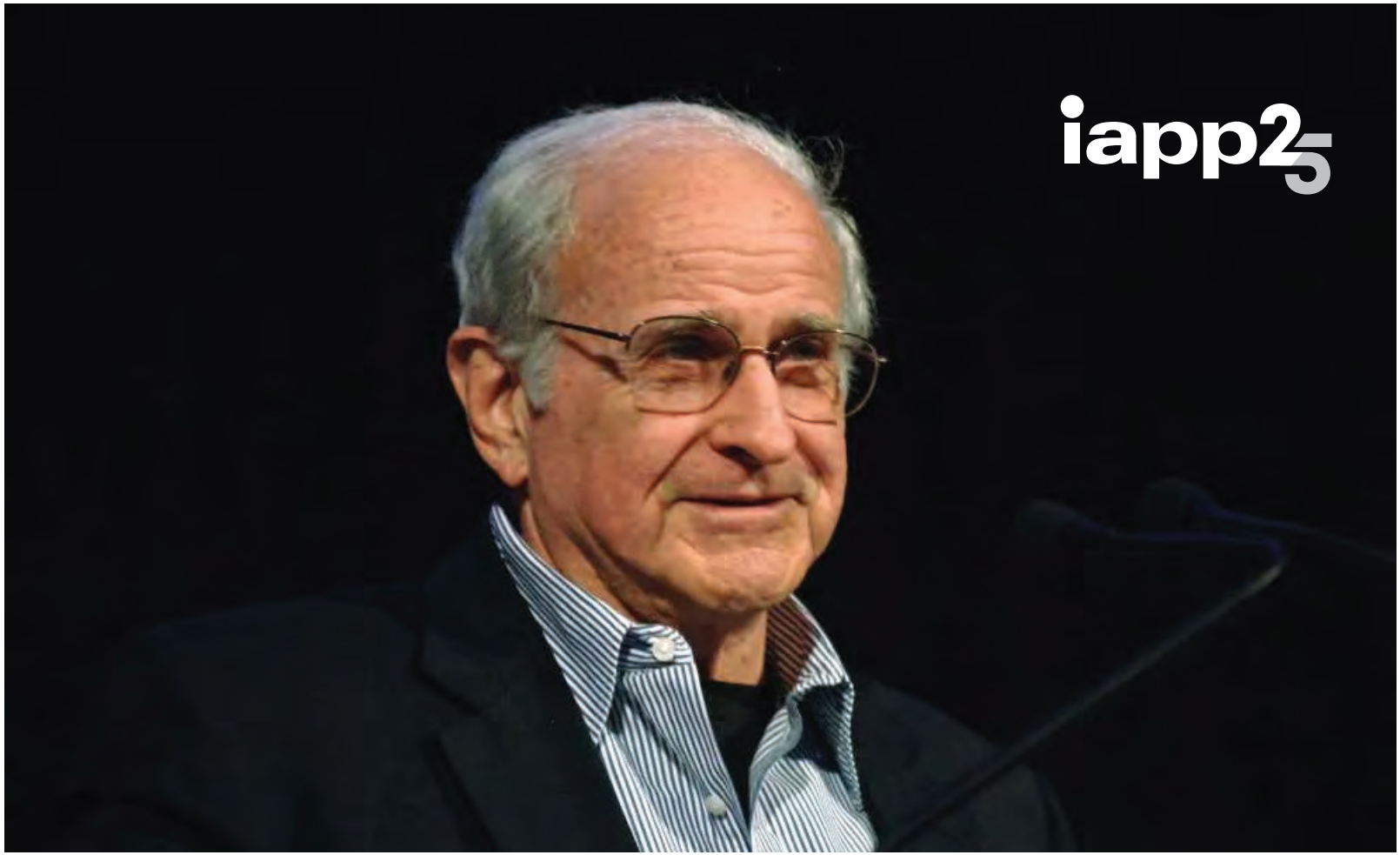
When considering some of the major figures who helped shape the privacy profession in the last 25 years, the first who leaps to mind is groundbreaking information privacy scholar Alan Westin. Though his early work came to fruition nearly 60 years ago with the publication of the foundational text "Privacy and Freedom," Westin's research, writing and influence continues well into the 21st century, leading to the creation of the Westin Research Center and the Westin Fellowship program at the IAPP.

"Today, literally tens of thousands of statutes, court decisions, regulations and company best practice standards, throughout the globe, are based upon" principles set forth by Westin, friend and Arnall Golden Gregory Privacy Partner Bob Belair said in an IAPP article shortly after Westin's death in 2013. "He was the first to understand the implications that computer technology, as well as other kinds of automated technology, had for personal privacy," Belair added.

As part of his legacy, the IAPP Westin Research Center was created in 2013 to encourage, enable and produce practical, applicable research and scholarship in privacy. And each year since then, the IAPP's Westin Fellowship program has brought forward recent graduates to help the IAPP work on a broad array of privacy and digital governance research projects to support the growth and development of the profession and further an understanding of major issues in the field. In the last decade, 21 Westin Fellows have worked with the IAPP to advance these initiatives before blossoming into their own influential careers.

In 2020, the IAPP also launched the annual Westin Scholar Awards to support students who are identified by their professors as future leaders in the field of privacy or data protection.

"Today, literally tens of thousands of statutes, court decisions, regulations and company best practice standards, throughout the globe, are based upon" principles set forth by Westin.



LEADERS

Agnes Bundy Scanlon

Looking back to its earliest days, the IAPP was not called the IAPP. It was originally named the International Association of Privacy Officers until 2002, when officers was replaced with professionals.

Agnes Bundy Scanlan, CIPP/US, fully supported the decision to change the association's name. "As privacy professionals, we have many roles and responsibilities," she said at the time. "Safeguarding privacy is a team effort."

In 2002, Bundy Scanlan was the managing director and chief compliance officer at FleetBoston Financial and founding chairman of the IAPP's Board of Directors. In 1999, she became one of the first bank chief privacy officers. Later, Bundy Scanlan would play other leading and executive roles at TD Bank and Bank of America before eventually serving as the Northeast Regional Director of Supervision Examinations for the U.S. Consumer Financial Protection Bureau. She continues to advise clients with financial services firms, fintechs and others as president of The Cambridge Group. Privacy continues to be a topic of discussion in which Bundy Scanlan is engaged in her corporate independent director work.

Her leadership in the early days of the IAPP has had a lasting impact. In 2004, Bundy Scanlan was awarded the IAPP's inaugural Privacy Vanguard Award, recognizing IAPP members who demonstrate exceptional leadership, knowledge and creativity in the profession.

Bundy Scanlan's influence on other aspiring professionals was also demonstrated in a 2011 IAPP article about the career path of FTI Consulting U.S. Practice Lead for Information Governance, Privacy and Security Michael Spadea, CIPP/US, who shared his experience charting his trajectory into the profession.

While attending law school, a professor informed Spadea about an unpaid internship at Fleet Financial, which eventually became Bank of America. It was there, he said, that he connected with Bundy Scanlan. She became his mentor and helped connect him with other professionals, leading him toward a successful career in the profession.

"Agnes is an exceptional leader in our field," IAPP President and CEO J. Trevor Hughes said recently while reflecting on her leadership. "She recognized early that the profession needed structure and support to thrive. Many of our members may not know her by name, but they should. For they have all benefitted from Anges' efforts to build our community."

In 2004, Bundy Scanlan was awarded the IAPP's inaugural Privacy Vanguard Award, recognizing IAPP members who demonstrate exceptional leadership, knowledge and creativity in the profession.

LEADERS

Jules Polonetsky

As the IAPP came into its own as a global professional organization, the role of the modern chief privacy officer was beginning to be defined at major multinational companies, according to President and CEO J. Trevor Hughes, CIPP.

Since then, the CPO position has become commonplace in thousands of multinational organizations. Hughes said, among key thought leaders in digital policy during the IAPP's existence, only a few are near-universally recognized on a first-name basis.

One such individual, Hughes said, is Jules.

In 2000, current Future of Privacy Forum CEO and IAPP Board of Directors founding member Jules Polonetsky, CIPP/US, was hired as one of the first CPOs when he joined the advertising technology firm DoubleClick before it was ultimately acquired by Google. He then went on to work as the vice president for consumer advocacy at AOL until 2008, when he left to join FPF.

Hughes called Polonetsky a "remarkable leader in our field," not only for his contributions to the IAPP but to the larger global privacy community at large as well. "Through complex and challenging policy debates that have consumed us for the past 20 years, he has been a steady and trusted voice," Hughes said.

From the jump at FPF, Polonetsky said he wanted to develop a space "for the senior leaders in privacy to collaborate, learn from each other and develop best practices."

"My goal at FPF was to provide a pragmatic, centrist viewpoint to privacy debates, optimistic about data use and supporting the utility of data by helping put responsible safeguards in place," Polonetsky said.

Since the early years of the IAPP, Polonetsky said he viewed the organization as a "big tent and platform that has provided a stage for the broad privacy community."

"The IAPP has helped create the professionalism of this field, defining the skill sets needed, training now a second generation of skilled experts to guide organizations operating in an increasingly complex environment," he said. "As the data world becomes rapidly more complex, the IAPP is leading the way in exploring the skills needed to manage the complexity."

When the IAPP was formed, Polonetsky was serving as a commissioner at the New York City Department of Consumer Affairs and was tasked with ensuring all consumer advertising and sales complied with consumer protection laws. Before his tenure as commissioner, Polonetsky served as an elected New York Assembly member from 1994-97, and worked for then-U.S. Reps. Steve Solarz, D-N.Y., and Chuck Schumer, D-N.Y., respectively, from 1990-92 and 1992-93.

Polonetsky said while working for the Congressmen and serving in state government, he witnessed the policy conversations surrounding technology go from "geeky insider conversations between technologists, advocates and lawyers," to front and center in virtually all public policy issues facing society.

"Today the stakes are global leadership, the future of democracy, the shape of our workforce, the future of healthcare, the economy, rules for Big Tech and small, human autonomy and more," he said. "Every major social issue is played out with tech and data as an intermediary."

Between his work at FPF and in the private sector, Polonetsky has assisted in drafting codes of conduct, data protection best practices and data privacy legislation around the globe.

In 2023, Polonetsky received the IAPP Leadership Award, which recognizes an "individual or organization who demonstrates an ongoing commitment to furthering privacy policy, promoting recognition of privacy issues and advancing the growth and visibility of the profession."

He said the recognition from his peers and the broader privacy community was a "tremendous honor, unlike any other."

LEADERS

Ann Cavoukian

Privacy by design is a ubiquitous term among privacy professionals and a foundational principle for privacy and data protection law. Ann Cavoukian, a leading privacy expert and strong voice in the privacy community, coined the term and promoted the concept within the privacy community and among policymakers.

In 1997, she was appointed as the Information and Privacy Commissioner of Ontario, Canada, where she served three terms. Prior to assuming office, she published the groundbreaking paper "Privacy by Design," which laid out a framework that places privacy at the forefront of design specifications and encourages the strongest possible protections for consumers.

Cavoukian's privacy-by-design concept has been recognized as an essential framework. In 2010, the International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution instating privacy by design as an international standard. In 2012, the U.S. Federal Trade Commission included privacy by design as one of three recommended practices to ensure online privacy. It was later codified in the EU General Data Protection Regulation and many subsequent national privacy and data protection laws.

In 2005, Cavoukian was awarded the Privacy Innovation Award by the IAPP for her and the IPC's work on developing short privacy notices. In 2007, Cavoukian was listed as one of Canada's most powerful women by the Women's Executive Network when she received the Top 100 Award in the Trailblazers and Trendsetters category. She also received the 2011 Kristian Beckman Award and the SC Canada Privacy Professional of the Year Award and was named one of the Top 11 Movers and Shakers by Intelligent Utility Magazine .

Cavoukian's privacy-by-design concept has been recognized as an essential framework. In 2010, the International Conference of Data Protection and Privacy Commissioners unanimously passed a resolution instating privacy by design as an international standard.

"Ann Cavoukian's pioneering work on privacy by design has, without question, reshaped how organizations should approach data protection," said IAPP Managing Director, Canada, Kris Klein CIPP/C, CIPM, FIP. "By embedding privacy into the very framework of system design, she set a global standard that prioritizes user trust and data security from the outset."

"As a regulator, Ann Cavoukian was all-in and full of energy," Klein said. "There was an incident where health records were sent for destruction but mistakenly ended up scattered on a Toronto street during a film shoot. She actually went to the scene of the breach and personally scooped up as many health records as possible. That kind of hands-on approach showed her commitment to protecting people's privacy."

Today, she is the executive director of the Global Privacy and Security by Design Centre, where she continues to advise companies and governments on innovative systems and privacy-enhancing technology to protect personal privacy and security. Her work remains highly influential, as privacy by design principles still guide the development of consumer-facing products.

LEADERS

John Edwards

When John Edwards stood before the U.K. House of Commons Digital, Culture, Media and Sport Committee in 2021, he was looking to inhabit an office facing tough questions about the U.K.'s privacy future.

Fresh off its split from the EU, the U.K. was asking how, or if, it should develop data protection policies separate from the EU General Data Protection Regulation. A seasoned privacy regulator at this point, Edwards sought to assure his potential hirers for the Information Commissioner's Office there was a path forward.

"The United Kingdom is entitled to take Fleetwood Mac's advice to go your own way," Edwards said, according to a transcript of the hearing. "There is plenty of scope within the European Commission's adequacy determinations for recognition of difference."

Edwards got the job and has been carving out the U.K.'s data privacy destiny ever since. A Kiwi barrister and solicitor by trade, he rose through the public service ranks until he was appointed New Zealand Privacy Commissioner in 2014. His tenure there included implementing the Privacy Act of 2020 and restructuring the agency's role in the regulatory system.

Privacy is very different from when he first started, Edwards said.

"It was a niche industry — a backwater — and now it is a really significant feature of the digital ecosystem," he said. "And the digital economy is an enormous part of the global economy, so privacy has a front row seat on the global stage now."

In his first public address as a commissioner during the IAPP Data Protection Intensive: UK 2022, he assured listeners any regulation developed would have legal protections just as strong as the EU's, even if they took a different shape. His mantra throughout his career has been that privacy should be easy for consumers to understand and agencies to implement. His career has also focused on reducing compliance costs for small and medium businesses.

His mantra throughout his career has been that privacy should be easy for consumers to understand and agencies to implement.

Edwards said he's taken steps toward those goals at the ICO, including making a staff training on the GDPR and freedom of information laws accessible to the public when he came on, a move he said was "quite radical" for the time. He also pointed to the implementation of the Age-Appropriate Design Code, which he enforces, as a significant step toward both keeping children safe online and creating change in how technology platforms design their products.

Now, Edwards is poised to lead the agency as it undergoes significant changes under the proposed Data Use and Access Bill, which passed through the House of Lords earlier this year.

"Much of the perceived promise and perils of Brexit related to data protection continue to be seen through the frame of the role and efficacy of the ICO," IAPP Research and Insights Director Joe Jones said. "Especially against a backdrop of constitutional change that would, if finalized, create the Information Commission, with Commissioner Edwards becoming its nonexecutive chair of the Commission's nonexecutive members and executive members led by a yet-to-be-appointed chief executive."

The law is not the only change Edwards will face. He said there is still much to learn about the effect of artificial intelligence on data rights and the promise and challenges associated with quantum computing. He said fundamental structural insecurities in the online system continue to be exploited and there is little transparency around how online advertising transactions are affecting consumers.


iapp25
#DPI24
iapp

Kashmir Hill

While New York Times technology reporter Kashmir Hill may not consider herself a privacy professional — she often refers to herself as a privacy pragmatist — her investigative journalism has uncovered several instances of consumer privacy harm, and in some cases, this has led to organizational accountability and global enforcement initiatives.

In 2020, Hill helped uncover and reported on Clearview AI, a little-known startup that scraped more than 3 billion photos from the internet to build a large-scale facial recognition app, which was then marketed to law enforcement. She followed her reporting with "Your Face Belongs to Us: A Secretive Startup's Quest to End Privacy as We Know It," documenting all the findings related to Clearview's practices.

The work sparked data protection enforcement around the world. Data protection authorities in France, Greece, Italy, the Netherlands and the U.K. issued steep fines against the company for alleged data protection violations with additional scrutiny coming from Australia and Canada. In the U.S., the company recently finalized a multimillion-dollar settlement over Illinois Biometric Privacy Act claims.

With the use of facial recognition technology, "our face becomes a key to unlocking in the real world everything that is knowable about us," said Hill in her keynote speech at the IAPP Global Privacy Summit 2024. "It makes possible a new era of discrimination, based on what you do, who you work for, what you believe, and all of the choices you have made in the past."

Within the last year, Hill pulled back the curtain on the privacy implications of connected cars. More specifically, she unveiled General Motors was sharing various categories of driving information with data broker LexisNexis.

Hill's reporting uncovered how consumers' sensitive data was sold to insurance companies, which in turn evaluated the data with an eye toward potentially raising individuals' insurance rates.

U.S. state attorneys general took Hill's work and spun it into consumer protection cases.

U.S. state attorneys general took Hill's work and spun it into consumer protection cases. Arkansas, New York and Texas each have active litigation with GM over its sharing practices. At the federal level, the U.S. Federal Trade Commission banned the automaker from selling drivers' behavioral and geolocation data for five years.

GM no longer shares consumer driving information with LexisNexis as result of Hill's work.

Beyond her work leading to meaningful enforcement, Hill also regularly writes about the grips of technology on society. She's produced several facial recognition reports covering the technology's inherent bias. More recently, she wrote pieces on individuals finding romantic attachment with AI chatbots.

Hill has never shied away from getting personal in her tech reporting. She's documented experiences with various emerging tech and fads.

"I've lived on Bitcoin, tracked my husband using Apple AirTags, and spent 24 hours in the metaverse," Hill explained in her New York Times author page. "In 2018, I gave a TED Talk ("What your smart devices know [and share] about you") describing what happened when I transformed my apartment into a smart home and monitored the data being collected by a web of tech firms."

And why does Hill cover all this ground? In her own words, "It is important to me that people harmed in some way by technology are not further harmed by our story about what happened to them."


iapp25
NATIONAL BESTSELLER
KASHMIR HILL
YOUR FACE BELONGS TO US

LEADERS

Harriet Pearson

It was 1996 and Harriet Pearson , CIPP/US, pregnant with her second child, had just been promoted to her first executive role at IBM when senior leadership asked her to "figure out privacy" for the company. By 2000, what was supposed to be a project, an addition to her existing portfolio, became significant enough to create a new executive role — chief privacy officer.

"IBM's appointment of me as CPO was a first for the Fortune 500," Pearson said, remembering it received major media coverage, including her participation in a live segment on CNBC and interviews with The New York Times and other large outlets.

"Being a privacy professional is hugely satisfying, and cybersecurity governance and preparedness is similar: complex, pervasive and important," said Pearson, who held the CPO role at IBM for 12 years — where she was also appointed the company's first security counsel — before leaving in 2012 to launch and lead the cybersecurity practice at global law firm Hogan Lovells.

At a time when IAPP President and CEO J. Trevor Hughes , CIPP, said there were few privacy professionals, Pearson was responsible for information and policy practices at a company with hundreds of thousands of employees and thousands of clients.

"Harriet Pearson is a rare and courageous leader in privacy," Hughes said. "She took a leap, many years ago, to become the first CPO of a major technology company. Many at the time characterized the move as career-threatening risk. But Harriet defined the role as strategic: a leader focused on the effective and safe use of data in a complex digital world. That vision was prescient then, and remains vital today."

"I treasure those early years of building the IAPP and am so very proud to see how far the organization has come."

Today, Pearson is a leading expert in privacy and cybersecurity, and a pioneer for new generations of privacy leaders. In the late 1990s, she said the number of professionals specializing in privacy could fit into a large conference room and there was no professional networking and education group available to them. She worked with others in the field to create what would ultimately become the IAPP and served on the organization's board of directors for a decade.

"I treasure those early years of building the IAPP and am so very proud to see how far the organization has come," she said of the organization that 25 years later has more than 80,000 members across 149 countries.

"I used to insist during IAPP board meetings that there was no limit to how big the IAPP could become, given the pervasiveness of data issues and technology trends."

In 2007, the IAPP awarded Pearson its highest honor, the Vanguard Award. In 2016, she was named North America's "Legal Innovator of the Year" by the Financial Times and in 2015, the National Law Journal recognized her as a "Cybersecurity and Data Privacy Trailblazer."

Now, after 30 years of pioneering work in industry, law practice and most recently as executive deputy superintendent and head of the cybersecurity division at the New York State Department of Financial Services, Pearson has established Axia Advisory to provide strategy, policy and communications consulting in the areas of cybersecurity, privacy and AI governance.

"The community of professionals in privacy, security and AI governance, what we all have in common is that we're working on super cool, super interesting and important issues that are pretty new and cutting edge. And when you're working on new and cutting-edge things, it is even more important to have a network and a community that you can look to for support and guidance," Pearson told the IAPP in September 2024. "So, I am reengaging with the community to see where I can apply my learned experiences and capabilities in a way that's helpful."

LEADERS

Julie Brill

The foundational work of regulators and practitioners have together shaped the modern-day privacy profession. Julie Brill, AIGP, is among a novel group that has contributed to the buildup from both perspectives over the years.

In her role as chief privacy officer and corporate vice president for global privacy, safety, and regulatory affairs at Microsoft, Brill plays a leading role in maintaining privacy and online safety standards for one of the world's biggest multinational technology companies. Her work is vital to Microsoft, but standing up a compliance regime across an ever-growing global regulatory landscape also lends a model to other companies navigating the same challenges.

The compliance work is supported by Brill's working knowledge of a regulator's line of thinking, having been an influential enforcer at the U.S. Federal Trade Commission before joining Microsoft.

Brill was appointed FTC commissioner in 2010 by former U.S. President Barack Obama and unanimously confirmed by the U.S. Senate. She was regarded as the FTC's top leader in privacy and named the commission's "most important voice on internet privacy and data security issues," by MLex. At the FTC, Brill pushed for consumers to have options to protect their privacy and urged policymakers to implement regulations to develop mechanisms that would allow consumers to decide what information companies can collect.

