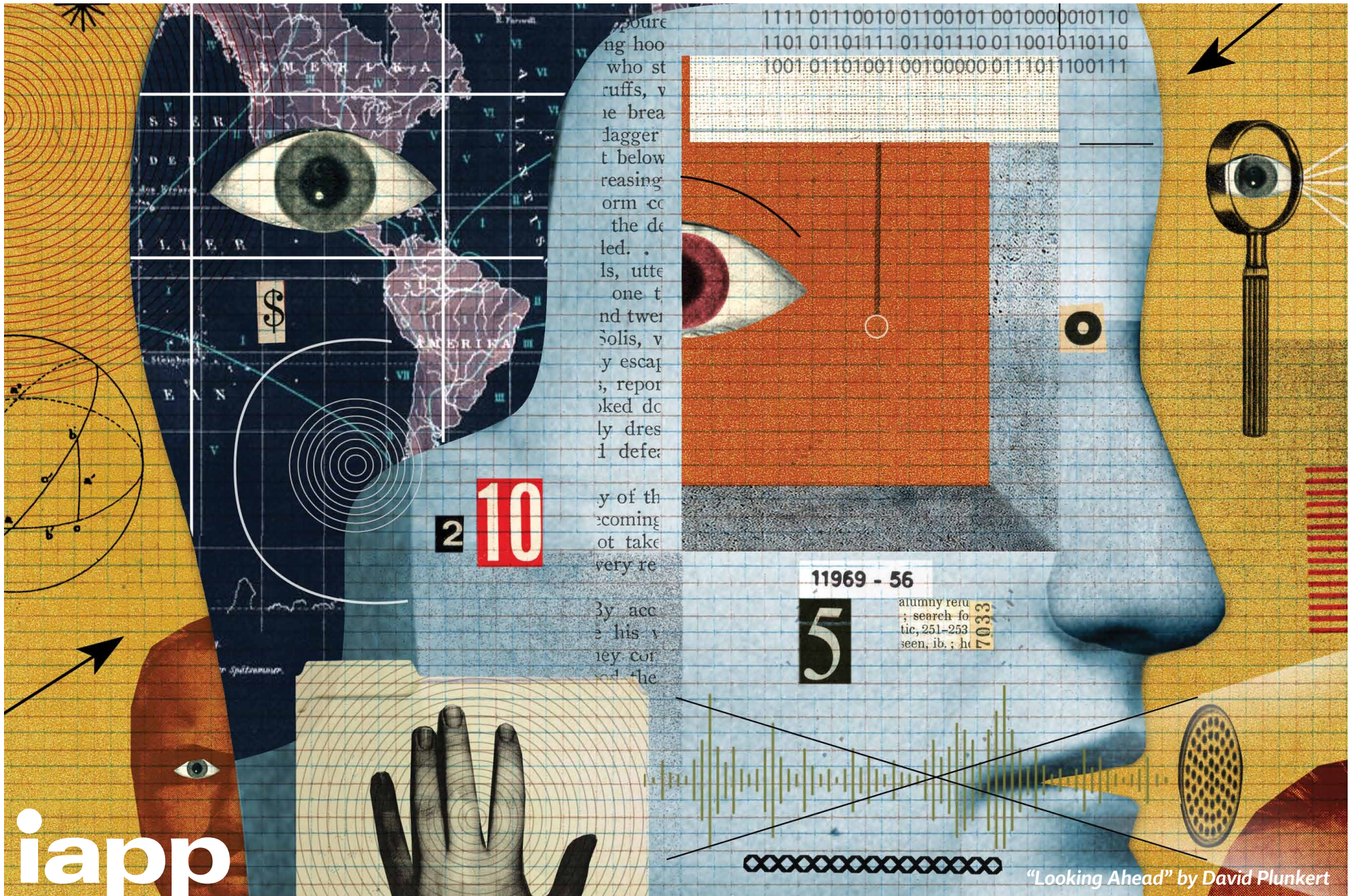


# VISIONS OF PRIVACY



...poure  
ng hoo  
who st  
ruffs, v  
ie brea  
lagger  
t below  
reasing  
orm co  
the de  
led. .  
ls, utte  
one t  
nd twer  
solis, v  
y escap  
, repor  
oked do  
ly dres  
1 defea