"While I still hope industry will rise to the challenge of protecting their customers' privacy, this issue has become too important — to the FTC's central mission and to consumers across the country — for us to continue to wait," said Brill during her keynote address at the IAPP Global Privacy Summit 2010. "If industry does not move in a meaningful way on this issue, I will not hesitate to call on Congress to provide consumers with meaningful notice and choice about how their information is used, and to give the FTC the enforcement tools it needs to make sure those choices are respected."

The unique experience of going from regulator to compliance advisor was more of an opportunity than a task, according to Brill in her 2016 interview.

Brill also advanced global cross-regulatory enforcement in her time at the FTC, playing a key role in advancing the EU-U.S. Privacy Shield. As she exited the agency in 2016, Brill told the IAPP that her highest accomplishment as commissioner was "helping to improve the dialogue between the United States and Europe with respect to how we do privacy here in the U.S."

The unique experience of going from regulator to compliance advisor was more of an opportunity than a task, according to Brill in her 2016 interview.

"I'll be in a position to advise companies about the process and what they will need to do to comply with the new enhanced requirements," she said, "and that will be something that's very important to know, that there are people like me, and others, who do have an understanding of what will be required and will work with companies to help them comply."

Brill was recognized in 2014 with the IAPP Privacy Leadership Award for her dedication to the privacy profession with promoting consumer privacy and advocating for solutions to support organizational transparency regarding privacy notice. At the time of the award, IAPP President and CEO J. Trevor Hughes, CIPP, said Brill "has been at the forefront of the discussion and action to protect today's consumers in the information age." He added, "It's an honor to recognize the work she has done to support the development of tools to give consumers better information and control over the collection and use of their personal online information."

LEADERS

Latanya Sweeney

Fundamental data privacy concepts like anonymity, pseudonymity and deidentification are now commonplace in the modern digital governance profession but they came to light from the work of pioneers like Latanya Sweeney.

Currently serving as Daniel Paul Professor of the Practice of Government and Technology at the Harvard Kennedy School, Sweeney's research goes back to the 1990s as a graduate student at the Massachusetts Institute of Technology when she first broke ground on what's now referred to as the "Weld Experiment."

In 1997, her research demonstrated the ease with which confidential information could be re-identified when crossed with other data sets. In this case, she successfully identified the then-governor of Massachusetts Bill Weld by cross-referencing data released to researchers from the state's Group Insurance Commission with the publicly available voter registration list for Cambridge, Massachusetts.

Not only did this combination of the two data sets identify the sitting governor, in other related research, Sweeney found through the 1990 Census data that the majority of the U.S. population — to the tune of 87% — could be uniquely identified by the combination of their gender, ZIP code and date of birth.

In a 2024 interview, Sweeney commented on her meteoric break into the data privacy space, saying, "One day I'm a graduate student. About a month later, I'm testifying in D.C ... laws around the world changed because of that experiment."

Indeed, Sweeney's work is cited in the Health Insurance Portability and Accountability Act and at least four court decisions and anonymity and de-identification requirements are included in data privacy laws around the world.

She is also co-credited with coining the term "k-anonymity," which aims to solve this problem: "Given person-specific field-structured data, produce a release of the data with scientific guarantees that the individuals who are the subjects of the data cannot be reidentified while the data remain practically useful."

After receiving her Ph.D. in computer science from MIT — the first African-American woman to do so — Sweeney founded the Data Privacy Lab at Carnegie Mellon University. The lab, which is now housed at Harvard University, focuses on teaching and research of privacy technology. In addition to reidentification, the lab has studied racial discrimination in online advertisements as well as genomic privacy issues.

Though Sweeney has published more than 100 articles in the data privacy and discrimination space, her article "Only You, Your Doctor, and Many Others May Know," is seen as a landmark piece of research. Sweeney noted that the state of Washington was one of 33 states that share or sell "anonymized" health records.

"I conducted an example re-identification study by showing how newspaper stories about hospital visits in Washington state leads to identifying the matching health record 43% of the time," she said.

As a direct result of the study, the state bolstered its anonymization protocols for health records. Her work has also revealed how secondary health data sold by pharmacies and data brokers could easily lead to re-identification.

Sweeney's work has been felt in the regulatory field as well. In 2014, she was named the chief technologist for the U.S. Federal Trade Commission. At the time, Edith Ramirez, the chairwoman of the FTC, said, "Technology issues are increasingly central to the FTC's work, and I am delighted to welcome Latanya to the FTC. ... She has done groundbreaking work in the anonymization of sensitive consumer information and privacy technology, and I look forward to the contributions she will make to the FTC's efforts to protect consumers."

Sweeney said her experience at the FTC was "fantastic."

"One of my goals was to make it easier for others to work on innovative solutions at the intersection of technology, policy and business. ... During my time there, I launched the summer research fellows program

and blogged on Tech@FTC to facilitate explorations and ignite brainstorming on FTC-related issues."

Sweeney's work has also veered into democratic elections. She worked with Ji Su Yoo and Jinyan Zang to help demonstrate identity theft and vulnerabilities in voter websites in the 2016 election.

In a recent podcast, Sweeney discussed the influence of her great grandparents, who were born in the 19th century, and in turn, helped raise her. They taught her the "Golden Rule — to do unto others as you would have them do unto you." But their influence reached deep into her work as well.

"My road to helping to pioneer data privacy had nothing to do with my great grandparents," she reflected, "but in reality, I was called back to think about my great grandfather many times in the early years of doing work, because … he lived most of his life in the Jim Crow South, and as a Black man at the time … he had a lot of principles about how you survive. And when you look at his principles of survival, they all came down to ways of having anonymity and how well it had served him."

As technology changes and "makes us all live in these sort of transparent lives and every minute of our lives is captured in data somewhere," Sweeney said, "I often think about his inability to have that kind of anonymity, and how if things change, culturally around you, it could be turned around against you if you don't have it."

LEADERS

Dan Solove

Professor Dan Solove is a leading expert in privacy law, a Bernard Professor of Intellectual Property and Technology Law at George Washington University Law School, a founder of privacy training company TeachPrivacy, author of books, law review articles, blog posts and more. He has testified before U.S. Congress, served as an expert in high-stakes litigation, and advised on emerging issues like facial recognition, data broker regulation and algorithmic discrimination. His work is so prolific that, as of 2020, he has become the most-cited legal scholar born after 1970. He has influenced the privacy field at large, shaping how lawyers, judges, academics, and professional communities understand and speak about privacy.

Solove's early scholarship, particularly his books "The Digital Person: Technology and Privacy in the Information Age" and "Understanding Privacy," laid the groundwork for privacy law as a distinct academic discipline. His "taxonomy of privacy," which breaks privacy down into discrete problems — information collection, information processing, information dissemination and invasion of privacy — has become a foundational framework cited by courts, regulators and academics globally.

He has explored how surveillance, data aggregation and bureaucratic decision-making can quietly erode individual freedoms. In "Nothing to Hide: The False Tradeoff Between Privacy and Security," he dismantled the idea that privacy is only for the guilty, reframing it instead as a structural safeguard essential to human dignity and democratic participation.

"The Myth of the Privacy Paradox" challenges the idea that there is a logical disconnect between how people "express strong concern about privacy yet fail to take easy and inexpensive steps to protect their privacy." He argues the issue is far more nuanced because, while people may hold broad values that stay the same regardless of context, their moment-to-moment privacy decisions necessarily depend on the context, how much they understand the risk of sharing their data, and how much of a difference they think their decisions will make.

More recently, Solove has written extensively about the risks posed by artificial intelligence and predictive analytics. "The Prediction Society: AI and the Problems of Forecasting the Future," which Solove coauthored with Hideyuki Matsumi, sounds the alarm about how "algorithmic predictions not only forecast the future but also have the power to create and control it." It criticizes current consent-based approaches and calls for more robust, context-sensitive regulation.

Despite his prominence within the field of privacy law, Solove is anything but inaccessible. Law professor and frequent co-author Woodrow Hartzog said of Solove: "What some people might not know about Dan is that he's a deeply generous and caring mentor, he has a deep love and knowledge of literature, and he's got a wicked sense of humor. So many people in the field, including me, owe their career to Dan. Because he is such a central figure in privacy, his passion, mentorship, and wit help set the tone and norms for the field."

David Botero, an incoming IAPP Westin Fellow and a mentee of Solove's, describes him as a selfless and encouraging person. "He is one of the most caring professors," says Botero, "especially when it comes to helping his students to build connections within the privacy space."

That ability to connect with people in a down-to-earth manner is perhaps what makes his body of work so appealing to such a wide audience. His ideas have influenced minds around the world and his writing has been cited in multiple Supreme Court cases. His legal acumen is honed on the body of privacy knowledge that he helped develop. But did you know he also wrote "The Eyemonger," a children's book that teaches the value of privacy? Have you read the cartoons he posts on his blog?

Technical ideas clearly delivered without pretense is a Solove signature. Along with Paul Schwartz, he quite literally wrote the book on "Privacy Law Fundamentals," a widely used reference text published by the IAPP that distills complex statutory and regulatory frameworks into an accessible

format used by privacy professionals the world over.

Solove's ability to make privacy law intelligible without diluting its complexity has made him a trusted voice across sectors. His work is ever-relevant as the field of privacy shifts and changes. He is a rare figure in the privacy world: both a thought leader and a teacher in the broadest sense. Whether he's mapping out the limits of consent, skewering privacy policies in a cartoon or mentoring the next generation of privacy professionals, his fingerprints are everywhere.

As Professor Hartzog says, "you can't be in this field without being exposed to Dan's incredible legacy as a privacy scholar." His impact as a teacher, author, mentor and innovator ripples throughout privacy law, and his influence will guide thought and law for generations to come.

Nuala O'Connor

The role of a privacy professional has increased and diversified in recent years thanks to connectivity with artificial intelligence and other touch points. It is hard to find a professional more equipped and adept at handling the transition than Nuala O'Connor, CIPP/G.

O'Connor served in several high-profile privacy roles in the private sector, advocacy and the U.S. government before taking a tide-changing position at Walmart as its first senior vice president and chief counsel of digital citizenship.

Most notably, O'Connor was appointed the first chief privacy officer for the U.S. Department of Homeland Security in 2003. That role came with responsibilities to uphold Privacy Act requirements within a department that launched arduous national security programs in the wake of terrorists attacks on 11 Sept. 2001.

Upon her exit from DHS in 2005, O'Connor told The Washington Post that her groundbreaking work was a successful "experiment" and "if the litmus test is the number of people we (ticked) off, then the answer is yes, although that doesn't make it the easiest place to be at times."

After DHS, O'Connor was entrusted with leading privacy endeavors at General Electric and Amazon.

Her impact on broader digital policy matters grew when she became president and CEO of the Center for Democracy and Technology, a renowned civil rights advocacy group. The CDT credited O'Connor with efforts to cultivate consensus around U.S. privacy legislation as well as increased policy focus on education privacy matters and major federal surveillance reforms in the wake of the Edward Snowden revelations in 2013.

Her impact on broader digital policy matters grew when she became president and CEO of the Center for Democracy and Technology, a renowned civil rights advocacy group.

"Nuala has been a groundbreaker in every privacy and tech policy she took on, defining what is possible in technology governance and linking compliance and policy to what it means for our society," Future of Privacy Forum CEO Jules Polonetsky, CIPP/US, said of O'Connor's work. "Remarkably, she has done so while mentoring co-workers and colleagues and being an incredible parent and spouse."

O'Connor jumped from the CDT to Walmart in 2019. Walmart Executive Vice President of Global Governance Rachel Brand described the nuanced digital citizenship role as covering "issues related to privacy, use of data and data governance, emerging technologies, cybersecurity, and records management."

AI matters were added to that mission in short order as O'Connor ushered in the Walmart Responsible AI Pledge in 2023. It features key pillars that encapsulate responsible AI governance and much of her own body of work: Transparency, privacy, security, fairness and accountability.

"The Walmart Responsible AI Pledge is about more than just AI," O'Connor wrote while introducing the pledge. "It is a moment in time for us to speak directly to our customers, members and associates; be transparent and address the concerns they may have with the rapid pace of technological innovation; and reinforce our commitment to using technology in ways that are safe and beneficial to them."

O'Connor is an IAPP Westin Emeritus Fellow and served on the IAPP Board of Directors for six years, including as board chair in 2010.


iapp25
Summit 2010
ciation.org/summit
IAPP Global Privacy Summit 2010

LEADERS

J. Trevor Hughes

As the IAPP celebrates its 25th anniversary, it's impossible to avoid highlighting the leadership of its long-time President and CEO J. Trevor Hughes, CIPP. Since September 2002, Hughes has steered the association from relative obscurity to a globally recognized, leading organization for privacy, cybersecurity, AI governance and digital responsibility professionals.

Now boasting 90,000 members across the public and private sectors in more than 150 countries, the IAPP has thrived under Hughes' leadership, vision and charisma.

From the beginning, Hughes had a vision others may not have seen, including where the organization would reside: Not in Washington, D.C., New York City or even Boston, Massachusetts. No, Hughes would build the IAPP from a quaint, coastal town in southern Maine — starting in a small office near a bagel shop, then a humble farmhouse, before expanding to a large office complex on Pease International Tradeport in Portsmouth, New Hampshire, with a growing sister office in Brussels, Belgium.

Agnes Bundy Scanlan, CIPP/US, the organization's first board of directors chair who hired Hughes in 2002, recalled his energy and vision back then. "It's something that has stayed with me, and I've seen it being an important part of the IAPP ever since. Trevor had a vision. He had a vision that I don't think the rest of us were ready for," Scanlan said.

Harriet Pearson, CIPP/US, who has also been recognized for her leadership in the space, said of the early days that Hughes "started creating experiences and serving members in a way that was optimal. … He was one of the early privacy professionals. He would have been successful at anything he chose to do, but this was a particular magic sauce."

In looking back on the early days, Scanlan told IAPP Associate Editor Jennifer Bryant that Hughes envisioned an organization that would span the globe, with conferences complete with in-house programming and publications, industry-leading certifications and training, as well as global conferences and regional KnowledgeNet meetings.

"Trevor's influence on the privacy profession has been both foundational and forward-looking," MasterCard Chief Privacy Officer, AI and Digital Responsibility and current IAPP board Chair Caroline Louveaux said. "His vision and leadership have helped elevate privacy and digital responsibility from a niche area of expertise to a strategic topic in boardrooms, policymaking communities and classrooms around the world. Trevor has shaped not just a profession, but a global movement."

"It would be an understatement to say that Trevor is one of the leaders of the privacy world. Trevor created the privacy community," said Goodwin Partner Omer Tene, who formerly served as vice president and chief knowledge officer at the IAPP from 2013-21.

"With a unique combination of vision, business acumen, intellectual curiosity, tireless energy and relentless mission focus, Trevor has created a global organization that supports a tremendous community of professionals who really do love their jobs," Tene continued.

IAPP Vice President and Chief of Staff Amy Sherwood, who has been with the organization since 2004, has seen Hughes' leadership and vision from the inside. "Trevor combines the unique skillset of business acumen with privacy expertise," she said. "He has been a champion of staff, who in turn have put their heart and soul into doing excellent work on behalf of our members. Trevor believes to his core that if you create a positive work environment you can do amazing things. He innovated a cool, flexible workplace, before it was a thing, and you can see it in this world-class association."

Over the years, Hughes has led the IAPP through the explosion of the profession with the advent of the EU General Data Protection Regulation and other laws in the U.S. and around the world. During the COVID-19 pandemic, Hughes steered the ship, even when IAPP staff could not work in the office or host in-person conferences. And with growing digital complexity with the rise of artificial intelligence and the proliferation of digital laws, Hughes has guided the IAPP with an expanded mission to meet its next iteration of challenges.

"Trevor's ability to navigate a path of stability and growth in an area characterized by a dizzying pace of change and deep policy divides, while remaining respected and liked across the political spectrum, among advocates, business representatives, academics, government and regulators around the world, is inspiring," Tene said.

"He has left his mark on generations of privacy professionals and in doing that," said Tene, "he's made all of us better."

Alastair Mactaggart

The absence of a U.S. comprehensive federal privacy law has been filled in recent years with the proliferation of comprehensive laws at the state level. California began the line of 19 state laws thanks to the relentless efforts of many stakeholders, but perhaps none more dedicated than Alastair Mactaggart.

Mactaggart's influential work helped lead to the California Consumer Privacy Act 's surprising passage in 2018, which took effect in 2020, and the ballot initiative that spawned amendments three years later through the California Privacy Rights Act.

His advocacy began in 2016, after a conversation with a Google software engineer revealed the vast extent to which companies collect and use consumer data. The curiosity quickly turned into the motivation that spurred years of work toward finalization of the CCPA.

"These giant corporations know absolutely everything about you, and you have no rights," Mactaggart said in 2018 remarks following the passage of the CCPA. "I thought, oh, I'd like to find out about what these companies know about me. Then I thought, well, someone should do something about that."

The CCPA represented a major shift for U.S.-based privacy professionals as the EU General Data Protection Regulation was coming online as California's law was passed. The two laws became foundational to the privacy compliance measures deployed across global jurisdictions.

Mactaggart called the CCPA "a great stride forward" the day it was signed. No one knew then that he had more strides to come in the form of Proposition 24, the ballot measure for the amendments under CPRA, which he announced as a keynote speaker at the IAPP's Privacy. Risk. Security. 2019 conference in Las Vegas.

Propelled by the Mactaggart-backed advocacy group Californians for Consumer Privacy, the measure significantly expanded the CCPA, including new rights, amended scope and the addition of sensitive personal information. The measure also proposed the California Privacy Protection Agency — a first-of-its-kind U.S. regulatory body tasked with exclusively enforcing privacy laws in the state.

The ballot initiative was approved by California voters 3 Nov. 2020, not even a full year after the CCPA took effect.

Mactaggart explained the urgency behind passing Prop 24 during a conversation with IAPP Editorial Director Jedidiah Bracy in October 2020. He feared industry would quickly dissolve the provisions of the CCPA if it didn't get a swift update, noting, "I don't think legislation is a strong enough moat around the law, even with regard to privacy."

In that same conversation, Mactaggart advocated for California exploring an adequacy decision with the EU, which is still being discussed between the CPPA and the European Commission. He said receiving adequacy would be "great for consumers, because clearly one of the strongest protections is the GDPR right now. So, we in California deserve those protections. And if we're part of a larger framework, there's less chance that I think these things go sideways."

Mactaggart's influential work helped lead to the California Consumer Privacy Act 's surprising passage in 2018

In 2022, California Attorney General Rob Bonta appointed Mactaggart to the CPPA Board, furthering his imprints on California and U.S. privacy. As a board member, he provides input and perspective on the CPPA's work, including enforcement and promulgation of regulations.

More recently, Mactaggart and the board have worked toward helping the CPPA tackle regulations clarifying provisions for automated decision-making technologies, risk assessments and cybersecurity audits under the CCPA.

LEADERS

Jan Philipp Albrecht

Before the EU General Data Protection Regulation came online in 2018, the European Union had not updated its data protection regime since 1995. Jan Philipp Albrecht made It his mission in European Parliament to change that and give EU citizens more modern protections over their online presence.

Albrecht, a former German MEP, helped to shepherd the law to passage in 2016 following consideration of thousands of amendments during the EU's unique legislative process. He acted as GDPR rapporteur for Parliament's Committee on Civil Liberties, Justice and Home Affairs, taking part in trilogue negotiations between Parliament, the Council of the European Union and the European Commission.

With the GDPR's passage, Albrecht touted the "confidence, legal certainty and fairer competition" provided under a law covering all member states and the European Economic Area.

"The general data protection regulation makes a high, uniform level of data protection throughout the EU a reality," Albrecht said in a 2016 statement. "This is a great success for the European Parliament and a fierce European 'yes' to strong consumer rights and competition in the digital age. Citizens will be able to decide for themselves which personal information they want to share."

The global data protection landscape might not be what it is today without Albrecht's vision for the GDPR. Threads of the landmark legislation can be found in a majority of the laws enacted across 144 countries.

The ability to navigate legislative negotiations was no small feat for Albrecht and trilogue participants. As noted in a 2016 interview, EU member states had to put the bloc ahead of the norms and processes observed within their respective jurisdictions.

"These were discussions in which everyone let themselves be influenced by everyone else to some extent, so that the best result could emerge," Albrecht said. "Nevertheless, it is a European process. This means not just taking a bit from here and there but also discussing things in a European context."

The amendment process was tedious, but showed Albrecht in his element, according to Future of Privacy Forum Vice President of Global Privacy Gabriela Zanfir-Fortuna. She said his work "personified that whole passion of making sense of the madness."

"He did that by always speaking truth to power. He was a true leader spearheading that effort and, frankly, representing the voice of 'data subjects' in the negotiation process with the Council and the Commission," Zanfir-Fortuna added.

Albrecht's post-GDPR work in Parliament included a focus on U.S. mass surveillance and its impact on Europeans' fundamental right to privacy. His concerns hit at the heart of the ongoing issue around data protection for signals intelligence in relation to EU-U.S. data flows.

In the leadup to the EU-U.S. law enforcement data sharing agreement in 2016, Albrecht signaled the need for a consumer redress mechanism to be included in the framework while any deal "should not compromise the existing legislation on data protection that we have in the EU."

Albrecht's argument was magnified when the EU-U.S. Privacy Shield was agreed to months later. The agreement replaced the Safe Harbor framework that was invalidated by the Court of Justice of the European Union, which highlighted the lack of adequate protection for EU citizens' data when transferred to the U.S.

In a statement after the agreement was finalized in 2016, Albrecht called the Privacy Shield "a blank cheque" for EU-U.S. transfers and said the European Commission "should not be simply accepting reassurances from the U.S. authorities but should be insisting on improvements in the data protection guaranteed to European consumers."

The advocacy led to the eventual invalidation of the Privacy Shield and more rights-focused negotiations toward its replacement, the EU-U.S. Data Privacy Framework.

LEADERS

Kabir Barday

The growing web of privacy and data protection regulations across global jurisdictions has put a premium on streamlined and adaptable legal compliance. Those needs spawned opportunities in the privacy technology vendor market that Kabir Barday, CIPP/E, CIPP/US, CIPM, CIPT, FIP, seized upon with the creation of OneTrust in 2016.

As founder and CEO of OneTrust, Barday has presided over an unprecedented rise for the company and helped spur broader investment in the markets for compliance tech vendors and data management platforms. The company was valued at USD1.9 billion in July 2019 and rose to USD5.1 billion in December 2020. Today it boasts approximately 14,000 customers across 100 countries along with 300 patents for compliance tools.

"Kabir formulated the idea for OneTrust in a breakout session at the IAPP Privacy. Security. Risk. 2016 and built it into a leading force in navigating privacy, AI, and digital governance," IAPP President and CEO J. Trevor Hughes, CIPP, said. "Thousands of companies around the world rely on the tools OneTrust has created. His leadership and vision have been central to the growth of our field."

The rise of OneTrust was fueled by the recognition of respective compliance needs stemming from the EU General Data Protection Regulation and the California Consumer Privacy Act. Barday and the company established compliance solutions through a holistic lens, realizing many companies would need to tailor compliance to a range of unique requirements in multiple jurisdictions.

"Our goal was to bridge the gap between legal requirements and real-world implementation," Barday said at IAPP GPS 2024. He added privacy was long viewed as a legal challenge, but OneTrust considered it "an operational one."

OneTrust's work helped privacy enter the mainstream in 2020. Inc. Magazine named OneTrust as the U.S.'s fastest-growing company, noting Barday recognized the need for compliance tools and claimed the way he seized the opportunity is "a lesson in diligent prep, great timing, and aggressive action."

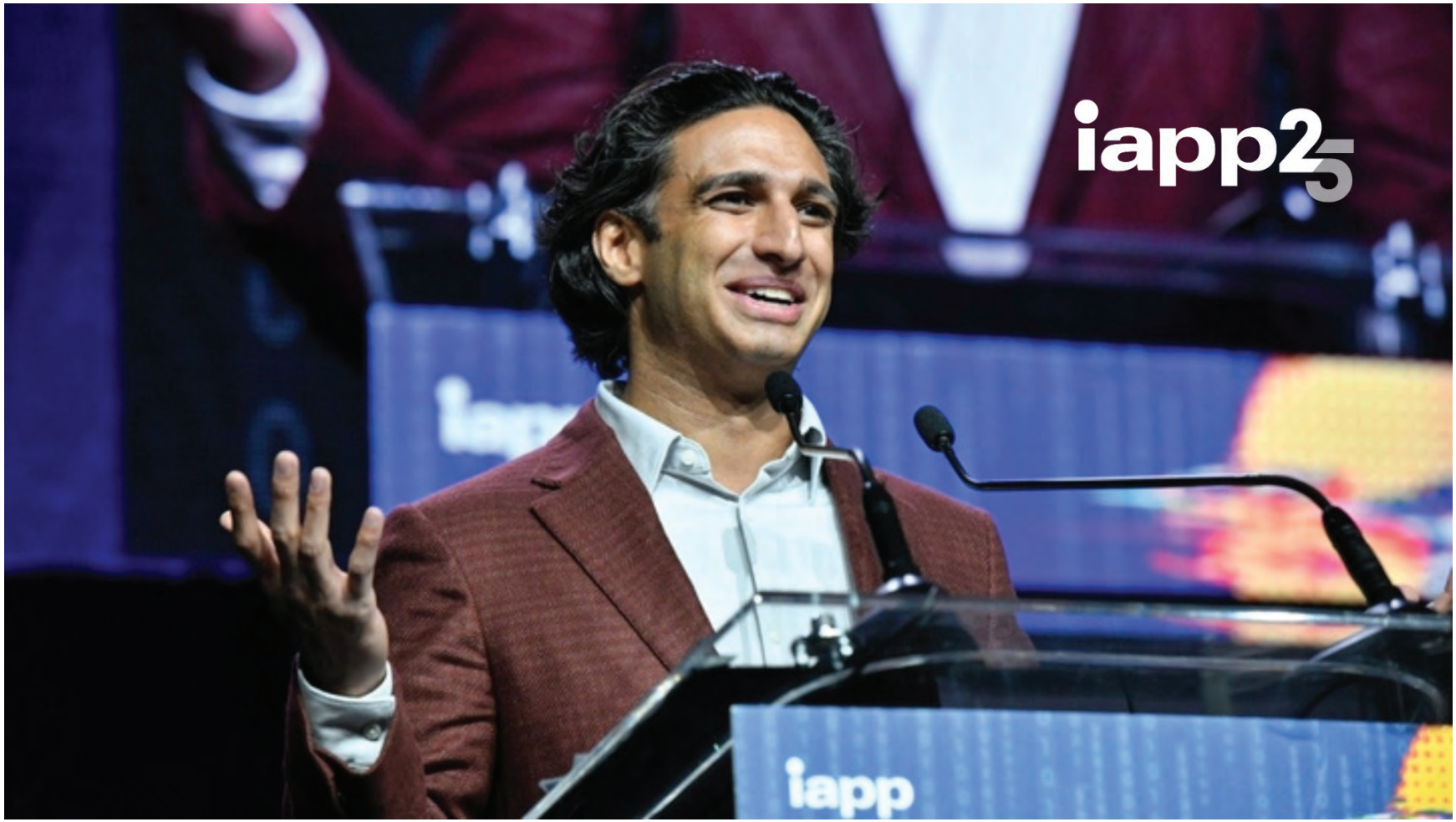
Speaking to the IAPP in 2020 about the Inc. ranking, Barday said the recognition signaled a "healthy market" for privacy compliance vendors and shift in perceptions around data privacy as a business imperative.

"Five years ago, privacy wasn't something that companies could compete on. It was just a compliance checkbox function. Privacy has now become increasingly something that companies can compete on," Barday said. "We are seeing that every day in how consumers make buying decisions based on trust. I think it's a great moment for the privacy professional to use that as a point to bring up in their board meetings to get increased visibility and investment in their function."

Prior to leading OneTrust, Barday served as AirWatch's director of product management. His work on the AirWatch Enterprise Mobility Management Platform's Privacy First initiative earned the company the 2016 HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology. The initiative focused on "developing product features to help organizations comply with privacy principles by default while providing transparency, access, and choice to end users."

The Georgia Institute of Technology Alumni Association also recognized Barday's leadership in 2020, placing him on its 40 under 40 list for his achievements in the privacy field.

As the privacy profession continues to proliferate and adapt to the digital governance ecosystem, Barday and OneTrust have created a model for how entrepreneurship and leadership can foster responsible innovation that can boost an entire industry.



LEADERS

Liz Denham

Elizabeth Denham began her career as a city archivist and privacy coordinator for a health region in Canada, at a time when there was no such career path as being a privacy regulator.

But a passion for data — which Denham told the IAPP in 2022 was in her DNA — launched an "incredible" and "astonishing career and responsibility" that has included serving as Information and Privacy Commissioner for British Columbia, Assistant Privacy Commissioner of Canada and U.K. Information Commissioner. Denham is a former chair of the Global Privacy Assembly and in 2019 was awarded Commander of the Order of the British Empire in the Queen's New Year's Honours list for her services to protecting information.

In 2022, Denham joined Baker McKenzie as international advisor to its data and technology practice, and in 2023 she joined the Information Accountability Foundation as chief policy strategist. Most recently, she was appointed chair of the Jersey Data Protection Authority, and she also serves as a trustee on the board of the 5Rights Foundation, a nonprofit focused on children's online privacy and safety.

"Sometimes I think I've been blessed by being at the right place at the right time," Denham told the IAPP in 2022. "My career happened because I was at the forefront of information management and information governance which led to the need for freedom of information and data protection legislation."

As U.K. Information Commissioner, a role she held for five years, Denham oversaw implementation of the U.K. General Data Protection Regulation and the Data Protection Act. The landscape around children's online privacy protections would not be what it is today without Denham's leadership. During her time at the ICO, the U.K. Children's Code was established to give a code of practice for online services likely to be accessed by children and has heavily influenced regulatory reforms around the world.

In 2022, the IAPP presented Denham with its Privacy Leadership Award, a recognition she received alongside privacy leaders and mentors, including the late former European Data Protection Supervisor Giovanni Buttarelli and academic and author Dr. Alan Westin.

IAPP President and CEO J. Trevor Hughes, CIPP, called Denham "a shining example of leadership in the privacy field" who has "demonstrated a steadfast focus on protecting privacy while navigating the rapidly changing technological and political realms."

As U.K. Information Commissioner, a role she held for five years, Denham oversaw implementation of the U.K. General Data Protection Regulation and the Data Protection Act.

LEADERS

Julia Angwin

Growing up in Silicon Valley, Julia Angwin believed she would eventually work in technology. Little would she know falling in love with journalism would lead her down a similar path — but instead of developing tech, she exposed its inner workings.

Angwin, now a New York Times contributing writer with a background in mathematics and business, has made an award-winning career out of understanding how technology shapes our lives during a time when digital privacy was still a new concept, she said during the IAPP Global Privacy Summit 2022 keynote panel.

"You used to buy software in boxes, it was all shrink-wrapped and you paid money for it, and all of a sudden it was free, and they were doing something with your data," Angwin said then. "That seemed weird."

That curiosity led Angwin along with other colleagues at The Wall Street Journal to publish "What They Know," a multi-part series digging into how personal information is pulled from cellphones and computers by corporations and public officials — usually without a person's knowledge. The series touched on everything from how companies can use personal data to offer targeted pricing to how license plate tracking became commonplace, even for people not suspected of crimes. Angwin collaborated with several journalists and researchers, including Ashkan Soltani, who eventually became executive director for the California Privacy Protection Agency. The series made a splash and was named a 2012 finalist for the Pulitzer Prize in explanatory reporting.

"I thought that would be a one-year series, and 12 years later, I'm still on the same story," she said during the 2022 panel.

The series reverberated throughout the privacy world: Future for Privacy Forum's co-founder, Christopher Wolf said, "the series has provoked debates and discussions about privacy that we have never seen before. It quite literally has made privacy front page news. In many ways, the series of articles about online privacy that The Wall Street Journal began publishing last year has set the tone for the privacy debate nationally."

That included in U.S. Congress, where lawmakers pressed big technology firms on their tracking practices and the Obama administration called for stricter privacy protections against data collection.

Three years later, Angwin published a book showing the travails of trying to escape these data collection practices in "Dragnet Nation: A Quest for Privacy, Security and Freedom in a World of Relentless Surveillance." She "mostly fails" at a full escape from digital tracking, noted Dov Greenbaum, CIPP/E, now the director for the Zvi Meitar Institute for Legal Implications of Emerging Technologies at Reichman University, in a 2014 book review for the IAPP.

The work demonstrated how even privacy-savvy people could have difficulty protecting their data online, Greenbaum said. And he noted it would likely only grow harder as technology advances. "As data storage becomes cheaper and algorithms to mine data become more advanced, we are likely to see a growing trend toward further and more expansive online privacy intrusions beyond those described in the book," he wrote.

Angwin would prove that to be true again in 2016, when she and a team of reporters at ProPublica published "Machine Bias," a multi-part series exploring how algorithms can be used to perpetuate bias and shape the way we interact with social media, online shopping and the criminal justice system. That work was a finalist for a Pulitzer Prize in explanatory reporting in 2017.

After reporting under those mastheads, Angwin founded The Markup, a nonprofit dedicated to technology reporting through a public service lens, now part of CalMatters. The news organization also developed "Blacklight," a tool which scans websites for tracking information. She left The Markup in 2023.

Several high-profile data scandals — such as revelations about how Cambridge Analytica and Facebook harvested user information

for political advertising without user consent — have happened since "What They Know." Angwin said in 2022 more people are aware of companies' tracking efforts than when she first started writing about privacy, but do not always understand why it is a problem, especially if they do not use a particular service. Her work, she said, is to help people understand how a collective problem affects them, too.

"I think that is what people want, they want to know a little bit more precisely, not just generally what bad, scary things are happening," she said then, "but what bad, scary things are happening to me?"

Bojana Bellamy

If you have ever met Bojana Bellamy, CIPP/E, the President of the Centre for Information Policy Leadership, then you have almost certainly sensed her expertise, boldness and charisma. Impacting global data privacy, cybersecurity and legal compliance now for more than 25 years, she continues to tackle the biggest issues in the field. From global privacy and digital policy, the EU's emerging digital law and policy framework, to the role of privacy-enhancing technologies in AI, to the risks impacting cybersecurity breaches and litigation, Bellamy has seemingly said and done it all.

She is the president of Hunton Andrews Kurth LLP's Centre for Information Policy Leadership, a prominent privacy and data policy think tank located in Washington, D.C., London and Brussels. Under her direction, the CIPL has connected industry leaders, regulatory authorities, and law and policymakers, producing guidance, recommendations, and best practices. Through its involvement in government consultations on issues such as reforms to children's privacy and U.S. federal privacy law as well its work to create accountability frameworks, assess the impacts of the EU General Data Protection Regulation and provide guidance on creating more agile, effective regulation, the CIPL offers critical structures for legal compliance as well as thought leadership on outcome-oriented regulation.

Bellamy also sits on several advisory boards, including the Internet Commission Advisory Board, the Organisation for Economic Co-operation's Privacy Guidelines Expert Group and the Thomson Reuters' Practical Law Data Protection Consultation Board, as well as the Advisory Board of the Tech, Law and Security Program at the American University Washington College of Law.

At any IAPP conference, you need only glance around the room to find someone deeply impacted by Bellamy's work.

"Bojana has inspired countless privacy, data, and technology policy professionals around the world with her unparalleled enthusiasm for the potential of responsible, data-driven innovation to benefit individuals, organizations, and society," Centre for Information Policy Leader Director of Privacy and Data Policy Matthew Reisman said. "She has made a lasting impact on our field through her work evangelizing concepts of organizational accountability, such as the CIPL Accountability Framework. Bojana's passion for moving forward our collective wisdom on how to get the best out of technology and data is infectious: she delights in engaging with and bringing together thinkers and practitioners of every background and discipline to learn from one another. It is a privilege to work with and learn from her."

In a story that many others can likely relate to, IAPP Vice President and Chief Knowledge Officer Caitlin Fennessy, CIPP/US, , recalled, "I remember so clearly the first time I met Bojana and suspect I am not alone. I was seated in front of her at a European Parliament committee hearing on EU-U.S. data transfers, considering how to address misunderstandings the presenters had raised, when Bojana stood up and boldly, clearly, and unequivocally set the record straight. She is bold, articulate, unequivocal, and yet always diplomatic and polished as she debates and discusses the best path forward for data protection."

CIPL Director of Privacy Policy in Brussels, Natascha Gerlach, CIPP/E, said Bellamy's impact on the CIPL has been instrumental.

"Bojana has been a leading voice in the global privacy and data protection community for many years, bringing a uniquely practical approach to the complex challenges of responsible data use," Gerlach said. "With her forward-looking vision on how to unlock the value of data in a way that preserves fundamental rights, she has helped shape the international dialogue on the future of privacy and responsible innovation. Under her leadership, CIPL has risen to the forefront of global thought leadership, providing actionable insights and progressive strategies for the accountable use of data to regulators, policymakers, and organizations alike."

The dynamism of Bellamy's thought is also evident in her written work. In an article she penned for the IAPP back in 2018 called "A letter to the unsung hero of the GDPR," her compassion shines through as she addresses privacy counsels, data protection officers and others, highlighting the value of their work, time and effort. In recognizing and giving credit to these sometime underappreciated "philosophers-and-ethicists-in-residence," she tells them, "what you do is unique, and you are amazing."

Bellamy is not just a leader of our community; she has profoundly shaped it with her insights into how laws and policies intersect with real-world practices. She was one of the 20 data privacy experts chosen to participate in the trans-Atlantic "Privacy Bridge Project," which provided recommendations to bridge the gaps in the privacy frameworks of the EU and the U.S., for example, by deepening collaborations between authorities and engagement between governments, discussing the new approaches to transparency, and enacting best practices for deidentification and security breaches. Her voice and expertise continue to make a lasting impact on EU-U.S. data protection and privacy policy from accountability to data transfers to deidentification and AI.

Notably, in 2019, she received the IAPP Vanguard Award, which recognizes "greatness and creativity in building a foundation for the fields of privacy AI governance, cybersecurity law and digital responsibility." On receiving her reward, she reflected that "What I and my career have been about has a real impact and purpose. Having that feeling really drives me as I come to work each day."

Helen Dixon

The seven core principles that comprise the EU General Data Protection Regulation helped set the stage for the global privacy profession's meteoric rise since 2018. Equally important to that growth trend is the continued reinforcement of those principles through strong, meaningful enforcement.

EU data protection authorities are showing their teeth in different ways to uphold the GDPR, with Ireland's Data Protection Commission among the most active enforcers. The brunt of the DPC's high-profile rulings were handled under the watch of former commissioner Helen Dixon, who navigated the challenges of building up the DPC's posture while simultaneously tackling data protection issues among the most prominent names in Big Tech.

Dixon spent a decade with the DPC, starting with her initial appointment in 2014 until her departure in February 2024. She presided over the expansion of the DPC's powers under the GDPR, which entailed becoming the lead supervisory authority for a majority of U.S. technology companies that established EU operations in Ireland.

Dixon approached the increased authority with fines totaling billions of euros during her tenure that simultaneously created strong deterrents while helping to shape best practices for GDPR compliance.

"At all times, the DPC stands for effective and proportionate implementation of the rules," Dixon said in a 2023 LinkedIn post announcing her departure from the DPC. "Year-in and year-out, the DPC handles and resolves thousands of complaints from individuals and, without any doubt, is in the vanguard internationally in concluding precedential investigations under the General Data Protection Regulation, the effects of which are applicable across the EU."

Dixon and the DPC proved to be a linchpin for EU-U.S. data transfers, as their dispute over the legality of Meta's transfer practices resulted in the invalidation of the EU-U.S. Privacy Shield by the Court of Justice of the European Union in July 2020.

During an IAPP LinkedIn Live highlighting the CJEU decision, Dixon discussed how "none of us may like the answer that (the CJEU) came up with" but ultimately her office was "significantly satisfied that the judgement does deliver clarity on the key issues that we needed decided." And for companies impacted by the invalidation and searching for a path forward, she said, "the company is obliged to suspend or not initiate the transfers based on the documented analysis it conducts."

That was not the only battle between the DPC and Meta during Dixon's tenure. The DPC's enforcement work against Meta subsidiaries alone has generated more than 2.5 billion euros in penalties.

Half of that total came 22 May 2023 when Dixon and the DPC fined the company 1.2 billion euros over allegations of unlawful Facebook data transfers, storage and processing to the U.S. The fine was paired with suspension orders that threatened Meta's EU operations and ultimately resulted in more robust compliance measures.

Dixon faced some criticism from regulatory counterparts and a range of stakeholders for how her office carried out its business, putting her in a challenging situation. In an op-ed reflecting on her time at the DPC, Goodwin Proctor Partner and IAPP Westin Emeritus Fellow Omer Tene said those that took issue with Dixon's efforts "failed to see the forest for the trees."

"The DPC led massively complicated investigations, including the grunt work of meticulous fact finding and legal analysis, which sometimes takes years," Tene wrote.

The buildup of the DPC's staffing is an overlooked aspect of Dixon's impact. Personnel grew from 27 to 215 under her watch and the DPC's budget increased to 29 million euros in 2025, which was up from 1.9 million euros in 2010.

Upon her departure, she called the DPC a "a critical element of EU machinery."

"The full implementation of the GDPR will remain a work-in-progress across the EU and, as the larger-scale enforcement cases now conclude, we see in Ireland and beyond, that these decisions are often subject to

judicial challenge," she wrote in her farewell. "It will take a further number of years to bottom-out definitive interpretations of applications of this principles-based law, but the groundwork is now well laid."

Earlier this year, Dixon resigned from her role as commissioner of Ireland's Commission for Communications Regulation. She recently announced her next move outside of regulatory leadership and the digital space, joining the board for Irish environmental nonprofit Repak as an independent non-executive director.

Lorrie Faith Cranor

Privacy engineering expert and professor Lorrie Faith Cranor, CIPT, has become one of the most influential voices in the privacy community, inspiring researchers to view privacy as a fundamental design standard rather than an abstract ideal.

As the Director and Bosch Distinguished Professor of the CyLab Security and Privacy Institute and the FORE Systems University Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University, Cranor has helped reshape the technology field with more than 200 co-authored research papers on online privacy and security.

In addition to her extensive academic work, Cranor in 2016 served as chief technologist at the U.S. Federal Trade Commission, where she brought her consumer-focused approach to national policymaking. Her tenure there underscored her belief that protecting data requires systems designed with human limitations in mind.

She also co-founded Wombat Security Technologies, later acquired by Proofpoint, a company dedicated to security awareness training that helps organizations educate employees on safe online behavior.

Cranor's work focuses on understanding how people interact with digital systems and where those systems fail them. Through decades of research, she has revealed how confusing language, poor interface design and misleading consent mechanisms leave users more exposed than they realize. By emphasizing usability alongside security, she has redefined what it means to build technology that genuinely protects consumer privacy.

In 2004, Cranor founded the Symposium on Usable Privacy and Security, a conference that brings together leading researchers, designers and policymakers to discuss emerging issues around consent, transparency and trust. The event has since become one of the most respected venues for privacy and security scholarship, setting the tone for how human-centered design influences data protection.

"Lorrie Cranor wrote the book on how to conduct and support gold standard privacy and security research that has a massive policy impact. Additionally, her work as chief technologist for the FTC showed how computer science, human-computer interaction, and engineering expertise can serve the public and how law and policy is all the better for it," Boston University School of Law Professor of Law Woodrow Hartzog said. "She's a towering and indispensable scholar in our field, and I continue to learn so much from her and her work."

If that wasn't enough, Hartzog said Cranor is "a brilliant artist." Her "Security Blanket" quilt, inspired by research on text-based passwords, "is still one of my favorite privacy and security creations," he said.