1111 01110010 01100101 00100000101110  
1101 01101111 01101110 01100101101110  
1001 01101001 00100000 0111011100111

2 10

y of th  
coming  
of take  
very re

11969 - 56

5

atumny reru  
; search fo  
tic, 251-253  
seen, ib. ; h

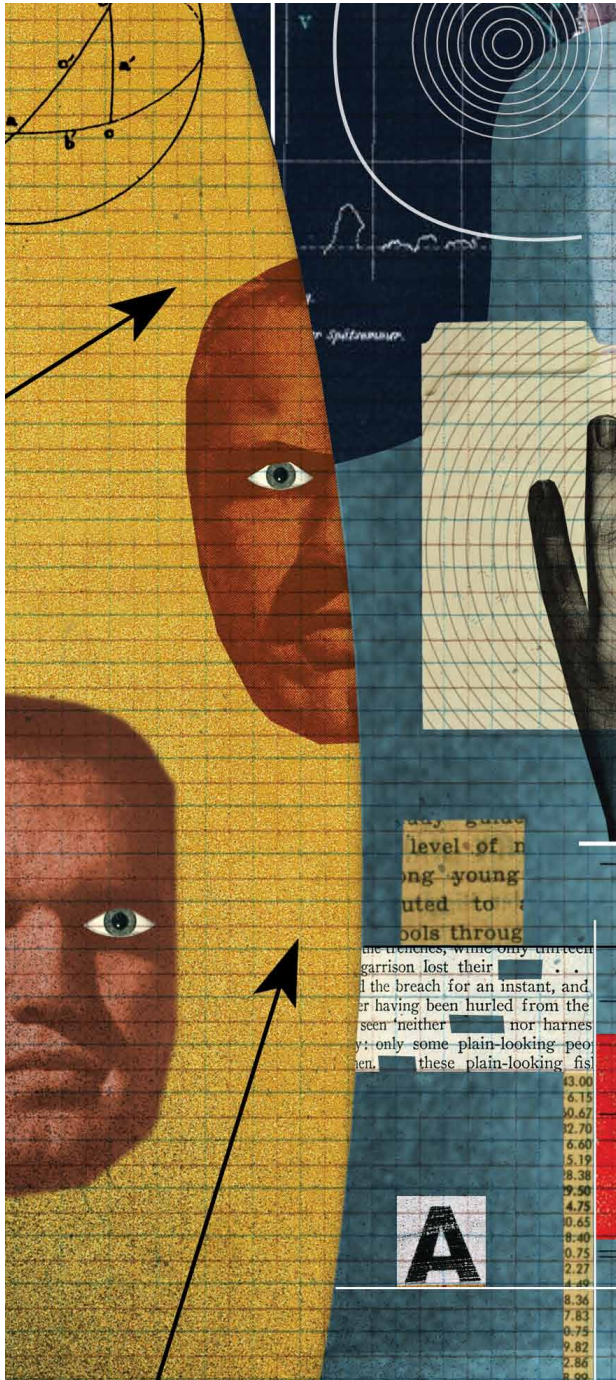
7033

iapp



"Looking Ahead" by David Plunkert





# CONTENTS

**About the IAPP** ..... iii

**Introduction** ..... iv

**Note from the Chairman of the IAPP Board of Directors**  
*Justin Weiss, CIPP/A, CIPP/E, CIPP/US, CIPM, FIP*

**Privacy: Here to Stay and Stronger than Ever**  
*Omer Tene*

**Author Biographies** ..... viii

## 2020: Visions of Privacy Anthology

**The Preservation of the Right to Reasonable Levels of Personal Privacy** ..... 1  
*Julie Brill*

**A View from 2030** ..... 5  
*John Edwards*

**IAPP at 20: Expectations for Privacy in the Year 2030** ..... 10  
*Elizabeth Denham*

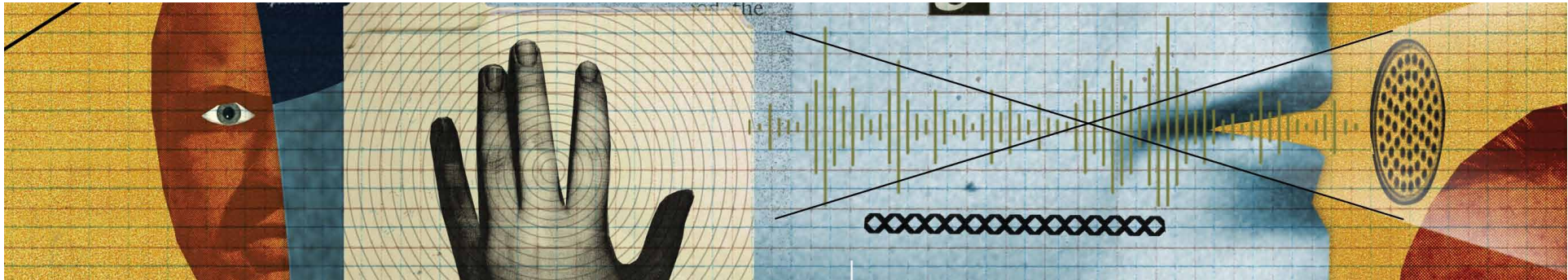
**2030: The Decade of Individual Control and Choice** ..... 14  
*Teki Akuetteh Falconer*

**The Universe of the Privacy Professional: Star Date 2030** ..... 15  
*Genie Barton*

**The Demand to be Forgotten and Its Associated Challenges** ..... 18  
*Heather Dean Bennington, CIPP/US*

**Privacy in 2030 Means Hitting the Off Button** ..... 20  
*John Bowman, CIPP/E, CIPM, FIP*

**An Idea Whose Time Has (Finally) Come** ..... 22  
*Lorrie Faith Cranor, CIPT*



CONTENTS

**In Hindsight: The Global Impact of the GDPR** ..... 24  
*Andrew Clearwater, CIPP/US*

**Seen But Not Herded** ..... 26  
*Ian Cooke, CIPP/E, CIPM, CIPT, FIP*

**Privacy, Evolved..** ..... 28  
*Barbara Cosgrove*

**Human Rights Coupled with Fiduciary Duties** ..... 30  
*Christopher Hart, CIPP/E, CIPP/US, CIPM*

**The Range of Responsibility** ..... 32  
*Peter Hustinx*

**My Privacy Robot** ..... 34  
*Jules Polonetsky, CIPP/US*

**Making the Grade: Privacy as Core Curriculum**..... 36  
*Alexandra Ross, CIPP/E, CIPP/US, CIPM, CIPT, FIP, PLS*

**No Hiding: When Personal Data Becomes Identified** ..... 38  
*Laura Tarhonen, CIPP/E*