Containing 1,000 popular passwords designed onto a fabric sheet and then quilted, Cranor said in a blog post, "The colors, size, and format of this quilt were designed to be reminiscent of a baby quilt, which I imagine might become a security blanket. Like the passwords included in this piece, a security blanket offers comfort, but ultimately no real security."

Among Cranor's most notable research contributions is "The Cost of Reading Privacy Policies," a paper co-authored with Aleecia McDonald. The study found it would take the average internet user roughly 10 minutes to read a single privacy policy, or nearly 200 hours per year to read each one they encounter. The research exposed the impracticality of expecting users to fully understand complex data practices and highlighted a systemic problem in how privacy is communicated online. Cranor's work called for clearer, standardized privacy notices that allow consumers to quickly grasp how their data is collected, shared and stored.

Her groundbreaking research has earned numerous honors. Cranor received the IAPP Privacy Leadership Award in 2018 for her research and advancement in the privacy field. She was also named one of Technology Review magazine's Top 35 Innovators Under 35 in 2003 and awarded the IEEE Cybersecurity Award for Practice in 2018 for her contributions to real-world privacy and security solutions.

"Lorrie Cranor, for 20 years, has been a leading voice and a leader in the privacy field," said IAPP President and CEO Trevor Hughes, CIPP. "She developed some of the earliest privacy-enhancing technologies, created a groundbreaking program at Carnegie Mellon University to train future generations of privacy engineers, and has been a steadfast supporter, participant, and leader in the field of privacy that entire time. Her merits as recipient of our Privacy Leadership Award are unimpeachable. She's as great a person as we have in our world."

Peter Swire

The last decade saw not one but two invalidations of major trans-Atlantic data flow arrangements by the Court of Justice of the European Union — first to EU-U.S. Safe Harbor and then Privacy Shield. Each seismic event sent waves through the business world, pressuring privacy professionals to find alternative transfer mechanisms to keep day-to-day business on track. Among those who helped lead a response was Peter Swire, CIPP/US.

But that's not when his story starts.

Swire has a long history in privacy. He helped create the landmark Health Insurance Portability and Accountability Act Privacy Rule while serving in the Clinton administration, setting the standards for health care privacy rules in the U.S. He was also the first person to serve as the chief counselor for privacy for the Executive Office of the President at the Office of Management and Budget.

According to a USA Today profile from 2000, Swire was prescient about many privacy topics still discussed today, particularly when it came to translating information into digital formats. For instance, the advent of state and local governments putting paper records on the internet would make it easier to compile essentially a "dossier" on a person by conducting an online search, he said at the time.

But it is Swire's work on cross-border transfers that has brought him attention in recent years, particularly after the "Schrems I and II" decisions.

Swire has written extensively about each decisions' long-range impact and the various issues associated with them, such as redress mechanisms. He told the U.S. Senate Committee on Commerce, Science & Transportation during a 2021 hearing that the Privacy Shield decision could be an opportunity for lawmakers to strengthen U.S. privacy laws, which might be welcome in a time of uncertainty.

His paper on the subject, co-authored with Georgetown University Law Center's Kenneth Propp, won him acclaim from the Future of Privacy Forum in 2021.

Future of Privacy Forum CEO Jules Polonetsky, CIPP/US, said Swire's impact ranges across academic scholarship, industry practices and government policy.

"From competition, to interoperability, to HIPAA and cross-border data flows, Peter has grappled with many of the hardest challenges in data protection, bringing intellectual rigor together with political sensibility and a pragmatic understanding of the possible," he said. "I am one of many who look to him as a mentor and a friend."

Other notable accomplishments include serving on President Obamas's Review Group on Intelligence and Communications Technology and as the co-chair of the World Wide Web Consortium's Do Not Track Process. He is the J.Z. Liang Chair in the School of Cybersecurity and Privacy, in the Georgia Tech College of Computing and research director for the Cross-Border Data Forum.

Swire has a long history with the IAPP, as well. He helped create the organization's first official textbook in 2005, called by former IAPP Vice President Peter Kosmala the "bible for the practice of privacy."

Swire is also a frequent contributor to the IAPP's editorial publications, including a number of op-eds and analysis pieces on cross-border data flows, prospects for a federal privacy law and other pressing topics in the space.

In 2015, the IAPP recognized Swire's work by presenting him with its Privacy Leadership Award. In accepting it, Swire said, "We are fortunate to be privacy professionals in this era when privacy is at the center of so many important debates in our society."

"Working on privacy gives me an opportunity to teach, and hopefully inspire, a new generation of students and privacy professionals," he said. "One great pleasure of attending IAPP functions is the opportunity to talk with former students and see how they have grown into leaders in their own right. Today, and moving forward, I feel fortunate to be part of some amazing organizations as we study and address some of the most pressing privacy problems in the world."

LEADERS

Danielle Citron

Whenever her name is mentioned, the immediate reaction is always one of admiration. An inspiring, remarkable, thoughtful leader and mentor to many, Danielle K. Citron, who is the Jefferson Scholars Foundation Schenck Distinguished Professor of Law, Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law, and inaugural director of the LawTech Center at the University of Virginia School of Law, writes and teaches about privacy, civil rights and free expression.

In her work, Citron examines how social attitudes, cultural practices and the law affect how we think about privacy. Conceptually, she has helped to evolve privacy from the idea of "information control" to a notion enabling self-knowledge (both physical and mental), intimacy, and the building of close relationships. As she explains, privacy "carves out an invisible space with our bodies and thoughts so we can develop a sense of self and identity." In a world with a seemingly unlimited supply of privacy definitions, hers helps us to map out how to maintain dignity, vulnerability and trust within a technology-driven marketplace.

To describe Citron as a pioneer or innovator would be accurate but fall short; her legal thought is more akin to that of an oracle, soothsayer or seer. She has been writing about cybercrime since the dawn of the Information Age. Her work on the criminalization of revenge porn and regulatory oversight of predictive algorithms have been informing policy debates for well over a decade. She had analyzed the looming legal challenges posed by deepfakes well before most of us had even heard of that term.

As another example of her foresight, several years prior to the passage of any comprehensive U.S. state privacy laws, Citron's paper on The Privacy Policymaking of State Attorneys General examined the centrality of U.S. state attorneys general as "agents of regulatory change" in enforcing U.S. consumers' privacy rights. (Her work here also won the IAPP's award for best paper at the 2016 Privacy Law Scholars conference.) In a foretelling of developments in state-level privacy enforcement that we are seeing accelerate today, she urged state attorneys general at the time "to act more boldly in the face of certain shadowy data practices."

In her work, Citron blends legal erudition with incisive and pragmatic privacy advocacy. Counterintuitively, she has shown that "intimate privacy…and free speech are not at odds but instead reinforce each other." She has written numerous book chapters and published more than 60 law review articles and essays on issues ranging from the right to sexual and intimate privacy, student surveillance, combatting online harassment and cyberstalking, to reform of Section 230, automated decision making and government surveillance.

Her first book, Hate Crimes in Cyberspace, was named one of the 20 best moments for women in 2014 by the editors of Cosmopolitan, while her latest one, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age, has been featured and excerpted in The New Yorker, Wired, Fortune, The Guardian, and The Times. In addition to her legal repository, she has written more than 50 opinion pieces for major media outlets, including The New York Times and Slate. Her TED Talk on deepfakes has been viewed more than 3.5 million times, and she has given hundreds more talks at universities, federal and state agencies, foundations, associations, and think tanks. She chats and converses regularly with the IAPP and has appeared on the big stage at our annual conferences.

Citron is also vice president of the Cyber Civil Rights Initiative, a nonprofit founded in 2013 that is devoted to fighting for civil rights and liberties in the digital age. She is a MacArthur Fellow, member of the American Academy of Arts and Sciences and the American Law Institute and has served on advisory boards for the Electronic Privacy Information Center, Future of Privacy Forum and the IAPP's Privacy Bar Section Advisory Board .

In 2024, she won the IAPP's Leadership Award, which "recognizes an individual or organization who demonstrates an ongoing commitment to furthering privacy policy, promoting recognition of privacy issues, and advancing the growth and visibility of the profession."

Citron has worked for years to help lawmakers design laws that protect intimate privacy and combat online abuse, and her

legal scholarship has been cited in state and federal court decisions, federal regulations, and White House reports. She has testified before multiple Congressional committees—on deepfakes, artificial intelligence, and how to define "reasonable" content moderation practices—as well as before the House of Commons in the UK. She has served as an adviser to the White House's Gender Policy Council during the Biden administration and to then-California Attorney General Kamala Harris' Task Force to Combat Cyber Exploitation and Violence Against Women. Over the years, she has been an advisor to companies such as Twitter, Facebook, TikTok, Twitch, Bumble and Spotify, among others, on safety and trust issues.

Danielle Citron has also achieved the recognition of being ranked first amongst the Top 100 Law Scholars, an indicator of scholarly influence, and is the first woman to appear at the top of that list.

Ryan Calo, Lane Powell & D. Wayne Gittinger Professor of Law at the University of Washington School of Law, and her frequent co-author, said: "It is hard to overstate Danielle Citron's contributions to the field of law and technology. Her work on internet hate crime, automated decision-making, and privacy has inspired generations upon generations of academics, students, and practitioners. I am in constant awe of Danielle and honored to call her my dearest friend and co-author."

"Danielle is an extraordinary human, always eager to mentor, to bring people together, to support junior scholars, to lift her colleagues, and celebrate the achievements of her students," said Ari Ezra Waldman, Professor of Law at the University of California, Irvine, and another Citron co-author. "Danielle's teaching is also second to none."

Woodrow Hartzog, Professor of Law and Class of 1960 Scholar at the Boston University School of Law, said: "No one in our field has had such a deep impact across so many areas and in so many ways as Danielle Citron. Simply put, she's the GOAT [greatest of all time]. ... This is to say nothing of how great of a colleague, teacher, mentor, and friend she is. I honestly don't know when she sleeps. But what I do know is that we are all better because of her efforts and are so fortunate to have her as such an exceptional leader in our field."

To the benefit of many, Danielle Citron has long been, and remains, a privacy optimist. Never failing to spot how laws that protect intimate privacy can be improved, she maintains that privacy "can and should be ours." We will continue to be amazed by her fight for privacy, which remains fierce.

Peter Hustinx

The office of the European Data Protection Supervisor has grown in size and influence since its creation in 2001. Each appointed supervisor has left their own mark on the office, but the initial move to prominence came courtesy of Peter Hustinx.

Hustinx was appointed the inaugural EDPS in 2004. The role primarily positioned him to lead the supervision of EU institutions' data protection compliance. It also included advisory responsibilities, supporting member state data protection authorities while counseling the European Commission and European Parliament on data protection legislation.

"I saw the opportunity and wanted to be part of that," Hustinx said in a 2012 interview with Politico. He added that the first of his two five-year EDPS terms was dedicated to "making sure there was an authority that existed."

Hustinx was arguably the right man at the right time to cultivate legitimacy and expertise at the EDPS office. He had a prior track record as a data protection regulator, running the Netherlands' data protection authority, the Autoriteit Persoonsgegevens, for 14 years prior to the EDPS appointment. He also chaired the Article 29 Data Protection Working Party, the predecessor group to the European Data Protection Board.

"He's taken a two-man body, which is what it was when it started in 2004, and he's turned it into a real data protection authority, which you can put side-by-side with any of the national ones," former EDPS Director Chris Docksey told the IAPP in a 2013 interview.

During his decade-long run as EDPS, Hustinx tackled issues that helped shape and define the current EU data protection landscape. Most of that work was focused on ensuring regulation and standards remained relevant. For example, his office issued opinions seeking modernization or repeal of key EU data protection standards, including the Data Retention Directive and the EU-U.S. Passenger Name Record.

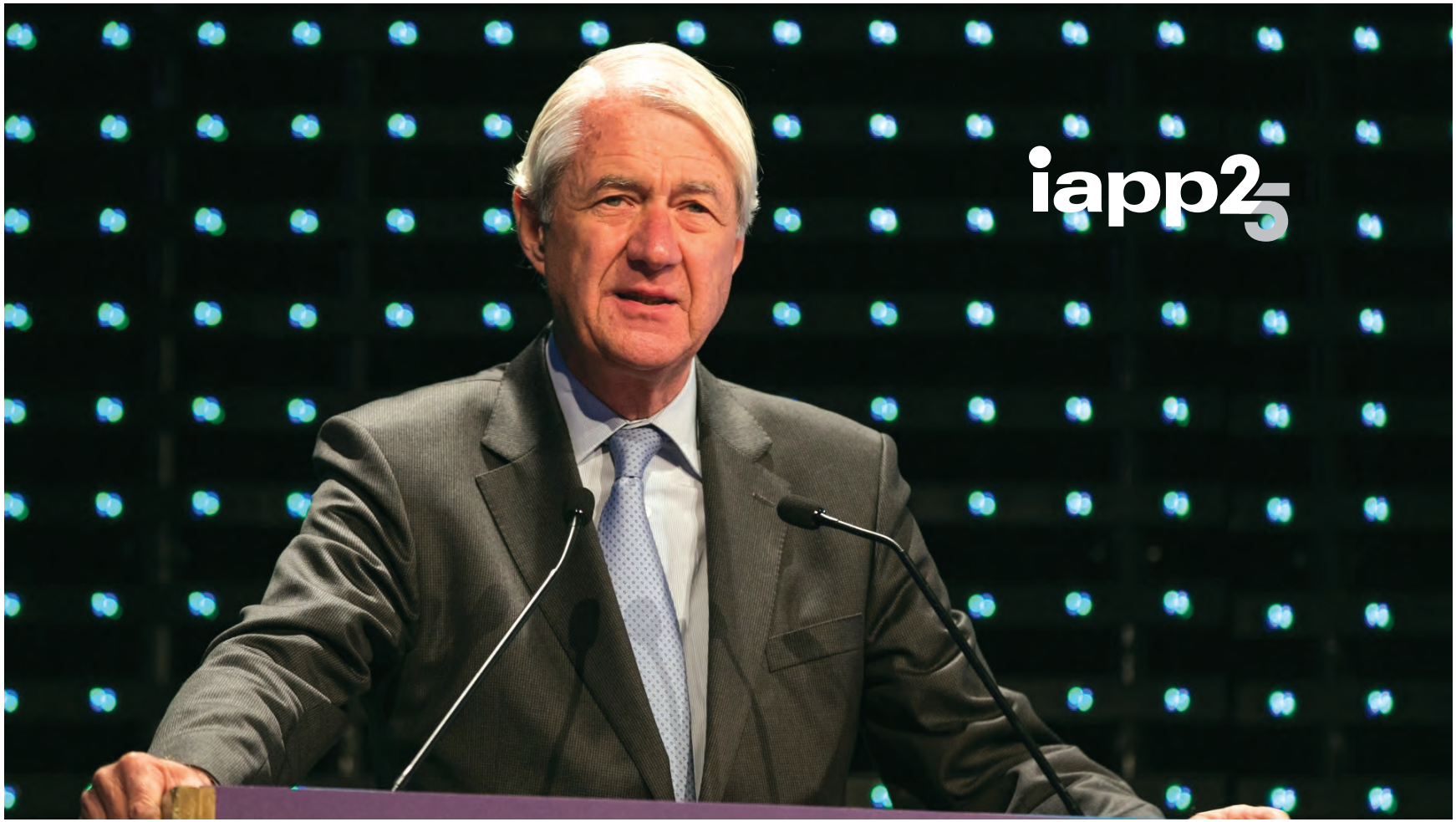
During his decade-long run as EDPS, Hustinx tackled issues that helped shape and define the current EU data protection landscape.

The interplay between data protection and national security was another area Hustinx keyed in on. He offered input toward EU security policies following several global terrorist attacks in the early 2000s and helped broker the 2007 deal to allow the U.S. to access banking data from the Society for Worldwide Interbank Financial Telecommunication's system for the purpose of tracking terrorists' banking activities.

"His positions always took account of all the other interests and yet at the same time, significantly advanced data protection," former Irish Data Protection Commissioner Billy Hawkes told the IAPP in 2013. "He was always able to offer a strong opinion, which people respected, as to what the right course of action might be with a particular item on the table."

For his efforts to better protect citizens' data, the Confederation of European Data Protection Organizations awarded Hustinx with the first European Data Protection Award in 2013, and the Electronic Privacy Information Center granted him the 2015 International Champion of Freedom Award.

Hustinx joined the IAPP Board of Directors in 2015, just ahead of the passage of the EU General Data Protection Regulation in 2016 and the beginning of the IAPP's most transformative years. At the time, IAPP President and CEO J. Trevor Hughes, CIPP, called Hustinx's body of work "invaluable" as it "set the tone for global privacy regulation across sectors and organizations."


iapp25

Nicole Wong

It is not uncommon to see Silicon Valley's best policy professionals make the jump from industry to civil service. Nicole Wong's decades of work to formulate privacy and digital governance policy principles exemplify the type of impact that can be made in the private and public sectors.

Wong has held some of the most influential positions a digital professional could have. Her industry resume includes a stint as vice president and deputy general counsel at Google, legal director at the then-named Twitter, and a partner at Perkins Coie. Those roles led to her appointment as U.S. deputy chief technology officer in the Obama administration, helping guide internet policy initiatives on innovation and privacy.

Dictating policy decisions for a run-of-the-mill company is one thing, but Wong's role at Google in particular left her setting policy for the internet and its global users.

The seriousness of her role was reflected in 2007 as she and her Google colleagues worked to address online speech concerns raised by the Turkish government stemming from illicit YouTube content. Wong opted to weed out illegal content through IP address blocking in Turkey while also considering where its own policies around free speech and hate speech needed to be applied.

According to a 2008 profile in The New York Times Magazine, work on such tasks earned Wong the title of "The Decider" among her colleagues.

"Wong and her colleagues arguably have more influence over the contours of online expression than anyone else on the planet," legal scholar Jeffrey Rosen wrote in the NYT Magazine piece. She framed her role a little differently, telling Rosen, "I definitely am not trying to pass judgment on anything. I'm taking my best guess at what will allow our products to move forward in a country, and that's not a judge role, more an enabling role."

Wong spent nearly nine years between Google and X before U.S. President Barack Obama tapped her for the deputy CTO role within the Office of Science and Technology Policy.

The private-sector perspective proved particularly valuable in Wong's contribution to the White House's 2014 study, "Big Data: Seizing Opportunities, Preserving Values."

The 90-day study examined big data's potential to transform everyday life and the future of work, as well as how it might change the connections between government, citizens, businesses and consumers.

In a 2021 interview with the IAPP, Wong said the "most common and urgent message" stemming from the study was a "profound asymmetry of power between individuals and the companies that collected and used their data."

"When you asked people what they were most concerned about, sometimes they talked about privacy, like concerns about identity theft or government or corporate surveillance. But often they talked about being worried about being overlooked or denied opportunities because of information about them," she said. "The distinction between data privacy and data fairness raised important questions about whether we have the right frameworks and the right policy tools when it comes to data governance."

The study shed light on themes that remain pertinent to digital governance conversations, including privacy and artificial intelligence. It also generated recommendations from Wong and OSTP colleagues that supported more conversations on a federal U.S. privacy law, more attention to the privacy implications of education technology, and improved technical expertise at consumer protection and civil rights agencies to address emerging discriminatory practices.

Wong left her government position after a year and has since taken on advisory roles. In addition to running her own consultancy service for 12 years, she currently serves as board chair for Mozilla Foundation and as a board member for CalMatters and Open Technology Fund.

The IAPP awarded Wong its 2021 Privacy Leadership Award, recognizing her "ongoing commitment to furthering privacy policy, promoting recognition of privacy issues and advancing the growth and visibility of the privacy profession."

LEADERS

MOMENTS

Birth of the IAPP

"In the heady days of the dot-com boom, a new profession was born. The emergence of the Internet and new privacy regulation in Europe and North America by the late 1990s had ushered into the executive suite a new arrival: the chief privacy officer."

Though different organizations back then used different titles, "those chosen for this new leadership role quicky sought one another out."

In 2010, the IAPP celebrated its 10th anniversary by, among other things, publishing its first white paper "A Call for Agility: The Next-Generation Privacy Professional" and used the words above to describe the early moments for what is now the world's largest organization for privacy, AI governance and digital responsibility professionals.

"The IAPP soon became the focal point for fostering the support and growth of the nascent privacy profession," the white paper notes. "Through its conferences and Certified Information Privacy Professional credentials, the IAPP gave structure to this new discipline."

But of course, the formation of the IAPP was the result of multiple threads that came together through a deep history that included the emergence of digital technology and the internet, increased law and regulation and the need for businesses to respond to both.

As more business professionals were asked to take the lead in this emerging space, "more formal communities began to develop," J. Trevor Hughes, CIPP, and Andrew Clearwater, AIGP, CIPP/E, CIPP/US, CIPM, FIP, wrote in a 2014 Ohio State Law Journal article on the history of the privacy profession. There were initially two professional groups that developed to meet this need: the Privacy Officers Association and the Association of Corporate Privacy Officers.

Launched in 2000, the POA was created by Davis Wright Tremaine Partner Peter Grant and Brent Saunders, who worked as a consultant at what was then called PricewaterhouseCoopers and would eventually become CEO of Johnson & Johnson. The POA "focused on conferences and providing relevant privacy news and updates."

At the outset, 12 early leaders were selected as members of the POA's initial board, including Harriet Pearson, CIPP/US, Richard Purcell and Agnes Bundy Scanlan, CIPP/US. They decided to hire an association management company to run the organization and launched the Privacy Officers Advisor, which would eventually morph into the IAPP's first regular publication.

The ACPO "was a very small group" also created in 2000 "with a few handfuls of members led by Alan Westin," the law review article states. "Membership was so minimal in those early years that, when Bundy Scanlan spoke at one of their first conferences, 'there was a pillar in the middle of the room, and it didn't matter because the room wasn't big enough for there to be people behind it — there was no back of the room.'"

It soon became clear — with "many overlapping members and board leaders" — that a union of the two associations would make sense. By 2001, the new, unified group was called the International Association of Privacy Officers, and the first Privacy and Data Protection Summit was held in Arlington, Virginia. Some of the field's early leaders spoke at the event, including Peter Swire, CIPP/US, Bob Belair, Alan Westin, Jim Koenig, Bundy Scanlan and Barbara Wellbery, among others.

In a 2013 IAPP obituary for Westin referring to his work with the ACPO, Pearson said that "Westin early on understood the value of bringing together a community of people to work on privacy issues, whether it was from business, government or advocacy groups, and some of that early work he did bringing groups together really inspired the formation of the International Association of Privacy Professionals."

By the summer of 2002 — the year the IAPO would hire Hughes as its first executive — membership had "swelled to 150-200 members" and by early 2003, the IAPO updated its name to the now-familiar IAPP.

After the name change, Bundy Scanlan said that "as privacy professionals, we have many roles and responsibilities" and "safeguarding privacy is a team effort."

As Hughes and Clearwater pointed out, "Although still small, the groundwork had been laid for a broad and deep professional field."

MOMENTS

Launch of the IAPP Global Summit

It was 1999 and U.S. Congress had just passed the Gramm-Leach-Bliley Act.

The law, formally known as the Financial Services Modernization Act of 1999, changed how banks, securities and insurance companies operate by requiring them to explain how they share information and protect sensitive data. Agnes Bundy Scanlan, CIPP/US, then a compliance and chief privacy officer for Bank of America, said the industry's whisper network was struggling to figure out how to comply with the law.

A year later, what is now known as the IAPP was founded, and an early point of order was how to address the Gramm-Leach-Bliley Act. In a tiny conference room in Crystal City, Virginia, a small group of regulators, privacy folks and financial compliance leaders gathered for a one-day event — the first ever Global Privacy Summit.

Today, the event draws thousands of people in the privacy, artificial intelligence and cybersecurity fields to Washington, D.C., each spring. A four-day event with trainings, workshops and multiple keynote speakers, attendees have direct access to regulators from around the world and a place to comingle and network. Other organizations stand up their own conferences and events on surrounding and overlapping days to catch some of the action.

J. Trevor Hughes, CEO and president of the IAPP, said the first Summit was quite different.

"I cannot remember if there were even 200 attendees at the first Summit, but I do know that most of our breakout sessions now are larger than the entire conference back then," Hughes, CIPP, said.

Scanlan, the first chair of the IAPP, thinks the group may have been even smaller, less than 100. But the speakers were impressive: foundational privacy scholar Alan Westin, as well as a member of the Federal Trade Commission. At the end of the day, people walked away with hand-written lists of phone numbers and emails to get in touch.

Subsequent events would grow bigger and more organized. But Scanlan said even that first event showed the concept of Summit had promise.

"We in the financial services world were always talking to each other, but we as practitioners did not have a place to get together," she said.

"That first gathering, it was really just to get together — and talk about this damn law, and how to comply with it."

In a tiny conference room in Crystal City, Virginia, a small group of regulators, privacy folks and financial compliance leaders gathered for a one-day event — the first ever Global Privacy Summit.

MOMENTS

The "tech effect"

Since the IAPP's inception in 2000, the internet has increasingly become part of everyday life. In the first decade alone, internet users grew from 390 million to 1.9 billion in 2009. By 2010, approximately 30% of the global population, which numbered just under 7 billion people, were online, with 21% of those users in the developing world and 67% in the developed world. By 2023, an astounding 67% of the global population was online.

Add to this rapid growth, the improved ability to share files, exponential processing ability via Moore's law, the rise of the web browser, the increased ease of online search and the economic incentive to advertise through this growing generative network. It's easy to understand why there was a need for privacy protections for individuals and the corresponding growth of the privacy profession.

By 2010, popular use of the personal computer morphed into the convenience and mobility of the smartphone. In January 2007, after nearly three years of top-secret development, Apple CEO Steve Jobs unveiled the iPhone, and in its wake, the "app economy" was born. Google jumped into the game as well with its introduction of the Android a year later, which is the world's most used operating system as of October 2024.

Online social engagement also underwent a revolution. Early platforms like MySpace and Friendster gave way to Facebook, Twitter and YouTube. By 2023, nearly 5 billion people — almost 60% of the world's population — used some form of social media.

Big tech companies began experimenting with novel forms of social networking, data collection and online advertising, which led to privacy incidents, including those involving Google Buzz and Street View, Facebook Beacon, and others. The "Do Not Track" policy debate over web tracking came to fruition and has not yet been resolved.

Business flourished with new opportunities to advertise and collect data about their customers. Yet, governments — from California and Canada to Cape Verde and Japan — responded as well. New privacy laws started emerging in the early 2000s, building on the 90s-era of privacy laws, including the EU Data Protection Directive and a host of sectoral laws in the U.S.

And on the ground, professionals were being tasked with helping to manage novel privacy issues in addition to their full-time positions. For the IAPP, this proliferation of the internet, mobile phones, online advertising and social networking — this "tech effect" — meant the mission of defining, supporting and improving the profession of privacy became more important.

Online social engagement also underwent a revolution. Early platforms like MySpace and Friendster gave way to Facebook, Twitter and YouTube. By 2023, nearly 5 billion people — almost 60% of the world's population — used some form of social media.

MOMENTS

Launch of IAPP Publications

In 2001, the Privacy Officers Association — that's what the IAPP was called back then — launched a monthly print magazine called The Privacy Officers Advisor. Complete with featured stories on the latest issues challenging privacy professionals at the time, including EU-U.S. data relationships, California's role in the legal space, workplace litigation, data breaches and more (sound familiar?), the POA was among the first publications to focus directly on privacy.

"This publication, in the early days of the organization, was the primary means of communicating with the small but growing membership on the wide variety of new developments," said Wilmer Hale's Kirk Nahra, CIPP/US. Nahra was the publication's first lead editor.

Though Nahra did not start the publication, he had been a frequent writer "from the first days." Once the opportunity to become the editor emerged, he took it and then spent more than 15 years in the role, witnessing the organization's "massive development" first-hand.

"I worked with a very small internal staff — to both do some overall editing and to identify topics and writers on the various issues," he explained. "For the first several years I was a very hands-on editor — then over time it became more staff driven."

By September 2005, the POA was renamed The Privacy Advisor and managed by a small team.

"The members loved it," Nahra recalls. "At the time, it was the best way in the industry to keep an eye on all the major developments. There were some news organizations doing real-time news developments, but this was the main place for people's thinking and analysis about the important issues that were developing."

As with now, the IAPP relied, in large part, on its member contributors to share best practice and analysis on significant issues developing on the ground. In the early days, Nahra recalls, it "went very quickly from having to beg for articles to being overwhelmed with submissions.

"It also became — in my opinion — a critical place for building the community," Nahra said. "You knew who was working on these issues and who to pay attention to in the space."

With The Privacy Advisor in full swing, members received in-depth monthly analyses, but when J. Trevor Hughes, CIPP, took the helm, he realized members also needed timely news updates. Though email newsletters were in relative infancy at the time, Hughes reached out to well-known privacy attorney Reed Freeman, who had organized a news-driven email client alert, which was sent to a few hundred recipients and generally featured two to three news "blurbs" with each send.

Hughes asked Freeman if he could repurpose the newsletter for the IAPP, and he agreed. That's when the IAPP Daily Dashboard was born.

The birth of the Daily Dashboard crucially allowed the IAPP to also share organizational news about its conferences, certification, training and KnowledgeNets, and its delivery continues to this day.

For more than 20 years, the Daily Dashboard has hit members' inboxes Monday through Friday with the latest privacy — and now artificial intelligence governance, cybersecurity and digital responsibility — news developments. It goes out to more than 75,000 inboxes and serves up the latest news, contributed analysis, op-eds and in-depth research from the IAPP's Research and Insights team.

Over the years, the IAPP also rolled out regional digests for Canada, Europe, the Asia-Pacific region and the U.S., as well as an all-Spanish Latin American Dashboard Digest. It sends a monthly Career Central Digest to share job openings with members, and most recently, the IAPP launched a weekly AI Governance Dashboard dedicated to regulatory, legal, business and technology updates for this burgeoning field.

Though The Privacy Advisor, which went electronic-only in 2010, was retired in 2022, the IAPP continues to publish in-house, contributed and third-party news, analysis and research through its email newsletters each day.


THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp
Why are more companies joining the U.S. - EU Safe Harbor privacy framework?
California's model approach to privacy
The SWIFT Case: Europe's Decisive Confirmation of its Fundamental Data Protection Principles
Reforming Australian privacy laws
Privacy and Security Litigation in 2006: Is the Tide Turning?
Privacy Officers ADVISOR
Privacy Success: The CPO Can't Do It Alone
First Salary Survey Shows Variations According to Industry, Experience, and Organization
Workplace Privacy: Steps Your Company Can Take to Reduce the Risk of Litigation
Customs and cross-border dat
Notes From the Executive Director
Flexes Muscles at Winter Conference

MOMENTS

European Data Protection Supervisor

As data protection concerns continue to grow, the European Data Protection Supervisor remains a crucial regulator in the digital landscape.

From contributing to the drafting and enforcement of the EU General Data Protection Regulation to issuing opinions on international data flows, the EDPS has helped define the European Union's identity as a leader in privacy.

The EDPS position was originally created in 2001 to serve as a supportive, trusted advisor for EU institutions, bodies, offices, and agencies to "help them be exemplary" and provide guidance on complying with data protection regulations. The EDPS also acts as an advisor to member states' data protection authorities and provides guidance to the European Parliament, the Council, and European Commission on data protection legislation.

The role was officially established in 2004 when Peter Hustinx was appointed as EDPS where he completed two five-year terms. As EDPS, Hustinx shaped the authority from a regulatory body tasked with supervising EU institutions to a key voice in global debates over how data should be collected, processed and protected.

Former EDPS Director Chris Docksey previously told the IAPP Hustinx's efforts took the EDPS from a two-man body in 2004, to a "real data protection authority, which you can put side-by-side with any of the national ones."

After Hustinx's terms ended, the European Parliament and Council appointed previous EDPS Assistant Supervisor Giovanni Buttarelli in 2014. During his term as EDPS, Buttarelli urged organizations to prioritize privacy and digital security.

In his five-year strategy released in 2015, Buttarelli aimed to promote innovation without sacrificing consumer security and ensure organizations remained transparent about their data processing practices.

Buttarelli also looked to shape the EDPS into a more collaborative body by forming international partnerships and solidifying the regulators' role as the "single EU voice in the international arena."

Buttarelli was awarded the IAPP's 2019 Privacy Leadership Award for his "ongoing commitment to furthering privacy policy, promoting recognition of privacy issues and advancing the growth and visibility of the privacy profession."

The EDPS has continued to prioritize building strong partnerships with international regulators through active participation in global bodies such as the Global Privacy Assembly. Buttarelli's contributions helped to create common standards that emphasize both individual rights and accountability in digital ecosystems.

The EDPS also has an active advisory role in new digital laws such as the Data Governance Act through having representation on the European Data Innovation Board, which advises and assists the Commission on various issues like standardization, portability, interoperability, as well as representation on the High Level Group for the Digital Markets Act, which advises the Commission on implementation, enforcement and consistency. It also has a primary role in monitoring application of the Data Act insofar as it concerns the Commission, the European Central Bank or other Union bodies.

Former EDPS Assistant Wojciech Wiewiórowski currently serves as EDPS after he was appointed to lead the authority in 2019. Wiewiórowski has issued extensive guidance on targeted advertising and consumer concerns, urging the EU to bolster data protection regulations to prevent companies from potentially harmful practices.

The European Parliament and Council are currently at a standstill in their decision to either elect a new EDPS or re-appoint Wiewiórowski to serve another term. As the next EDPS has yet to be decided, a new leader will need to move the office forward to meet the complex regulatory challenges of the EU's evolving digital market.

MOMENTS

First IAPP certification

In late October 2004, the IAPP hosted the Privacy and Data Security Academy and Expo in New Orleans. In addition to platforming a range of privacy professionals from across technology, health care and law, the conference was also the inaugural testing site for the IAPP's first certification offering, the Certified Information Privacy Professional.

"The privacy community was much smaller 21 years ago," said ArentFox Schiff Partner Reed Freeman, CIPP/US, one of the keynote speakers in New Orleans. "At the time, privacy law in the United States was largely driven by the FTC and its Section 5 authority to police unfair and deceptive acts and practices; this was long before the California Consumer Privacy Act and other state laws."

Developed in coordination with groups from Carnegie Mellon University and the Ponemon Institute, and made available through grants provided by Hewlett Packard and Microsoft, the CIPP certification was billed as "the first-ever, broad-based privacy certification in the United States."

"We hosted 150 lucky trial registrants for that first exam, a two-hour, 120-item objective test that was drafted entirely by Larry Ponemon," said Peter Kosmala, course developer and instructor at York University and former IAPP vice president. "Without the early participation of these examinees — whom we can legitimately regard as 'pioneers' for this effort — we wouldn't have the program that eventually developed and matured to what it is today."

Since 2004, nearly 100,000 IAPP certifications have been awarded, with more than 60,000 currently active. Testing is offered at more than 6,000 locations around the world in four languages.

The CIPP designation has become an umbrella for five different certifications, each concentrated on specific jurisdictions: CIPP/US, CIPP/E, CIPP/A, CIPP/C and CIPP/CN, focused on the U.S. private-sector, Europe, Asia, Canada and China, respectively. A sixth CIPP concentration, CIPP/IT, was renamed to Certified Information Privacy Technologist in 2014, and a seventh, CIPP/G, focused on U.S. public-sector privacy, was retired in 2018.

Twenty-one years later, the CIPP certification has become one of the most popular and sought-after privacy certifications in the industry and its development marks an important milestone for IAPP's mission and reputational growth. Since 2004, nearly 100,000 IAPP certifications have been awarded, with more than 60,000 currently active. Testing is offered at more than 6,000 locations around the world in four languages.

Previous IAPP research has demonstrated the value of IAPP certification for privacy, artificial intelligence governance and digital responsibility professionals. The IAPP Salary and Jobs Report 2025-26 found that professionals with at least one IAPP certification earn, on average, 4% more than those without an IAPP certification. Additionally, respondents that hold any designation of the CIPP certification alongside the Certified Information Privacy Manager certification earn 63% more than those without any IAPP certifications, suggesting the strength and importance of a CIPP certification.

"Pulling together the first CIPP exam was a huge effort for the IAPP, and it has paid off handsomely as a key indicator of expertise in the field," Freeman said.


iapp
CERTIFICATION
FOUNDATION
Companion Course Book for the
Foundation Training Workshop
CIPP
iapp
iapp25

MOMENTS

The "data breach effect"

At the turn of the century as more business was conducted online, the risk and breadth of data breaches grew exponentially. Though data breaches have been around for as long as data has been collected, it wasn't until the early 2000s that the "massive" data breach rose at scale.

For example, in 2004, an employee of America Online "used his inside knowledge of AOL's computer system to steal a list of 92 million AOL customer account 'screen names'" and then sold them to a third party. At the time, AOL was the world's largest internet service provider.

In 2006, data broker ChoicePoint ended up paying USD15 million to settle charges that it failed to protect its customers' personal data. At the time, the settlement was the largest civil penalty over data security in the history of the U.S. Federal Trade Commission. The incident took place when criminals stole personal data belonging to 145,000 customers. According to NBC News, "In all, there were some 25 major disclosures, with information on 52 million individuals exposed. ... The ChoicePoint disclosure was significant not only for its scale, but for the light it shed on the growing data broker industry."

Other early but significant data breaches involved retailers T.J. Maxx and Marshalls after it was discovered hackers "stole data from at least 45.7 million credit and debit cards of shoppers." The breach was discovered in 2007, though it was believed hackers had been siphoning customer data for more than a year. The adversaries installed "WiFi sniffers" to capture data sent over the network, including credit and debit card numbers, expiration dates and CVV codes.

The incident led to questions about the data security practices of retailers and the harm it can cause consumers.

A key group for helping consumers understand their privacy rights was the Privacy Rights Clearinghouse, which was originally founded by Beth Givens in 1992 "to help people understand their rights and choices." The Identity Theft Resource Center, established in 1999, provided victims of data breaches with assistance and education.

Data breaches were not only proliferating in the private space but also hit government agencies. In 2006, the U.S. Department of Veteran Affairs was hit by a massive data breach involving 26.5 million military veterans. The data, which included Social Security numbers and birthdates, was stolen from a VA worker who had taken the information without authorization. At the time, according to Privacy Rights Clearinghouse, the breach was one of the "biggest of the computer age."

Though the 1995 European Data Protection Directive contained provisions that emphasized the importance of data security, it was not until 2002 that a data breach notification law was passed. California led the way with SB 1386, which became operative in 2003. Since then, all 50 U.S. states and U.S. territories passed a data breach notification law. Though there is not a federal data breach notification law in the U.S., some federal laws require it in specific circumstances, including the Federal Trade Commission Act, the Financial Services Modernization Act and the Health Insurance Portability and Accountability Act.

Other nations have data breach notification laws of their own. Passed in 2016, the EU General Data Protection Regulation requires a comprehensive data breach notification response with a strict timeline and other countries around the world now also require notification, including Australia, China, Japan and New Zealand.

The IAPP Resource Center features an "Incident and Breach Management" topic page to help members find news, resources, tools and insights into cyber incidents and data breaches, with guidance on how best to respond as an organization or individual after being impacted by a breach. The IAPP also features a "State Data Breach Notification Chart" to assist practitioners.

MOMENTS

IAPP Information Privacy book first published

The privacy profession has grown leaps and bounds over decades thanks to the proliferation of legal requirements around personal data and the dedication of compliance professionals to meet those standards.

Effective compliance practices stem from certification and training. And any coursework requires a foundational body of knowledge.

For privacy professionals, that compendium was the IAPP's first official textbook for the Certified Information Privacy Professional. "Information Privacy" first published in 2005, helping privacy pros learn the standards that would define the profession while creating the roots for subsequent IAPP jurisdictional certification textbooks in the years after.

Former IAPP Vice President Peter Kosmala, now a course developer and instructor at York University in Toronto, was tasked with overseeing publication of the book after helping erect the IAPP certification program. He recalled the first certification exam at an IAPP Privacy Academy event in New Orleans in 2004, noting the participants went into the exam "blind" and their post-exam feedback focused on needing more details around exam questions.

"The book was, on the one hand, something that was the official reference to the exam, but also really became sort of the bible for the practice of privacy," Kosmala said. "It was an attempt to sort of define the discipline at the same time as professionalizing the community."

After settling on an advisory board to guide the textbook's creation, the next step was finding authors. With the academic nature of the project, Peter Swire and Sol Berman were tapped to draft the contents of the book.

Swire described the task as building "from scratch, with numerous topics and little to go on."

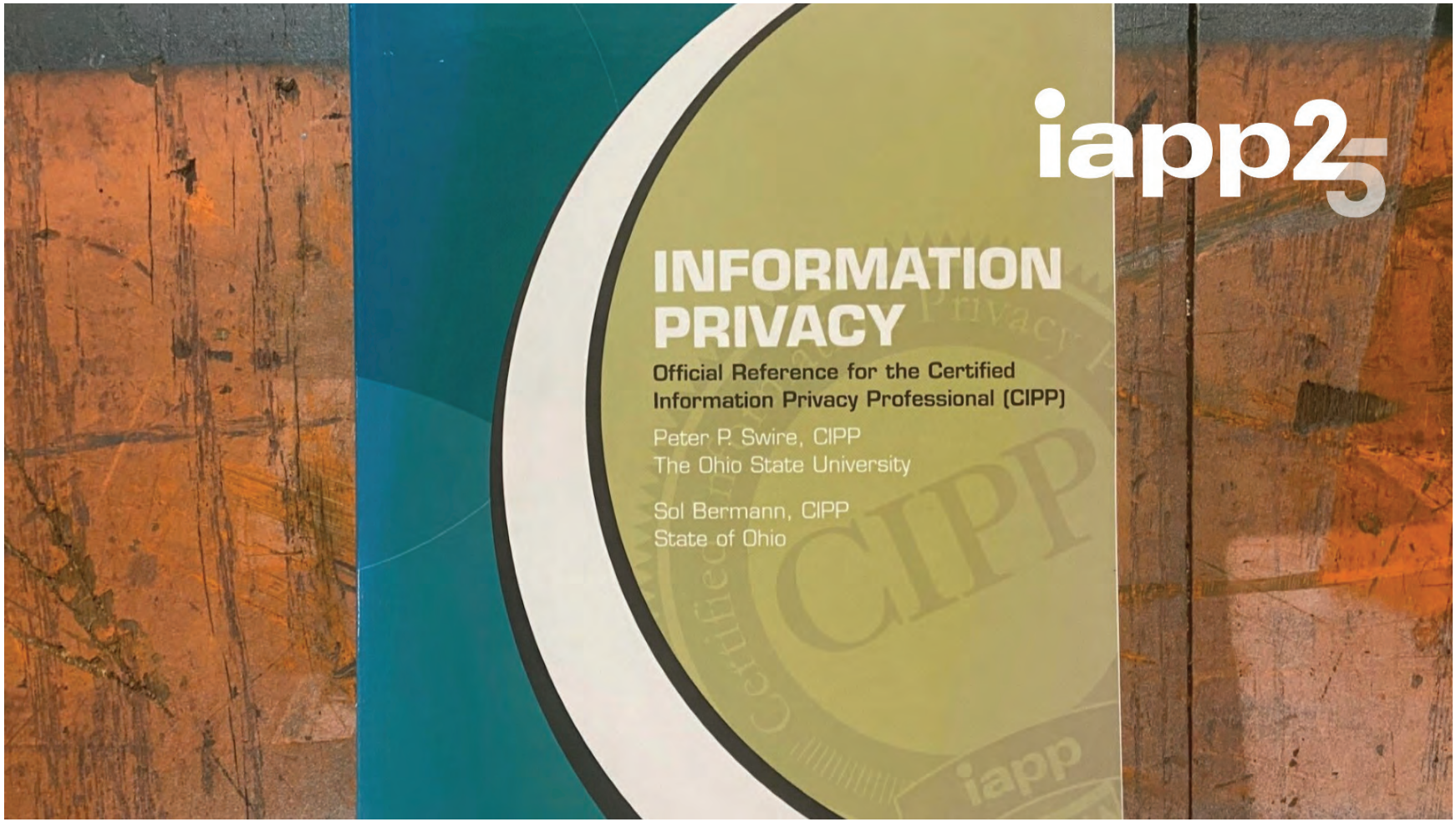
"Our goal was to write a book that would work for all sorts of people, from lawyers to technologists to marketing experts," he said. "That remains an important IAPP goal today, to create a big tent for people with different backgrounds."