**Privacy Assistance Beyond the Speed of Thought** ..... 40  
*Alexander White, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP*

**Privacy Law Will Become More Specialized in 2030** ..... 43  
*Christopher Wolf*

**An Anthology of Privacy Predictions** ..... 45  
*Stephen Kai-yi Wong*



# About the IAPP

The International Association of Privacy Professionals is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers and organizations manage and protect their data.

The IAPP is a not-for-profit association founded in 2000 with a mission to define, support and improve the privacy profession globally. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the only globally recognized credentialing programs in information privacy: the Certified Information Privacy Professional (CIPP®), the Certified Information Privacy Manager (CIPM®) and the Certified Information Privacy Technologist (CIPT®). The CIPP, CIPM and CIPT are the leading privacy certifications for thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice. //





# Introduction



## Note from the Chairman of the IAPP Board of Directors

**Justin Weiss, CIPP/A, CIPP/E, CIPP/US, CIPM, FIP**

*Global head of data privacy, Naspers*

Curiosity about the potential to leverage volumes of data through artificial intelligence to enhance, supplement or even displace humans' roles in making accurate predictions for themselves is on the ascendant. In light of COVID-19 and many people's difficulty in managing themselves through it, some kind of robot intervention to help us navigate an uncertain future actually sounds appealing. Siri, Alexa, Watson — if you are listening — please do intervene. As human beings we are clearly confounded when we experience something that wasn't anticipated, or rather, hadn't been given sufficient weight at a time when we could've planned better for it. We are most gratified when we spend our emotional and physical

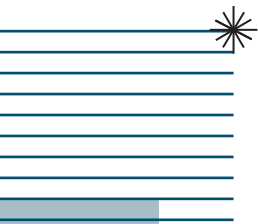
capital planning for endeavors that actually come to pass.