What Swire and Berman generated was a refined view balancing core privacy principles and legal interpretation of that time. The book's domains included privacy law and compliance, information security, web privacy and security, data sharing and transfers, and employee privacy.

Swire said the tone of the book was aimed at a middle ground for privacy debates between advocates, industry and law enforcement.

"Our textbook tried to show the value of both perspectives, so that personal data would be governed thoughtfully," Swire said. "Many privacy professionals benefit from a nuanced appreciation for examining which data uses make sense, or don't, for your organization and for the broader society."

"Our goal was to write a book that would work for all sorts of people, from lawyers to technologists to marketing experts. That remains an important IAPP goal today, to create a big tent for people with different backgrounds."


iapp25
INFORMATION PRIVACY
Official Reference for the Certified Information Privacy Professional (CIPP)
Peter P. Swire, CIPP
The Ohio State University
Sol Bermann, CIPP
State of Ohio
CIPP
iapp

MOMENTS

Launch of IAPP Canada

The IAPP's global ties are evident through a growing and diverse membership as well as its operations in different parts of the world. While headquartered in Portsmouth, New Hampshire, the company has established a presence on the ground in several jurisdictions, including Canada.

The IAPP Canada commenced its work in March 2009 under the direction of Kris Klein, CIPP/C, CIPM, FIP, who remains director to this day. It was spurred by the successful launches of the Certified Information Privacy Professional/Canada certification in 2006 and early IAPP events in "The Great White North," including the Canada Privacy Symposium event in 2008.

Klein recalled the concept for IAPP Canada stemmed from a conversation with IAPP President and CEO J. Trevor Hughes, CIPP — a fellow Canadian — at a 2007 IAPP Privacy Academy event in San Francisco.

"Looking back, it seems obvious the IAPP would expand into Canada," Klein said. "The demand was there, privacy in Canada was only becoming more complex and important, and we were home to some of the world's early global leaders in privacy."

At the time of launch, Canada already had established privacy laws from years and decades prior, including the Personal Information Protection and Electronic Documents Act at the federal level. And the country, indeed, played home to privacy community stalwarts like Ann Cavoukian, Ph.D., Elizabeth Denham CBE, Michael Geist, Ian Kerr, Jennifer Stoddart and more.

"Looking back, it seems obvious the IAPP would expand into Canada," Klein said. "The demand was there, privacy in Canada was only becoming more complex and important, and we were home to some of the world's early global leaders in privacy."

IAPP Canada's buildup required more than a simple idea between friends. Like any new initiative, it took groundwork to secure support.

"One moment was a cross-country tour in the early days, when Trevor and I did something like seven KnowledgeNets in seven days," Klein said. "From British Columbia to Quebec, and with plenty of stops in between. The turnout, the energy and the depth of the discussions made it pretty clear that privacy professionals across Canada wanted and needed a community like this."

Sixteen years later, the IAPP Canada remains a guiding light for an ever-growing community, which now includes those trying to navigate artificial intelligence governance and other digital responsibility fields.

The peer-to-peer opportunities raised through IAPP Canada, particularly at CPS, remain as valuable as certification and training, according to Klein. He added the bridge between professionals and Canada's federal and provincial privacy commissioners is another area that would not be as strong without the communal atmosphere cultivated by the IAPP.

"IAPP Canada's role wasn't just about training. It was about creating a real and strong professional community," Klein said. "It has created a space for Canadian privacy professionals to connect, learn from each other and even influence the path forward on a myriad of privacy issues on a global stage."

MOMENTS

Launch of IAPP ANZ

The IAPP has spent the last 25 years growing its reach to nearly every corner of the world. Most need look no further than the EU and the U.S. to understand the impacts, given how regulatory regimes spawned a proliferation of compliance professionals in each jurisdiction.

But some of the IAPP's other regional touch points, including Australia and New Zealand, make an even more compelling case for how far the organization and the broader privacy community have come.

ANZ's privacy roots reach back to the creation of the iappANZ in September 2008. The volunteer-based association was an affiliate of the IAPP, running its own programming and strategy geared specifically to support the work of professionals in the region.

Former Australian Privacy Commissioner Malcolm Crompton, CIPP/US, founded the iappANZ and served as its first president. Other founding officers included Kevin Shaw, Annelies Moens, CIPP/E, CIPT, FIP, David Templeton and Philip Youngman, while the first iappANZ Board included 18 members.

According to Crompton, iappANZ was born in the same way as the IAPP: At a privacy conference. He said the practitioner sessions at the International Conference of Data Protection and Privacy Commissioners in 2003 started turning the gears before recurring informal practitioner meetings in 2006 created the real momentum.

"In order to ensure that the events only continued if there was sufficient interest, at the end of every event, I asked attendees 'shall we meet again?' and people continued to want to meet," Crompton said in a 2018 interview with the iappANZ's newsletter, Privacy Unbound.

The iappANZ began its programming August 2008 with its inaugural ANZ Summit. The first networking meeting was held March 2009 in Brisbane. Crompton said the association's peak for events came in 2017 and 2018 as it tried to gather professionals to prepare for the global impacts of the EU General Data Protection Regulation.

The iappANZ wound down its singular operations in December 2018 and joined the broader IAPP endeavor. Crompton said iappANZ's 10-year standalone run was a product of "absolute commitment and passion of the individuals involved in the board."

"I've been so fortunate to have the counsel, encouragement, and feedback of the iappANZ foundational members during my time leading the IAPP work in the ANZ region," IAPP Managing Director, Australia and New Zealand, Adam Ford said. "The work that this group of volunteers put into the structure and operations of the organization is now enabling us to uplift and support our members across the region during these critical periods of regulatory and policy reform."

Upon assuming operations in the region, the IAPP built on the iappANZ's foundations.

In the first year after the merge, IAPP-certified ANZ individuals with IAPP certification doubled to 224 and the number of members in the region went from 685 to 1,125. Today, the ANZ region boasts 695 certified individuals and 1,960 members.

Stephen Bollinger, AIGP, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP, former IAPP Country Leader for Australia, said the "amazing resources and community" helped spur membership and certification spikes. Understanding community needs was also key, as Bollinger noted there was a concerted effort to establish more KnowledgeNet chapters across the region. The IAPP now has KnowledgeNets for Adelaide, Sydney, Brisbane/Gold Coast, Melbourne, Perth, Auckland and Wellington.

"The iappANZ, and then the IAPP, provided the ANZ privacy profession with an identity that it lacked before," said IAPP Country Leader for New Zealand Daimhin Warner, CIPP/E, who first participated in iappANZ in 2014. "The professional friendships I made during the early years have lasted until today, and there is a regional collegiality in New Zealand and Australia that I am not sure exists to quite the same degree anywhere else."

MOMENTS

The "Brussels effect"

A term coined by Professor Anu Bradford, the Brussels effect describes how the EU became a global regulatory power through its "market size, regulatory capabilities, stringent regulations, inelastic targets, and non-divisibility" and significantly guided the behaviors of corporations subject to its regulations.

As perhaps the best example of this, and one Bradford describes in her book, is the EU General Data Protection Regulation, which went into effect 25 May 2018. This extensive data privacy regulation would quickly become the international standard for how data controllers — from huge technology companies to small businesses from any industry— could use the personal data of citizens. The GDPR changed the data protection landscape globally and highlights the impact the EU's market and regulatory power has under the Brussels effect.

The EU was also the first to adopt artificial intelligence legislation through the EU AI Act, as part of its broader digital regulatory framework. Remaining a leader in digital policy, the EU has enacted additional digital regulations that promote competition in digital markets and place content moderation obligations on online intermediaries, among others.

Shortly after the GDPR went into effect, many non-EU countries passed their own comprehensive data privacy laws, often modeled with similar language and provisions. Countries like Brazil, China and India now have comprehensive data privacy frameworks that mirror the provisions of the GDPR, and many other countries followed suit by amending existing laws to complement the GDPR's standards.

The GDPR's influence also led to the establishment of data protection authorities around the world. Additionally, the law's requirement to appoint data privacy officers within private organizations revolutionized the data privacy field, opening more opportunities for privacy pros globally.

As of January, 144 countries have their own comprehensive data privacy law — up from 120 countries in 2017. Now, approximately 82% of the world's population is covered by some national data privacy framework.

Upon reflecting on the Brussels effect of the GDPR, IAPP Managing Director, Europe, Isabelle Roccia, CIPP/E, stated, "the GDPR's influence has gone well beyond its mere copy-paste by other jurisdictions. It contributed significantly to the EU promoting its position on data flows in trade agreements and paving the way for many EU digital laws, from online safety to digital markets, to now inform others' policy approach as well."

The European Commission and the European Parliament adopted the GDPR almost a decade ago and it remains a fixed model for others to follow. The Brussels effect of the GDPR and the digital regulations that followed are still felt by industries, consumers, and governments globally and their significance continues shaping individuals' rights, internal data governance, and enforcement actions throughout the world. The broader Brussels effect also continues to promote EU policies and influence on its own terms and keeps Europe a dominant political force on the world stage.

Shortly after the GDPR went into effect, many non-EU countries passed their own comprehensive data privacy laws, often modeled with similar language and provisions.

MOMENTS

Launch of IAPP EU

Over the past 25 years, the IAPP has sought to expand its presence across the world, promoting its mission to define, promote and improve the professions of privacy, AI governance and digital responsibility globally. Efforts to broaden began in September 2008 with the launch of IAPPanz, followed shortly after by IAPP Canada in March 2009. In November 2009, IAPP EU was launched, focusing on the increasingly growing privacy environment in Europe.

Work to expand IAPP's global footprint began in 2004. In December of that year, the IAPP participated in a delegate tour across Europe, visiting Dublin, London, Paris and Brussels, meeting with key regulatory officials and professionals in the industry. Four years later, the IAPP returned to Europe, this time visiting Madrid, Brussels and Rome. That same year, the IAPP hosted its first conference in Europe, the Data Protection and Privacy Workshop in Strasbourg, France, which was a strategic choice, as it was host to annual meetings of international data protection authorities.

In 2011, Rita DiAntonio was appointed as the first IAPP Europe managing director. She previously served as Head of Editorial at Cecile Park Publishing, the originator of the early European privacy journal e-Commerce Law and Policy.

DiAntonio was pivotal for the IAPP's early expansion in Europe. She helped grow the Europe Data Protection Digest, a newsletter that keeps members abreast of privacy and related developments in Europe; the CIPP /E certification designation and related training, geared towards European data privacy professionals; and the Europe Data Protection Congress, an IAPP conference that is still held over a decade later.

In 2015, Paul Jordan, a data governance and regulatory expert, joined as the second managing director and continued to help expand IAPP Europe for the next six years. The first IAPP name plate was also hung in 2015 at Place du Luxembourg in Brussels, Belgium, in partnership with the association management company Interel.

"When IAPP looked to set up its office to cover Europe, it was pretty natural that Brussels would be the epicenter of it all," says Managing Director, Europe, Isabelle Roccia, CIPP/E, who joined in 2022.

Soon after, the first country leaders were appointed across Europe, including France, Germany, Ireland and the U.K. Since then, the growth of IAPP's European wing has been evident, outgrowing their office in 2018 and again in 2025.

IAPP Europe is now a core part of the organization.

The early focus on Europe by the IAPP was prescient, as the consequential General Data Protection Regulation published in the EU in 2016. It was one of the first modernized and sweeping data privacy laws, and it also helped spawn the "Brussels effect" of data privacy regulation across the globe.

"Brussels made sense at the time when the GDPR was being developed, but being in Brussels also made the IAPP really radiate across Europe," says Roccia. "We are able to support members at a national level about national developments, not just what happens in Brussels, but also what happens with DPAs and courts. The GDPR, for example, is very important for any organization that has operations in or with Europe, and so that helps tie us into the IAPP's international footprint."

IAPP Europe is now a core part of the organization. European membership had grown to more than 15,000 members by 2019, and the CIPP/E is now the most popular IAPP certification, held by more than 20,000 professionals worldwide. Its importance will only grow as the proliferation of digital laws, such as the EU Artificial Intelligence Act, the Digital Services Act and the U.K. Data (Use and Access) Act continue.

MOMENTS

Snowden revelations

Twelve years ago, Edward Snowden exposed a vast surveillance network run by the U.S. government, kickstarting a moment that spawned changes around the globe.

The former National Security Agency contractor leaked top-secret information about how the agency's surveillance programs not only swept up information about foreign nationals, but Americans, using methods such as telephone metadata and internet information. His cooperation with several journalists detailed how this work included hacking into Chinese servers, bugging the EU's mission in New York and using secret court orders to require technology companies to search for user data.

"For the first time, the global public was forced to confront the extent to which their digital privacy had been traded in the name of national security and public safety," Byron Tau wrote in his 2024 book "Means of Control."

Depending on who you ask, Snowden was either a hero who brought to light a great injustice, or a criminal who undermined U.S. national security. Originally from North Carolina, Snowden fled the U.S. prior to his whistleblowing and settled eventually in Russia to escape potential criminal charges of espionage. Those came in 2015; whether he should be pardoned has been a subject of fierce debate for years.

The international fallout from the revelations came on quickly; the EU began crafting new rules about how internet servers and social media providers could send data to third countries by the end of 2013, and, significantly for privacy pros, the EU-U.S. Safe Harbor and Privacy Shield programs were both invalidated by the Court of Justice of the European Union in 2015 and 2020, respectively.

Changes in the U.S. included Congress passing the USA Freedom Act of 2015, which outlawed the bulk collection of phone records of U.S. citizens. A section of the Patriot Act allowing this practice, Section 215, expired in 2020 thanks to a sunset clause.

Websites across the spectrum moved from the HTTP to the HTTPS protocol and started taking data security more seriously.

More technology companies, facing the frustrations from consumers, started boosting their security protocols and offering encryption services. This did not go unnoticed by the intelligence community; the year after the Snowden revelations, then-FBI Director James Comey said the backlash could threaten the agency's ability to prosecute crimes where digital evidence could be crucial.

"Perhaps it's time to suggest that the post-Snowden pendulum has swung too far in one direction—in a direction of fear and mistrust. It is time to have open and honest debates about liberty and security," he said.

The U.S. government still can search databases to surveil communications if a U.S. citizen is contacting a target overseas without a warrant, through the Foreign Intelligence Surveillance Act's Section 702. Debates about whether to let the provision expire have raged on in Congress for years, with the most recent attempt to change it failing last year. That practice may face stronger headwinds after a New York federal court judge found it unconstitutional in January.

The disclosures also changed the public's views on the government and privacy, Müge Fazlioglu, CIPP/E, CIPP/US, a principal researcher on privacy law and policy for the IAPP, wrote in 2023. Their occurrence alongside high-profile data breaches like the Facebook-Cambridge Analytica incident eroded trust that companies and the government would protect their information.

Still, Fazlioglu noted then, the full picture of the long-term effects of Snowden's actions was still unfolding.

"Moreover, the issues raised by the leaks are anything but settled. There continues to be a wide range of views expressed about the right balance between national security, privacy and civil liberties. More importantly, a lot of work remains to address the fears, concerns and distrust that has built up over the years," she wrote.

"These realities of the post-Snowden era will likely persist, and they will continue

to shape not only our laws, but our very understanding of what it means to have privacy," she continued later.

But Glenn Greenwald, the journalist whose work on Snowden helped the Guardian win a Pulitzer Prize, cautioned attendees of the 2015 IAPP Global Privacy Summit not to judge the success of Snowden's efforts on whether U.S. surveillance practices change right away, saying those changes would likely not happen without a protracted fight.

Instead, "it is much more important that individuals around the world realized for the first time the threat posed to their privacy from the threat of mass surveillance," he said.

The "Schrems effect"

On 6 Oct. 2015, the Court of Justice of the European Union invalidated the Safe Harbor data transfer agreement between the EU and the U.S. amid backlash in the EU following the 2013 Edward Snowden disclosures.

The effort to challenge the trans-Atlantic data sharing framework in the EU was spearheaded by Austrian lawyer Max Schrems, who would go on to found the EU privacy rights group NOYB. Schrems would ultimately win not one, but two major legal cases at the EU's highest court invalidating both the Safe Harbor and its successor transfer framework, the EU-U.S. Privacy Shield in 2020.

The CJEU's decisions, which became widely known as "Schrems I" and "Schrems II," functionally left companies to primarily rely on alternative data transfer mechanisms such as binding corporate rules and standard contractual clauses to transfer data. Although both frameworks remained operational on the U.S. side through the U.S. International Trade Commission.

Following the 2015 CJEU Safe Harbor ruling, Schrems said in a statement to the IAPP that the decision represented a "major blow for U.S. global surveillance that heavily relies on private partners."

While geopolitical dynamics of the trans-Atlantic data transfer issue played out from 2015-on, IAPP Vice President and Chief Knowledge Officer Caitlin Fennessy, CIPP/US, said the IAPP was coming into its own as a global professional association at the time. The Schrems I and II decisions shifted "privacy issues and concerns from the purview of a small cadre of knowledgeable professionals" into a major business imperative for organizational stakeholders up and down the company ladder, she said.

"Data transfer policy has grown up alongside the IAPP and the privacy profession itself," Fennessy said. "That changed dramatically following Snowden, Schrems I and the adoption of the EU General Data Protection Regulation, which all followed in rapid succession."

In February 2016, the European Commission unveiled the Privacy Shield. At the time, officials touted their confidence the new pact would be immune to similar legal challenges that resulted in the demise of the Safe Harbor. The new Privacy Shield featured provisions like a redress mechanism for EU citizens, boundaries around U.S. surveillance and an annual joint review of the framework.

Then-European Commissioner for Values and Transparency Věra Jourová declared in 2016 the Privacy Shield "will protect the fundamental rights of Europeans when their personal data is transferred to U.S. companies."

"For the first time ever, the United States has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards, and oversight mechanisms," Jourová said.

The European Commission's optimism over the validity of the Privacy Shield was dashed two years later when Schrems challenged the legality of SSCs in Irish courts after Facebook switched to that transfer mechanism following the Safe Harbor invalidation.

In July 2020, the CJEU ruled that the Privacy Shield was invalid, though the decision also upheld the legality of SSCs provided the third country where EU data was transferred offered safeguards in terms of limiting access by public authorities and offering judicial redress.

At a press conference following the ruling, Jourová and fellow European Commissioner for Justice Didier Reynders said the Schrems II decision "provides further valuable guidance for us" and stated both the EU and U.S. "will not be starting from scratch," when it came to negotiating what would ultimately become the EU-U.S. Data Privacy Framework.

Fennessy, who served as a policy advisor at the ITA from 2009-18 and helped negotiate the Privacy Shield on behalf of the U.S. government, said the Privacy Shield invalidation was a wake-up call for leaders of multinational companies.

"The complexities and challenges hit the desks of CEOs and boards and reached into

the highest levels of government in the U.S. and EU," said Fennessy, who became the ITA's Privacy Shield Director beginning in early 2018. "All of a sudden, multinational businesses realized that in the digital economy, if they could not move legally data across the Atlantic, they could not legally do business in the EU."

The European Commission's adequacy decision approving the EU-U.S. DPF was first announced 13 Dec. 2022. The agreement featured new redress mechanisms for EU citizens, such as the establishment of U.S. Data Protection Review Court, which would adjudicate qualified complaints.

However, legal challenges to the framework continue.

In September 2023, French Member of Parliament Philippe Latombe filed a complaint with the EU General Court challenging the DPF, which raised fears of a possible "Schrems III" scenario. After two years, however, the General Court dismissed the complaint and upheld the DPF as constituted.

Fennessy said the DPF's resiliency to this point is a product of policymakers from both the EU and U.S. learning valuable lessons from legal proceedings in the EU during Schrems II, that they failed to consider after Schrems I.

However, the complexities and intricacies surrounding global data transfer policy are only increasing, as more jurisdictions look to set their own rules and requirements.

"When the U.S. and EU negotiated the DPF, they had the benefit of the CJEU's substantive analysis of the shortcomings of the Privacy Shield and sought to address each of them directly," Fennessy said. "Today, trans-Atlantic data transfer policy is experiencing a moment of relative calm and stability. The global landscape for data transfers is becoming more complex by the day as countries around the world implement their own adequacy mechanisms and adopt unique or regional standard contracts to govern data transfers."

MOMENTS

Privacy on the Ground

At IAPP Global Privacy Summit 2016, Deirdre Mulligan and Kenneth Bamberger took to the keynote stage to accept the IAPP Privacy Leadership Award for work that informed their book, "Privacy on the Ground: Driving Corporate Behavior in the United States and Europe."

Originally published in October 2015, Bamberger and Mulligan's research examined corporate privacy management in five countries: France, Germany, Spain, the U.K. and the U.S. After a multitude of interviews with chief privacy officers, data protection officers, engineers, lawyers, advocates and regulators across the five countries, they discovered the one thing that had been overlooked previously was the privacy professional.

"For decades, privacy discussion has focused on laws governing treatment of personal information, privacy on the books, what it says and what it should say," Bamberger said. "But until now," Mulligan continued, "we've had precious little insight into how those words we've argued so passionately about actually shaped the behavior of the companies that handle so much of our data."

Bamberger and Mulligan decided to "look under the hood to see what really mattered."

"It turns out that all of this discussion about privacy on the books, all of these articles, these debates, these hearings, they missed something crucial about what really matters: They missed you. They missed the crucial role of the privacy professional."

What Bamberger and Mulligan found, they said, was that privacy pros had "respective levels of power and influence within" companies, access to boards and senior management, and an external network connecting a broader field of experts, regulators and advocates through associations such as the IAPP.

To document the evolution of the privacy pro's corporate influence, "Privacy on the Ground" starts with Yahoo's 2004 decision to disclose the identity of a Chinese dissident to the Beijing government, which led to the man's imprisonment. The move led to widespread criticism and was "felt in boardrooms throughout Silicon Valley," they said.

Fast-forward a few years later, Yahoo opposed the U.S. National Security Agency's demands to turn over consumer data. "That time," they said, "the company did the right thing and was celebrated."

But what changed, especially since relevant, existing laws really had not in the intervening time?

The company, they said, changed dramatically by empowering and resourcing its privacy and law enforcement staff. "It built privacy in and, when the government came knocking this time, Yahoo was ready to engage in an important discussion about the interplay between privacy and surveillance." That corporate evolution was seen elsewhere, they noted.

"What you do is really special," they added.

Their research has left its mark in the intervening years.

"'Privacy on the Ground' had a significant and lasting impact on privacy policy and practice," Indiana University Professor of Law and Information Accountability Foundation Executive Director Fred Cate said. "It was the first systematic look at how privacy leaders in companies actually approached their work. And it offered the first evidence, as opposed to intuition or impression, that formal privacy law had only a limited relationship to the quality of privacy protection afforded by organizations. It therefore made a particularly important contribution to solidifying the essential role of privacy professionals."

In considering its influence, IAPP Vice President and Chief Knowledge Officer Caitlin Fennessy said, "'Privacy on the Ground' may have even more resonance today, as the U.S. and EU revisit their approaches to digital governance, than when it was first published a decade ago. Mulligan and Bamberger demonstrated how crucial the appointment of responsible privacy leaders inside organizations has been in steering effective privacy practices,

whether navigating prescriptive regulations or building best practices to earn consumer trust. At a time when this latter, principles-based approach prevailed, privacy officers helped to ensure strong privacy in practice. Since its publication, governments around the world have embraced these findings, encouraging or requiring the appointment of knowledgeable privacy professionals as part of broader data protection reform."

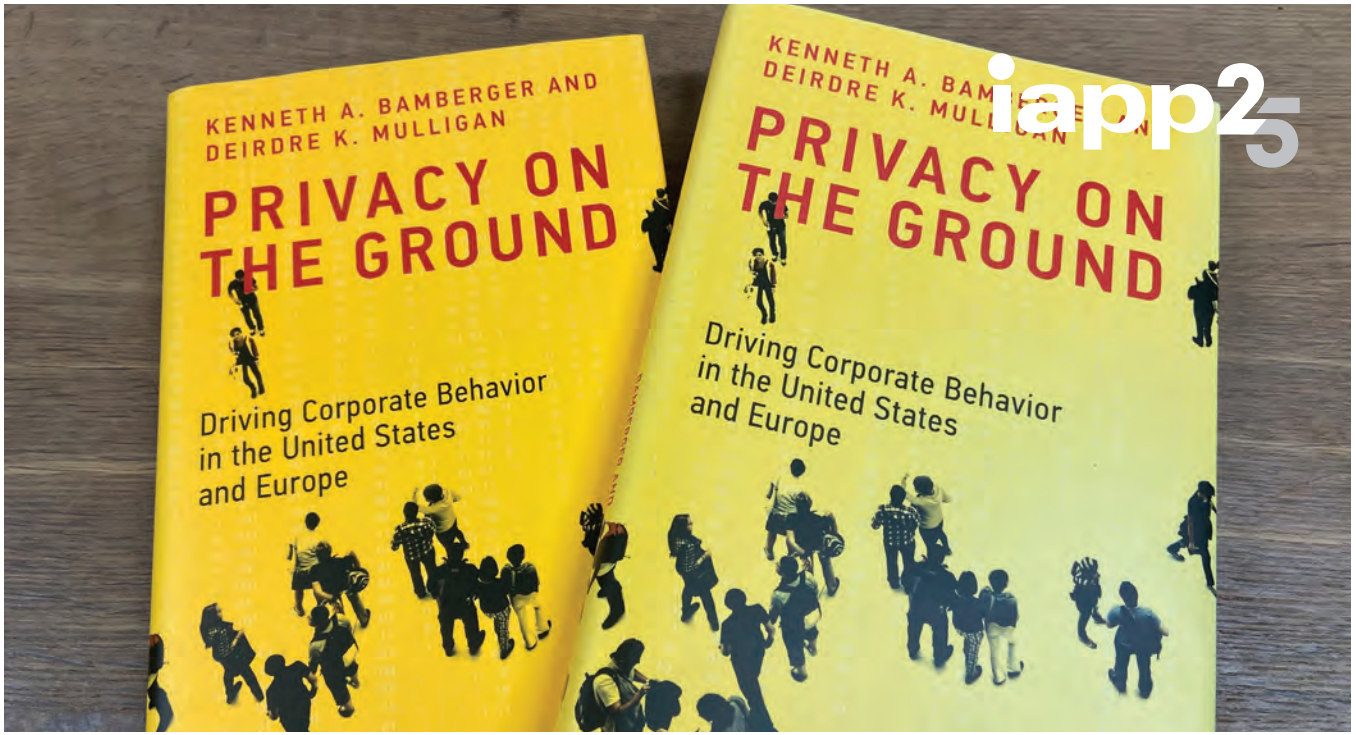
For Gerard de Graaf, who currently serves as Senior Envoy for Digital to the U.S. and Head of the EU Office in San Francisco, the book "illuminated profound realizations for corporate privacy practices by shifting the focus from legal formalism to the practical realities of privacy governance within organizations. They demonstrated how much privacy compliance can be deeply influenced by corporate culture, industry norms, and professional practices."

He said it also provided "a critical perspective on how important accountability mechanisms and internal corporate governance approaches are in bridging regulatory gaps. I am thankful to Ken and Deirdre for advancing the discussion beyond rigid legal comparisons, highlighting the importance of corporate governance, accountability, and practical implementation in shaping effective privacy protections."

Though their 2016 speech predated implementation of the EU General Data Protection Regulation, Bamberger and Mulligan's words were prescient. Not only did they note the GDPR would lead to tens of thousands of jobs for privacy pros, they also looked further ahead to a trend that was just beginning to emerge then and is now in full swing.

They noted CPO job titles were beginning to change and expand to address new challenges brought on by artificial intelligence, machine learning and other technologies. A trend that has now been reflected in the IAPP's 2024 mission expansion to include AI governance, cybersecurity law and digital responsibility.

"The privacy professional community has built a path-breaking model for dealing with the challenges of the information age," they said, "melding strategy and operations, spanning outside commitments and internal legitimacy. ... These are the models that will serve us well."



MOMENTS

Apple v. FBI

In late 2015, the digital age debate around encryption and law enforcement access to private data re-emerged as a national controversy following the horrific terrorist attacks in San Bernardino, California. At issue was a request from the U.S. Federal Bureau of Investigation to Apple demanding it provide access to the terrorist's iPhone, which was encrypted.

Notably, Apple refused to comply with the FBI's request, which set off months of debate and congressional hearings. Should law enforcement be able to use so-called backdoors into protected user data to fight crime and ensure national security? Does that outweigh the personal privacy and data security of every iPhone user around the world?

For Apple, the answer landed on the side of maintaining consumer trust and security over introducing a vulnerability into user data.

Former IAPP Board member Jane Horvath was working as Apple's Senior Director of Global Privacy at the time of the attack, and in 2020, she explained at a technology conference why Apple placed so much value in being able to offer encryption to customers as way of ensuring consumer trust.

"Our phones are relatively small, and they get lost and stolen," Horvath said. "If we're going to be able to rely on our health data and finance data on our devices, we need to make sure that if you misplace that device, you're not losing your sensitive data."

Law enforcement's request for building backdoors into protected user data was not new in 2015. Within the halls of government, the U.S. National Security Agency and Clinton White House began lobbying Congress in the 1990s to require telecommunications companies to install a back door in cell phones for investigatory purposes via the Clipper chip. The chip faced backlash from some lawmakers, as well as the information security and privacy advocacy realms and was never fully adopted.

By February 2016, months after the San Bernardino attack, the IAPP reported, "this week, the crypto debates reached fever pitch – potentially becoming an election issue in the U.S. and affecting the way governments around the world attempt to access personal information from technology companies." A federal judge ordered Apple to "technically assist" the FBI in unlocking the iPhone.

In a direct letter to its customers, however, Apple CEO Tim Cook said the company would not comply, explaining why encryption "has become so important to all of us. … For many years, we have used encryption to protect our customers' personal data because we believe it's the only way to keep the information safe. We have even put that data out of our own reach, because we believe the contents of your iPhone are none of our business."

At the IAPP Global Privacy Summit in April 2016, then-FBI General Counsel Jim Baker responded to the encryption debate, in a highly anticipated and well-attended breakout session, saying that the agency was dealing with a "going dark" problem. In order to protect people and the economy, the FBI relied on electronic surveillance.

"That said, the tool we've relied on is becoming less and less effective today with respect to content because of encryption," he said. "As it's spread throughout the world, as it's become easier to use, and become the default, more people will use it."

With a "zero-failure rate" when fighting terrorism, Baker said the agency needed to use all the tools in its toolbox in that battle. But, he added, "We love encryption. … I've been a victim of privacy crimes several times, including at the [Office of Personnel Management]. I wish that data had been encrypted."

Eventually, the FBI was able to use a third-party to access the shooter's phone. In hindsight, the Apple-FBI issue was only part of a long-running tussle over encryption, which continues to this day.

In 2022, Apple announced the launch of three new privacy-preserving services including Advanced Data Protection for iCloud, which featured end-to-end encryption for 23 sensitive data categories. However, the launch also brought news

Apple was halting its plans to introduce screening capabilities for child sexual abuse material stored in iCloud after privacy advocates criticized the feature could be a possible means for compromising its own encryption.

In February 2025, Apple announced it was withdrawing its Advanced Data Protection feature for U.K. users' iCloud accounts after the Home Secretary served the company with a technical capability notice under the Investigatory Powers Act. The notice called for Apple to create a back door in its encryption to assist with law enforcement investigations.

As Apple and the U.K. government were clashing in the U.K. behind the closed doors of the Investigatory Powers Tribunal, the FBI once again jumped on the opportunity and signaled it would similarly demand "lawful access" to encrypted data.

Though the debate continues, the so-called Apple v. FBI controversy that began in 2015 highlighted the significant part privacy and data security play in the modern economy and national security. As a private company, Apple took a very public stand on behalf of its customers in the name of their privacy and security. The fact that a CEO publicly endorsed the importance of privacy was a significant moment in the history of the privacy profession, making it a front-and-center issue undergirding democratic freedoms and expression.

In his 2016 letter to Apple customers, Cook said opposing the FBI's order "is not something we take lightly. We feel we must speak up in the face of what we see as an overreach by the U.S. government.

"We are challenging the FBI's demands with the deepest respect for American democracy ... We believe it would be in the best interest of everyone to step back and consider the implications. While we believe the FBI's intentions are good, it would be wrong for the government to force us to build a backdoor into our products. And ultimately, we fear that this demand would undermine the very freedoms and liberty our government is meant to protect."

MOMENTS

The "California effect"

Earlier this year, we celebrated what's known to many as the "Brussels effect," but the EU's capital is not alone in its policymaking influence. California — which boasts the world's fourth-largest economy — has long set the tone for consumer and environmental regulations in the U.S., and its norm-setting legacy is well established in the privacy world.

California has led the U.S. in privacy legislation ever since voters added a right to privacy in 1972 through another ballot initiative, said Lothar Determann, a partner at Baker McKenzie Palo Alto and the author of the IAPP's "California Privacy Law." But its effect differs slightly from Brussels in that the EU is able to entice other countries to adopt its style of regulation by granting access to the market through adequacy decisions,

The state does not have such formal powers, but "the 'California effect' roots in other U.S. states, the federal government, and other countries following California's lead, because they agree with California's privacy protection policies and measures, for example, by adopting breach notification requirements, online privacy policies, and, most recently, restrictions on personal information selling," he said.

The 2002 breach of a state data server exposing the personal information of more than 250,000 state employees was the impetus for SB 1386, a law that set standards for any incident where Californians' data was compromised. State agencies were required to send out notices if personal information was acquired by an unauthorized individual.

The law would not go into effect until 2003, but Joanne McNabb, CIPP/G, the former head of the California Office of Privacy Protection, wrote in 2018 there was a need to anticipate the law's requirements ahead of time. She penned a disclosure that would become commonplace in data breach response protocols: a breach notice.

Also passed that year was the California Online Privacy Protection Act, known as CalOPPA. The law required any website accessible to Californians to post details about its privacy and data collection practices -— now a staple of many privacy policies.

As IAPP Managing Director, Washington, D.C., Cobun Zweifel-Keegan, CIPP/US, noted last year, "Requiring detailed posted privacy notices was a game changer, not because it led to more informed consumers, but because it provided a hook by which regulators could enforce privacy promises via general consumer protection laws like the Federal Trade Commission Act." The law still has teeth today, with the California Attorney General's Office citing CalOPPA in settling an unlawful data selling case with DoorDash.

Fast forward 15 years, when California passed the California Consumer Privacy Act in 2018. The law established new privacy rights in the state and data obligations for businesses by allowing people to request what data a company has collected on them. Businesses, in turn, needed to find a way to facilitate these requests; consumers also have a right to know what kind of information is being sold on them and to whom.

That bill was passed after San Francisco real estate developer and investor Alastair Mactaggart gathered enough signatures to put a question on the ballot enshrining similar rights; an eleventh-hour deal with Mactaggart resulted in the California Consumer Protection Act, widely seen as a compromise between privacy advocates and the technology industry. Mactaggart was not finished, however; a year later — from the keynote stage at the IAPP Privacy. Security. Risk. Conference — he launched another ballot initiative to establish the California Privacy Rights Act. The initiative passed in November 2020, adding more privacy rights and creating the California Privacy Protection Agency.

Because California is such a major economy, its policies inherently have influence on the rest of the country, said Global Data Innovation CEO Dominique Shelton Leipzig, AIGP, CIPP/US, who represented the California Chamber of Commerce during CCPA negotiations. But its regulations have carried a mix of consumer protection rights and business realities that make them more accessible for the rest of the country, she said.

"The result is an enduring ripple effect: businesses nationwide are now aligning governance, compliance and innovation strategies to anticipate where California will lead next," she said. "I see that influence not only continuing but accelerating — especially as we enter a new era defined by AI, and California's regulations on automated decision-making."

MOMENTS

50,000 members

Before 2019, the IAPP's membership was increasing gradually.

In 2004, there were 1,000 members; 10 years later, there were 20,000, according to archival IAPP data. Increases came largely at around 2,000 to 4,000 new members per year, with some years seeing as many as 6,000 and as few as 714.

As with so many things, the EU General Data Protection Regulation changed that. Even though the GDPR had been percolating in the background for several years, its entering into force in the spring 2018 sparked an interest never seen before: the IAPP saw a 25% jump from May 2018 to April 2019, bringing it to the significant milestone of 50,000 members.

"An additional 10,000 members in less than a year was just wild relative to what we'd seen in the past," said IAPP Membership and Customer Relations Director Matt McNeil, who was working in membership at the time.

"Even back in 2017, we went up less than 10,000 members, and that was at the peak of training and sales we were doing related to GDPR."

The milestone showed how far the privacy field had come, LinkedIn Vice President and Chief Privacy Officer Kalinda Raina said at the time.

"Now, most companies, if not the vast majority, are at a place where they need a privacy professional, which really wasn't true even five or 10 years ago," she said in a press release marking the occasion. "The fact that the organization has been able to navigate the explosive growth of this issue is truly extraordinary."

To mark the occasion, the nonprofit brought the 50,000th member all the way from Australia to the Global Privacy Summit, presenting them with a pair of custom-made Converse sneakers in IAPP green.

The milestone also signaled a time for change within the IAPP, McNeil said. The IAPP had been seeing an increase in European membership and had launched its European office in the years leading up to the GDPR's implementation. It revamped its certification process in 2019 to change how people bought and submitted for credentials.

What was then the membership and engagement team was more expansive than its name implied, with customer support and administrative duties encompassed under the department's umbrella. Product support was mixed in there, too.

The rate of growth made that kind of consolidation unmanageable, McNeil said. So, the IAPP split the departments up, creating the membership management and the customer support departments in place today.

"It was a very rapid change that luckily we had the foresight to see it coming," he said.

To mark the occasion, the nonprofit brought the 50,000th member all the way from Australia to the Global Privacy Summit, presenting them with a pair of custom-made Converse sneakers in IAPP green.

MOMENTS

The FTC's $5 billion fine of Facebook

On 24 July 2019, the U.S. Federal Trade Commission entered into a USD5 billion settlement agreement with Facebook after the agency's year-long investigation into the company's privacy practices. Rooted in the FTC's allegation that Facebook violated a prior administrative order with the agency regarding its privacy practices, the agreement required the social media company now called Meta to restructure its privacy program with new oversight and transparency mechanisms and brought about a financial penalty that became not only the largest fine ever imposed by the FTC, but one of the largest administrative penalties in U.S. history.

The settlement was based on complaints that Facebook repeatedly engaged in deceptive practices about its privacy settings and users' abilities to opt out of these settings, in violation of the 2012 settlement. Among the alleged practices were deceptive disclosures about users' abilities to opt-in to the company's facial recognition feature and using telephone numbers for purposes other than the disclosed security feature.

The agency also found that the online platform had removed its policy for sharing users' personal information with third-party apps after the 2012 order was entered. It further alleged that the company allowed third parties to continue collecting personal information from users without their knowledge or providing an opt-out mechanism, despite notifying users that the sharing would be discontinued after April 2014.

Additional allegations included improper due diligence when contracting with third-party apps and further mismanagement and oversight of how these third-party apps handled users' personal data.

This remains the largest settlement in the FTC's history.

Under the 20-year settlement, Facebook agreed to various obligations aimed at ensuring transparency and accountability throughout its privacy program. This included the establishment of an independent privacy committee to the board of directors, appointed by an independent nominating committee. It also required Facebook to designate independent compliance officers to oversee the privacy program and submit quarterly certificates of compliance.

The order empowered third-party assessors with further independence in fact-finding and gathering information for its biennial assessments of the company's adherence to the new privacy program. The third-party assessor is appointed and removed by the FTC.

The order also restructured the company's privacy policies across its products by creating quarterly reporting obligations, documentation obligations, and incident reporting requirements for events involving 500 or more users. It further required the social media platform to exercise stronger management over third parties, implement password encryption, and publish clear and conspicuous disclosure of its collection policies, including its facial recognition capabilities.

Upon announcing the settlement agreement, former FTC Chairman Joe Simons stated that the USD5 billion settlement was designed both to penalize the alleged misconduct and "to change Facebook's entire privacy culture to decrease the likelihood of continued violations."

The 2019 settlement highlighted the strength of the FTC's enforcement authority for consumer privacy complaints and violations, despite the lack of federal comprehensive data privacy legislation. It also had the lasting effect of putting companies on notice that violating their privacy policies or maintaining insufficient privacy practices could lead to severe financial penalties. This remains the largest settlement in the FTC's history.

MOMENTS

Brazil's LGPD

Two years after the GDPR went into force and almost exactly five years ago, on 18 September 2020, Brazil's Lei Geral de Proteção de Dados came into effect. Substantively, the LGPD borrows the broad architecture used in the EU General Data Protection Regulation but uses Brazil's own vocabulary and safeguards. The law applies broadly and extraterritorially to processing that takes place in Brazil, offers of goods or services to people in Brazil, or personal data collected in Brazil, regardless of the location of a company's headquarters. It grounds processing in core principles such as purpose limitation, adequacy, necessity, transparency, security, prevention and accountability.

Institutionally, Brazil's national data protection authority, the ANPD, was created as a sector-agnostic regulator for the LGPD. Under Article 55-K, it has exclusive power to apply LGPD sanctions. Over time, the ANPD has been formalized with a board and independent decision-making capabilities.

The ANPD's enforcement capability has grown quickly. In February 2023, the ANPD issued a Dosimetry and Sanctions Regulation that defines how penalties are measured and calculated. Since then, the authority has used its powers in a series of cases, including public-sector warnings in early 2024 and a high-profile preventive order in July 2024 that suspended Meta's plan to use Brazilians' data for AI training.

The LGPD contains detailed rights and obligations. Controllers must notify both the ANPD and affected individuals of security incidents that present relevant risk or damage. Since 2024, the deadline for such notification is three days from when the controller becomes aware of the breach, or six days for small-scale controllers.

Brazil has also moved to bring order to cross-border data flows. On 23 August 2024, the ANPD approved the International Data Transfer Regulation and published Brazil's standard contractual clauses, with an implementation deadline of 23 August 2025.

Brazil is building a durable privacy baseline across Latin America, and its trajectory is clear.

The LGPD's penalty framework permits the ANPD to issue fines up to 2% of an entiity's gross revenue, up to a cap of BRL50 million. It can also impose additional penalties, such as publicizing the infringement, suspending the "personal data processing activity related to the infraction for a maximum period of six months," or "partial or total prohibition of activities related to data processing," based on the severity of the infraction.

Recognizing the large number of smaller entities that do business in Brazil, the ANPD tailored rules for small-scale controllers in 2022. These allow simplified records, extended deadlines in some procedures, and no mandatory data protection officer if the controller provides a contact channel. In 2024 the authority went further and issued a binding data protection officer regulation that clarifies duties and confirms when a controller is required to appoint a DPO.

Taken together, the LGPD now has a full toolkit for regulation and enforcement: clear scope, articulated principles, a single regulator with exclusive sanctioning power, deadlines for incident reporting, and operational guidance for global transfers. Companies doing business in or with Brazil would do well to treat the ANPD's regulations as living documents, since the authority continues to refine breach, DPO, and transfer frameworks while building a visible enforcement track record.

Brazil is building a durable privacy baseline across Latin America, and its trajectory is clear: protecting people's privacy, giving businesses certainty, creating workable tools for cross-border transfers and setting a reference point for neighbors shaping their own laws.

MOMENTS

China's PIPL

Three years after the EU General Data Protection Regulation came into effect, China passed its own comprehensive data privacy act: the Personal Information Protection Law. The PIPL developed upon the principles espoused in the GDPR to create a unique framework that emphasizes national security, state oversight and stricter localization requirements, while still reflecting global privacy norms like transparency, purpose limitation and individual rights. It unified the Chinese Data Security Law and Cybersecurity Law, forming a trio of statutes designed to govern data privacy. While earlier regulations were sector-specific or tailored toward cybersecurity, the PIPL squarely focuses on personal data, with detailed obligations and procedures for entities that handle the data of people in China.