We privacy professionals have our own special relationship with human predictions because we are constantly being asked to make them. Among our tasks, we try to anticipate how people will feel about the way their personal data is to be collected, used and retained, by whom, in different contexts. We are asked to foresee and explain how data protection regulators will respond to various novel scenarios. We try to assign risk ratings to future events, and we advise on how the stuff of news cycles ought to translate into actionable changes within companies and in governments. As our profession con-

tinues to mature, we are actively learning how to refer to risk management, data protection laws, ethics, our understanding of media, technology, engineering, businesses and governments to do this work.

With the IAPP marking its 20th anniversary in the midst of an extraordinary 2020, it is a perfect time for privacy professionals to take stock of where we are and project forward to anticipate what the next decade could look like in privacy and data protection. That's why we've put together this document, "Visions of Privacy," which is filled with thought leadership and predictions for what the next 10 years might bring.





As recent history has shown, intervening events will certainly have a major impact on our privacy trajectory. As we look back at the IAPP's predictions in 2010, no one flagged the likely emergence of Edward Snowden and the effect his revelations about U.S. government surveillance would have on the EU-U.S. Safe Harbor Framework or the broader public awareness of personal privacy. Similarly, no one's gut told them a Cambridge Analytica-style scandal would elevate to the forefront questions about the impact of social media on democratic elections and the risks associated with unfettered third-party access to data. Instead, certain people predicted that RFID chips would be the big issue of the decade, while others thought that concerns about "do-not-track" features might have been resolved by now.

Even as we entered into this new decade just a few short months ago before the pandemic spread across the world, the talk in many privacy circles centered

on privacy legislation in the United States and the likely outcome of the "Schrems II" decision in the Court of Justice of the European Union. Many were focusing on the implementation of Brazil's data protection law and the prospect of national privacy legislation in India. We were just wrapping our heads around a "CCPA 2.0" endeavor announced on stage at the IAPP's Privacy. Security. Risk. conference in Las Vegas last year. And yet, today, in light of COVID-19, we're now vigorously debating how best to build privacy into contact-tracing apps and considering antibody passports in earnest!

All of this to say that we should, I think, be gentle with ourselves when some of our predictions don't come to pass on the timeline we expect simply because they are superseded by major events, or — put differently — we lacked access to what would turn out to be the most relevant data at the time. All of these debates are important and will remain so. While the

weight that will be given to each of them may well shift in light of political, social, environmental and other major events, what will not change is that human values are at the center of what we highlight as privacy professionals. Technology will continue to evolve. Data breaches will still happen. Regulators will continue to enforce the law. Privacy will still matter to humans, whose rights we work to protect.

In light of this year's COVID-19 turbulence, a friend of mine posted online that the expression "20/20 hindsight" has revealed its true meaning. Perhaps we can reclaim this expression and also embrace what it means to have 20/20 foresight: anticipating and preparing for what may come while remaining ready to pivot in light of change. We hope you enjoy this compendium of thinking from some of the brightest leaders and visionaries in privacy and data protection and that it assists you in your own preparedness to navigate our future as part of the IAPP. //



# Privacy: Here to Stay and Stronger than Ever

## **Omer Tene**

*IAPP vice president and chief knowledge officer*

Twenty years ago, when I started my career in privacy and data protection, few people I met knew what it meant. When I told someone I'm in the field of privacy, I'd typically get a blank look. Or at best, folks would say, "Ah, that's data security. Yes, I have a cousin who works in IT." Having been a corporate lawyer before then, I was used to a very different response. If I said I'm in corporate law, I'd typically be asked, "What kind of corporate lawyer are you?" Are you in mergers and acquisitions or bankruptcy, structured finance or private equity, banking or litigation? People would get it.