For privacy pros versed in the GDPR, the PIPL can feel similar in structure yet distinct in execution. For example, instead of addressing the processing of personal data by data controllers, the PIPL addresses the handling of personal information by PI handlers. Thus, it defines key terms differently and applies to a different subset of data handlers and handling operations.

Both laws require entities to have legal bases for handling PI, some of which they share and some of which are unique. Consent is the primary basis under which data is managed in both laws, but the PIPL requires the PI handler to obtain "separate consent" in certain circumstances. This means individuals may have to indicate both their general consent as well as one or more instances of separate consent when, for example, the data handler is managing their sensitive PI. The PIPL also contains no equivalent of the GDPR's "legitimate interest" basis for processing PI.

Both laws create fundamental individual rights, including the right to access, the right to rectify, the right to refuse, the right to data portability, rights related to automated decision-making and the right to delete/erasure. The PIPL requires data handlers to proactively delete PI rather than waiting for a data subject request as is the requirement under the GDPR. The PIPL also creates an individual right to sue data handlers if the data handler does not honor the individual's request to exercise these rights.

While earlier regulations were sector-specific or tailored toward cybersecurity, the PIPL squarely focuses on personal data, with detailed obligations and procedures for entities that handle the data of people in China.

Cross-border data transfers impose different obligations under each law, such as the PIPL's requirement that certain data transfers must pass a security assessment, comply with standard contractual clauses published by the Cyberspace Administration of China or become certified through CAC-designated agencies. A recent judgment on a PIPL cross-border data transfer lawsuit highlighted that regardless of whether a company does business in China, it must comply with the PIPL if it handles the PI of individuals in China.

Although similar principles undergird both laws, the PIPL is far more than just China's version of the GDPR — it reflects the country's broader policy goals around the strategic value of personal information in a digital economy. For privacy professionals, navigating the PIPL means understanding both the letter of the law as well as how it intersects with national security, data sovereignty and digital governance obligations. The PIPL is a landmark law that is shaping the rules of the road for over an eighth of the world's population and impacting compliance obligations for businesses far beyond.

MOMENTS

India's DPDPA

In 2017, a year before the EU General Data Protection Regulation went into force, the Supreme Court of India recognized the fundamental right to privacy in the case known as Puttaswamy v. Union of India.

However, it would take another six years for India to ultimately pass its comprehensive privacy law, the Digital Personal Data Protection Act. During that period, the world's largest democracy underwent significant digital transformation and a cultural shift in views toward privacy.

IAPP member and PwC India Associate Director for Data Privacy Abhishek Tiwari, AIGP, CIPP/E, CIPM, FIP, said the intervening years were largely marked by the COVID-19 global pandemic and India's subsequent shift online. Previously, he said, the notion of privacy itself was somewhat foreign to many Indian citizens who define themselves by their generosity and openness toward one another.

"The COVID-19 era was when we saw a lot of adoption among the Indian people of doing everything online from transactions, using applications, to work itself," Tiwari said. "Our attitudes used to be, 'If I care for you, I share for you,' so we approached handling personal data this way too."

In 2018 and 2019, India's Parliament introduced its first attempts at passing a comprehensive privacy law with two versions of the Personal Data Protection Bill. The proposed legislation featured a broader definition of what constituted personal data compared to the EU General Data Protection Regulation, a broader definition of "consent" and a more stringent definition of legitimate use, while imposing significant data localization requirements.

However, the PDPB was withdrawn in Parliament in 2022 after 81 amendments were added to the legislation by the Joint Parliamentary Committee.

Then, in 2023, the Digital Personal Data Protection Bill was introduced. What would ultimately become the DPDPA was based on the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and accountability, according to Deliotte Data Privacy Manager Ravin Nandle, AIGP, CIPT. The bill also proposed establishing the Data Protection Board of India.

"Keeping in line with the global trend, the bill has extraterritorial applicability," Nandle wrote in 2023 shortly after the DPDPA was introduced. "It will apply to all organizations processing digital personal data outside the territory of India, if such processing involves profiling or offering goods and services to data principals within the territory of India."

Compared to other major pieces of legislation, Tiwari said the DPDPA sailed through Parliament.

"The timeline moved very fast if you think about how from 2017, when the work was started, it took almost five years for the DPDPA to be introduced," Tiwari said. "Then it took just one and a half years for Parliament to pass the bill. Most people don't actively watch Parliamentary sessions, but a lot of professionals here made sure to watch the sessions and listen to the discussion."

Once the DPDPA passed, the IAPP published a series examining the top-10 operational impacts of the new data protection law, which featured contributions from leading Indian privacy law professionals. The series touched on topics such as the scope, key definitions and lawful data processing activities, data processor obligations, enforcement and consent management.

"While individual data privacy and consumer rights lie at the heart of the GDPR, and similar data protection laws elsewhere, the DPDPA appears to have also been driven by India's concerns around national security and other political issues," CBRE South Asia Private Limited Legal Director Sandeep Sangwan, CIPP/A, CIPP/E, wrote in the first installment of the series. "This may explain the unique and distinct features of the act that depart from the GDPR and similar data privacy regimes."

Although it is unclear when the DPDPA will take full effect, the DPDPA's draft rules were subject to a public consultation that concluded in March. Stakeholders

are currently still awaiting government announcements on how certain rules will be operationalized, which are anticipated to be released throughout the rest of the year.

Tiwari said industry is already taking note of the key provisions, such as data subjects' ability to nominate an agent who acts as a proxy for their data protection legal matters. He said by India passing the DPDPA, it signals to multinational companies that India is serious about data privacy.

"Our clients are beginning to realize this is not just a copy and paste of some other privacy regulation," Tiwari said. "But everyone is excited overall. Companies are excited about how they can leverage complying with the requirements of the DPDPA, so we can win the trust of our global partners."

Looking ahead, Tiwari said the DPDPA stands to bring major economic benefits to India in the form of increased employment in the tech sector. He also applauded the government for organizing listening sessions in major cities to solicit feedback from citizens and stakeholders about how the DPDPA stands to impact them in practice.

"Our economy is going to get a major boom from implementing the DPDPA," Tiwari said. "In the past, some of the global players used to be a little hesitant about how data was shared in India, so now they can have confidence that we have a data privacy regulation in place."

Launch of ChatGPT and the rise of AI governance

On 30 Nov. 2022, an artificial intelligence research lab made a post that would change the way the digital world works.

"We've trained a model called ChatGPT which interacts in a conversational way," OpenAI announced in a blog post. "The dialogue format makes it possible for ChatGPT to answer follow-up questions, admit its mistakes, challenge incorrect premises, and reject inappropriate requests."

Before ChatGPT, OpenAI was getting attention for issues that would become the harbingers of the modern AI governance debate. In August 2021, Axios noted its Codex model marked a significant advance in language processing, allowing coders to offload some of their work. Two months before ChatGPT's debut, The Washington Post reported that OpenAI's DALL-E image generator had not only spurred the launch of several competitors, but also sparked concerns over copyright laws, stereotyping, bullying, harassment and disinformation.

Microsoft President and Vice Chair Brad Smith put it this way in a February 2023 blog post about ChatGPT's advent and what it would mean for responsible AI: "What will this change? Over time, the short answer is almost everything."

"Because, like no technology before it, these AI advances augment humanity's ability to think, reason, learn and express ourselves," he wrote. "In effect, the industrial revolution is now coming to knowledge work. And knowledge work is fundamental to everything."

Generative AI had existed before ChatGPT, but the chatbot's release had a technological and cultural effect, said Navrina Singh, the founder and CEO of Credo AI.

"For the first time, millions of people were able to see, touch, and converse with a large language model in real time," she said in an email. "It collapsed the distance between research and real-world experience."

That accessibility created "excitement and urgency," Singh said. "It revealed the extraordinary potential of AI; and the very real risks, to every boardroom, classroom, and kitchen table."

The impact of such technology became immediate in the regulatory world.

Rapid adoption in the EU exposed regulatory gaps just as the EU AI Act was nearing its final stages of development. At the time, Considerati Senior Advisor Cornelia Kutterer, AIGP, said, the bill's scope was focused on biometric surveillance and high-risk AI. By December 2022, regulators were introducing the concept of general-purpose AI systems to the text.

"This resulted in the late-stage adoption of rules specifically targeting foundation models: regulators shifted focus to models' broad capabilities and the systemic risks they pose, moving beyond the conceptual risk-based approach to explicitly target foundational models that exhibit emerging capabilities," Kutterer said.

The effects did not stop there for the EU, Kutterer added. Italy's data protection authority, the Garante, opened an investigation into AI platform's compliance with the EU General Data Protection Regulation after it briefly banned ChatGPT over concerns about its data collection practices. That action later resulted in a 15 million euro fine.

The chatbot's data training on a broad range of sources — from news websites to social media platforms to archives of scanned books — has led to European Parliament and the European Commission considering transparency disclosures and training data summaries in lieu of copyright reform. Kutterer noted those issues "have yet to be solved in practice," resulting in their litigation in Europe and the U.S.

ChatGPT remains central to the debate around responsible AI due to its wide popularity and use cases.

In the context of user safety, ChatGPT has brought tough conversations around chatbot and user interactions to the forefront, especially as some turn to the chatbot for companionship. Tackling issues stemming from those interactions has not

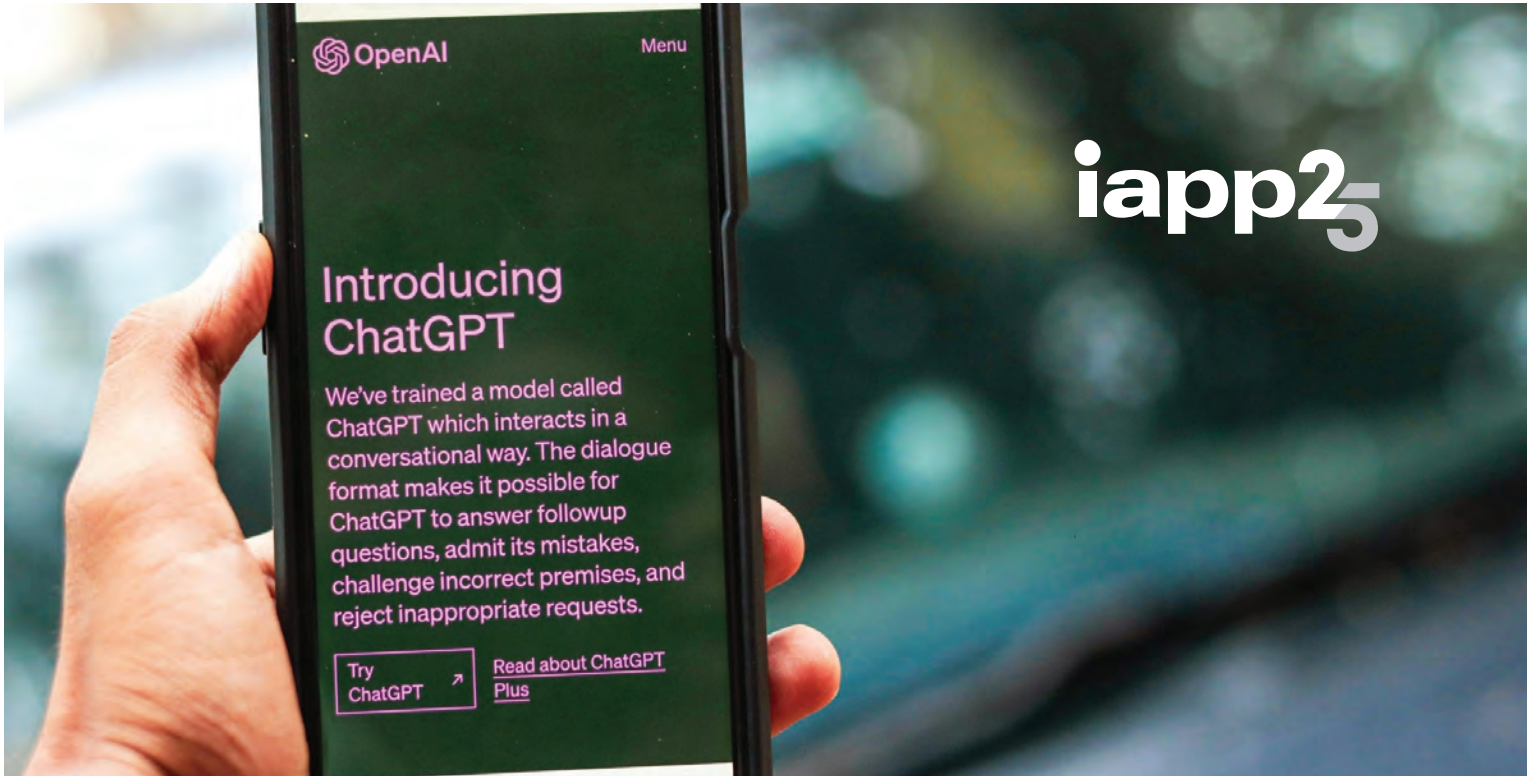
been easy, as OpenAI faces lawsuits for ChatGPT's role in encouraging self-harm and mental delusions, particularly among children.

Recognizing model hallucinations and how to fix them — something OpenAI noted would be "challenging" to fix in its Nov. 2022 blog post because of the way chatbots learn and operate — is an ongoing struggle. OpenAI and other AI developers are now on the frontlines of stopping cyberattacks using their own software.

While other AI developers have since launched competitors and face similar regulatory scrutiny, OpenAI is the most-used chatbot in the world. And CEO Sam Altman is an active voice in global and jurisdictional AI policy debates.

For Singh, ChatGPT's advent made AI governance an impossible issue to ignore. Whereas governance used to live in policy documents and principle statements, the concept has now become an "operational discipline."

"Today, boards and regulators expect scientific, evidence-based governance — measurable oversight, continuous evaluation, and the ability to demonstrate that AI models are monitored, risks are mitigated, and outcomes align with organizational values as well as emerging global standards such as the NIST AI RMF, ISO 42001, and the U.S. AI Action Plan," she said.



MOMENTS

The IAPP expands its mission

Less than two years after ChatGPT took the world by storm and a year after the EU reached a deal on the world's first comprehensive AI regulation, the IAPP expanded its mission to include artificial intelligence governance, cybersecurity law and digital responsibility.

The move was designed to reflect and support the evolving needs of organizations and professionals working across digital governance domains around the world.

The rapid rise of AI and other sophisticated technology along with the proliferation of digital regulations worldwide led to what the IAPP called the "digital entropy" organizations were feeling as a result. This concept was detailed in the IAPP's inaugural Organizational Digital Governance Report.

"We coined the term 'digital entropy' as something that might help encapsulate the confusion and complexity in the disorderly coming together (or not) of different digital law and policy domains and the commensurate confusion and complexity within organizations on how to respond," said IAPP Research and Insights Director Joe Jones. "Our perspective as arms-length researchers matched what we heard and saw in our governance data, what we heard from our advisory boards, and what we saw in our community more broadly: that there was a professionalizing, an organizing, and an aligning of efforts on digital governance more broadly. Yes, that took in privacy and AI governance, but we also saw the accumulation of other fields like cybersecurity law, online safety, and intellectual property to name just a few."

The mission change followed a succession of announcements from the IAPP, dating back to 10 May 2023, when it launched its AI Governance Center and a few months later, in October, appointed Ashley Casovan as managing director of the newly minted AIGC. By 5 March 2024, the IAPP continued its expansion beyond privacy and data protection, when it launched the new AI Governance Professional Certification.

"A little more than two years ago, I joined IAPP to lead what was then the new AI Governance Center," said Casovan, who has led the IAPP's AI governance efforts in multiple facets. To date, the IAPP has seen more than 17,000 individuals sign up for AIGP training and 12,000 for the exam, in addition to thousands of professionals who have attended AI Governance Global events, in Boston, Brussels and Dublin.

"It's been a wonderful experience seeing the Center grow, mature, and demonstrate value," Casovan said. "While there was a strong appetite to expand the remit of IAPP beyond being a professional association for those in privacy, being successful with this expansion was not a guarantee, especially with so many different organizations developing AI governance efforts."

For Casovan, the numbers are proof that "there is a need for a professional association in this emerging field. I think that we still have a long way to go both as an ecosystem and a professional community with AI adoption still at the early stages of its maturity curve, however, making space for professionals to share best practices, educate themselves, and demonstrate competency is more crucial now than ever."

As part of the mission expansion in 2024, the IAPP also launched the Cybersecurity Law Center and appointed Jim Dempsey, a leading cybersecurity law, privacy and internet policy expert, as its managing director. Dempsey had already published the Cybersecurity Law Fundamentals book with the IAPP (now in its second edition), and, that same year, shared his thoughts on the state of cybersecurity law in a podcast with co-author John Carlin.

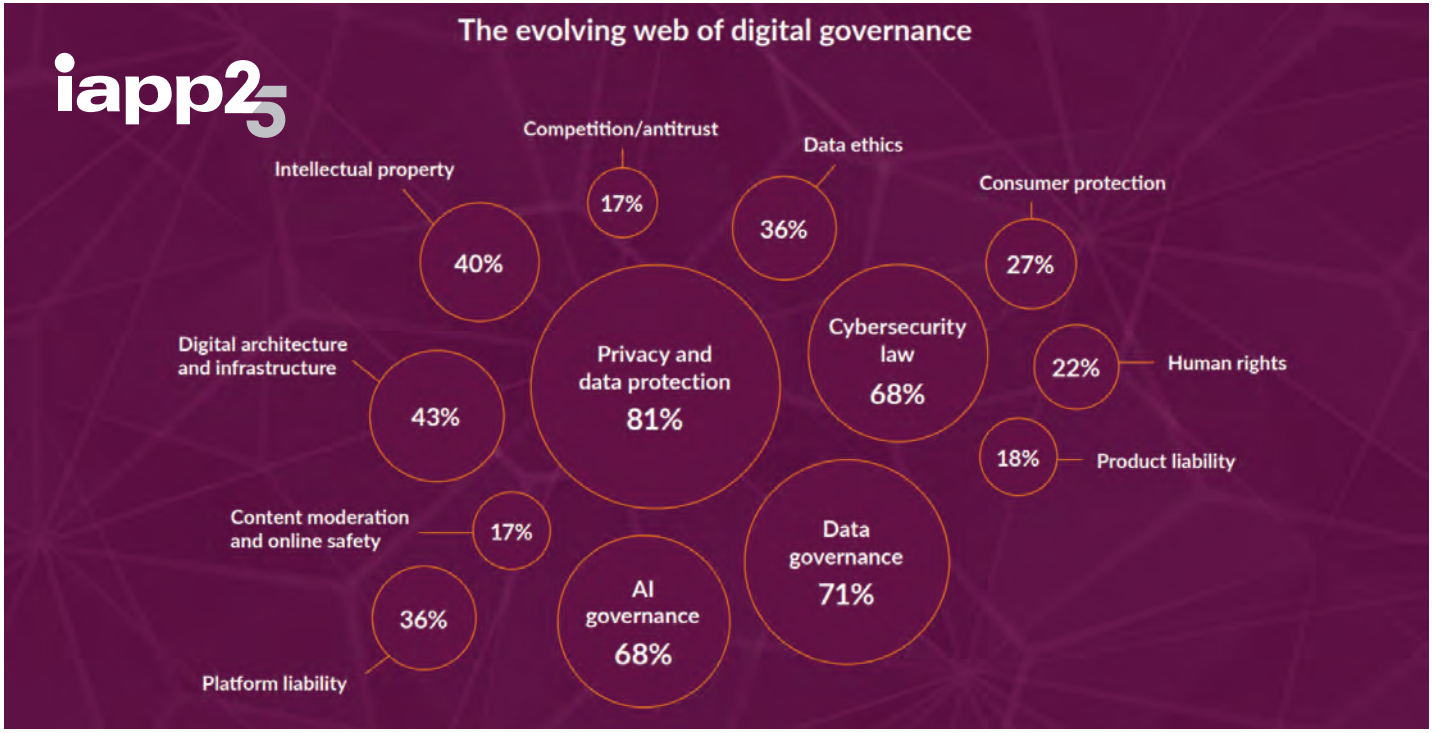
"Data governance silos were probably never a good idea, but in today's environment of rapid AI adoption, expanding regulatory requirements and aggressive cyber threat actors, it is impossible for any enterprise to manage its data without cooperation among privacy, cybersecurity and AI teams," Dempsey said. "That's why IAPP's move to expand our mission to include AI governance and cybersecurity law was so critical. Whether it's reporting to senior management and boards, shaping product development, or engaging with policymakers and regulators, a holistic understanding of all three domains is necessary."

By the end of 2025, it's clear data professionals are being tasked with a host of responsibilities. And though the year has seen the pendulum swing toward deregulation, the complexity for those in digital responsibility is not abating, and the IAPP continues to see more interest in its expanding mission. The AI Governance Dashboard now has more than 20,000 subscribers and the AIGG-North American conference has merged with P.S.R. and will debut next fall in Seattle.

The R&I team steadily offers valuable work in the area, whether through the latest Organizational Digital Governance Report, the AI Governance Profession Report, as well as benchmarking in the newest Salary and Jobs Report 2025-26: Privacy, AI Governance and Digital Responsibility.

"Technology and the data that drives it shape our understanding of the world today and the discoveries we will make in the years to come. Our profession has evolved to encompass everything at the intersection of data, technology, and human engagement, ensuring human interests guide our path forward and build confidence in the journey ahead," said IAPP Vice President and Chief Knowledge Officer Caitlin Fennessy.

"As we close our 25th anniversary year, our profession continues to grow and expand across new domains and issues," said IAPP President and CEO J. Trevor Hughes. "For some, this may be disorienting. The entropy of digital policy around the globe certainly makes our work more complex and challenging. But the overarching feelings must be of purpose and gratitude. Purpose, as our work has never been more vital or important. And gratitude, as we work each day in such a fascinating field, with such amazing colleagues."



MOMENTS


iapp25