In 2020, few people are dismissive about the importance of

privacy and data protection as a policy matter, profession, discipline and field. Today, when I say I work in privacy, people's eyes light up. They conjure online websites and social networks, creepy ads and intrusive home devices, consumer genetics and personal finance. And the list goes on. Everyone has their favorite privacy story, concern, gripe or fascination. No doubt, privacy and data protection have arrived.

Indeed, even at a time of a pandemic, which sows disease, death and economic devastation around the globe, privacy remains front and center. Nations try to deploy data to fight the pandemic? Hold on,

what are the privacy implications? Contact tracing through mobile apps? But wait, what about privacy? Antibody passports to facilitate restarting the economy? First, let's handle concerns about privacy and algorithmic accountability. Employees working from home? Are the platforms they're using privacy compliant and secure? Going back to work in the office? Can the employer take your temperature and ask about symptoms? To be sure, the pandemic may push new issues to the fore and challenge privacy but not set it aside.

Looking 10 years down the road, I'm convinced privacy and data protection will only expand. In





2030, when someone tells you they're a privacy professional, it'll be like me saying I'm a corporate lawyer back in 2000. You'll ask, what kind of privacy professional are you? In privacy law, compliance or engineering? Specializing in employment issues, civil rights or consumer matters? Are you a privacy professional dealing with cross-border data transfers or one handling data ethics and researchers' access to data? An engineer integrating privacy into product design or a designer creating user interfaces for newly engineered devices? Do you deal with privacy in Brazil, Japan and South Africa or with health care and breach notification in the U.S.?

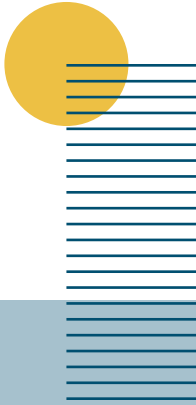
Already today, more than 500,000 organizations in the European Union registered as having data protection officers. In the United States, federal legislative efforts included requirements for every mid- to large-sized company to appoint a chief privacy officer. Eventu-

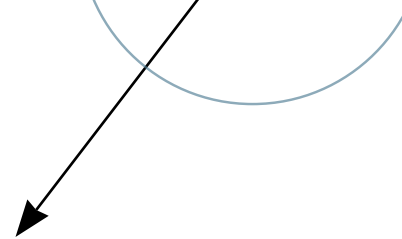
ally, this will result in hundreds of thousands of new roles. Some corporate privacy programs employ hundreds — or in a few cases, thousands — of employees. Those professionals are embedded in product teams and accompany development processes from the start. They conduct risk assessments, map data flows, vet vendors in procurement projects, report to the board of directors and make filings to the stock market.

In any job market, pre- or post-crisis, such tremendous opportunity beckons. And this is a field defined by diversity of disciplines and thoughts. The privacy body of knowledge, the canon of privacy, is not yet set in stone. It will comprise courses and modules from both sciences and the humanities, including law, ethics, economics, software engineering, cybersecurity, computer science and math. To create it, we will need to catalyze academic institutions to vastly enhance their

capacity to research, educate and train in privacy.

This compendium includes contributions by leading privacy voices from academia and government, industry and civil society, all around the world. Together, they reflect on how far we have come as a profession over the past two decades and what the future might hold. Constantly renegotiated as a social norm at the cutting edge of new technologies and business models, privacy has never been easy to predict. With some of the largest technology companies in the world less than 20 years old, who could have foreseen the issues raised by search and social networks, cloud and online commerce, let alone genetic testing and facial recognition, 20, 10 or even 5 years ago. As you read the following pieces, think of what you see coming for our field and how best your organization and our community can adapt and prepare for the challenges ahead. //





# Author Biographies



## ***Julie Brill***

Julie Brill is corporate vice president, deputy general counsel for privacy and regulatory affairs, and chief privacy officer at Microsoft Corporation. In this executive leadership position, Brill is at the forefront of many of the regulatory issues that underpin the digital transformation, leading the global policy and legal discussions involving privacy, internet governance, telecommunications, online safety, hate speech, accessibility and corporate standards. She is spearheading Microsoft's preparations for the EU General Data Protection Regulation, as well as other privacy mandates around the globe. Brill has a key role in Microsoft's interactions with regulators and policymakers developing regulations and standards around the world.

## ***Elizabeth Denham***

Elizabeth Denham became the U.K.'s Information Commissioner in 2016. The Information Commissioner's Office is the UK's regulator for data protection and information rights. It enforces the law, both civil and criminal, against organizations that have violated data protection rules. The ICO provides guidance on and regulates key laws, such as the EU General Data Protection Regulation, Data Protection Act 2018, the Privacy and Electronic Communications Regulations, and Freedom of Information Act 2000.

## ***John Edwards***

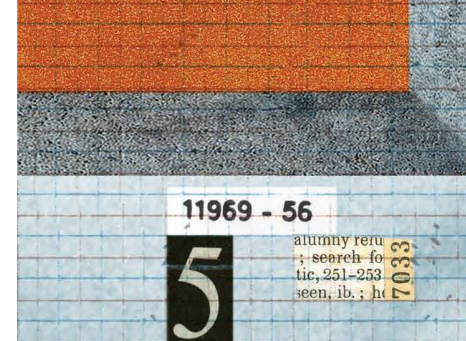
John Edwards was appointed to the independent statutory position of Privacy Commissioner of New Zealand in February

2014 for a term of five years. He provides independent comment on significant personal information policies and issues. Prior to his appointment, Edwards practiced law in Wellington for more than 20 years, specializing in information law while representing a wide range of public and private sector clients. He has acted in legal roles for the Ministry of Health, State Services Commission, Department of Prime Minister & Cabinet, and Inland Revenue Department. For 15 years, he held a warrant as a district inspector for mental health and has also been a district inspector for intellectual disability services.

## ***Teki Akuetteh Falconer***

Teki Akuetteh Falconer is a senior partner at Nsiah Akuetteh & Co., as well as founder and





executive director at the Africa Digital Rights' Hub. She is privacy and data protection consultant and has previously worked for the government of Ghana in facilitating the development of several key legislations for the ICT sector, including the National Communications Act, 2008 (Act 769), Electronic Communications Act, 2008 (Act 775), Electronic Transactions Act, 2012 (Act 772), and the Data Protection Act, 2012 (Act 843). She also worked in various capacities with regional bodies, such as ECOWAS. She was the first executive director of the Data Protection Commission to facilitate the implementation of Ghana's Data Protection Act.

### **Genie Barton**

Genie Barton is founder and principal at Privacy Genie, a consultancy focused on privacy and related data-use issues. With more than 25 years of experience

in privacy, technology, telecommunications and digital advertising in the private sector, federal government and not-for-profit sectors, Genie is uniquely positioned to offer strategic advice to companies or investors looking for practical guidance and fresh insights on current and emerging challenges and opportunities in the 21st-century digital ecosystem.

### **Heather Dean Bennington, CIPP/US**

Heather Dean Bennington is vice president in the Global Privacy Compliance team at BNY Mellon and is focused on providing data protection expertise to help manage the business risks and regulatory requirements associated with personally identifiable information. Prior to BNY Mellon – Pershing, she worked in MetLife's Corporate Privacy Office. She also has experience as an IT auditor, both from an internal and external standpoint.

### **John Bowman, CIPP/E, CIPM, FIP**

John Bowman is a senior principal in Promontory's privacy and data protection team. Bowman advises clients on all aspects of compliance with data protection laws and regulations. Prior to joining Promontory, John worked at the U.K. Ministry of Justice, where he was the government's lead negotiator on the EU General Data Protection Regulation. This work involved leading the U.K. delegation to the Council of the European Union's DAPIX expert working group in Brussels, developing the government's policy position on the GDPR, engaging with a wide range of stakeholders and advocates, and regularly briefing ministers.

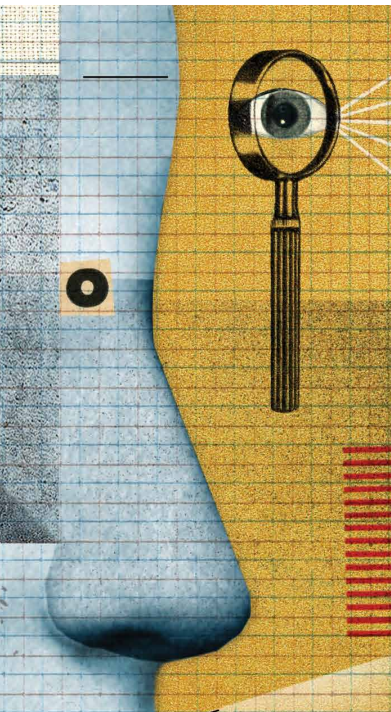
### **Lorrie Faith Cranor, CIPT**

Lorrie Faith Cranor is the director and Bosch distinguished professor in security and pri-

vacuity technologies of CyLab and the FORE Systems Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University. She also directs the CyLab Usable Privacy and Security Laboratory and co-directs the MSIT-Privacy Engineering master's program. In 2016, she served as chief technologist at the U.S. Federal Trade Commission, working in the office of Chairwoman Edith Ramirez. She is also a co-founder of Wombat Security Technologies, a security awareness training company. She has authored more than 150 research papers on online privacy, usable security and other topics.

### **Andrew Clearwater, CIPP/US**

Andrew Clearwater serves as vice president of privacy at OneTrust. Clearwater is a Certified Information Privacy Professional, holds an LLM in Global Law and Technology, and is a



licensed attorney. In his role as director of privacy, Clearwater provides counsel, leadership and guidance on data protection. Clearwater is also responsible for providing public policy analysis in the areas of privacy, data security, information policy and technology transactions. Clearwater is a globally recognized privacy thought leader and has spoken at many of the world's leading privacy conferences on behalf of OneTrust.

***Ian Cooke, CIPP/E, CIPM, CIPT, FIP***

Ian Cooke is the group IT audit manager with An Post (the Irish Post Office) based in Dublin, Ireland, and has 30 years of experience in all aspects of information systems, particularly in areas related to governance, risk, control, audit, compliance, process improvement, information security

and privacy. Cooke has served on several ISACA committees, including exam item development. He has also supported the update of ISACA study materials and was a subject matter expert for the development of ISACA online review courses. He is the recipient of ISACA's 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules and is currently a columnist for the ISACA Journal.

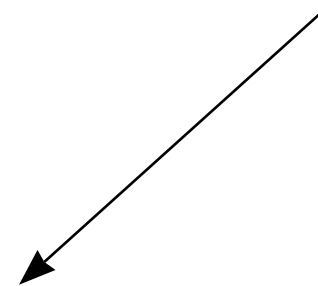
***Barbara Cosgrove***

Barbara Cosgrove is vice president and chief privacy officer at Workday, responsible for Workday's global privacy, ethics, and compliance strategy and operations. Cosgrove has extensive expertise in managing international data protec-

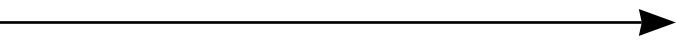
tion compliance programs and implementing data governance policies, technology compliance standards and programs, and privacy-by-design frameworks. She has also served as the chief security officer for Workday.

***Christopher Hart, CIPP/E, CIPP/US, CIPM***

With significant trial litigation, appellate advocacy and cybersecurity experience, Chris Hart has counseled and represented sovereign nations, Fortune 500 companies, startup companies, nonprofits and individuals in a wide variety of contexts for more than a decade. He represents clients before the U.S. Supreme Court, argues in appellate courts across the country, including successfully before the Massachusetts Appeals Court and Supreme Judicial Court, and advocates on behalf of clients in federal and state courts nationwide.







***Peter Hustinx***

Peter Hustinx was the first European Data Protection Supervisor from January 2004 until December 2014. From 1991 until 2004, he was president of the Dutch Data Protection Authority, and from 1996 until 2000, he was also chairman of the Article 29 Working Party. He has been closely involved in the development of data protection law from the start, both at national and various international levels. He received law degrees in Nijmegen, the Netherlands, and in Ann Arbor, Michigan, U.S. In July 2015, he received an honorary doctorate from the University of Edinburgh for his work in the field of information privacy and data protection.

***Jules Polonetsky, CIPP/US***

Jules serves as CEO of the Future of Privacy Forum, a nonprofit organization that serves as a

catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF is supported by the chief privacy officers of more than 130 leading companies and several foundations, as well as by an advisory board comprised of the country's leading academics and advocates. FPF's current projects focus on big data, mobile, location, apps, the internet of things, wearables, deidentification, connected cars and student privacy.

***Alexandra Ross, CIPP/E, CIPP/US, CIPM, CIPT, FIP, PLS***

Alexandra Ross is the founder of The Privacy Guru and director of global privacy and data security counsel at Autodesk, a leader in 3D design, engineering and entertainment software. Previously, she was senior counsel at Paragon Legal and associate general counsel for Wal-Mart

Stores. She is a certified information privacy professional (CIPP/US, CIPP/E, CIPM, CIPT and FIP) and practices in San Francisco, California. She holds a law degree from Hastings College of Law and a B.S. in theater from Northwestern University.

***Laura Tarhonen, CIPP/E***

Laura Tarhonen is a technology and data enthusiast with a strong focus on privacy and data protection. Currently she works as a data privacy leader at the group functions of the global retailer IKEA, where she supports data privacy activities in the European markets. Before joining IKEA, Tarhonen worked with managing the companywide privacy program of Finland's biggest media company, Sanoma. Her background is in law with a master's degree from the University of Helsinki. She also has some experience in working for





the public sector. She has both worked for the Finnish Data Protection Authority (Data Protection Ombudsman's Office) and Ministry of Transport and Communications. In the Communications Ministry, she worked on the big renewal of the Finnish telecommunications law, e-privacy and governmental surveillance initiatives.

***Alexander White, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP***

Alex White is currently the privacy commissioner for Bermuda. Prior to this, Alex was deputy chief privacy officer for the U.S. state of South Carolina, where he served as a state subject-matter expert on privacy. His office supported privacy compliance and best practices for more than 70 state agencies and entities. Prior to that, White worked in the insurance industry in emerging issues,

enterprise risk management, regulatory compliance, government affairs and product development, including drafting and review of cyber liability forms. In addition to his IAPP certifications, he holds a variety of privacy, legal, cybersecurity and risk management qualifications and is a two-time graduate of the University of Georgia, where he earned a bachelor's degree in history and a Juris Doctor.

***Christopher Wolf***

Christopher Wolf is senior counsel in the Privacy and Information Management practice at the law firm of Hogan Lovells US and previously led the practice as a partner. Wolf focused on internet and privacy law since the early days of those disciplines. He is founder and board chair of the Future of Privacy Forum and a recipient of the IAPP Vanguard Award, among other recognitions.

***Stephen Kai-yi Wong***

Stephen Kai-yi Wong is the current privacy commissioner for personal data in Hong Kong. Prior to joining the PCPD, Wong was a practicing barrister in private practice and secretary to independent advisory body the Law Reform Commission of Hong Kong. Before serving at the LRC, Wong had been a legal counsel in the Department of Justice from 1986 to 2007 (the then-Attorney General's Chambers before 1997), assuming various posts, including assistant director of public prosecutions and deputy solicitor general. Being an expert in human rights law, he was involved in the legislative process of the 1991 Hong Kong Bill of Rights Ordinance and was subsequently on loan to the United Nations Human Rights Committee in Geneva for one year until 1992. //



# The Preservation of the Right to Reasonable Levels of Personal Privacy



**Julie Brill**

*Microsoft corporate vice president and general counsel*

The internet has changed so many things so dramatically in the 20 years since the IAPP was founded that it's easy to forget just how new the online world still is. Back then, it had only been a few years since America Online switched from charging by the hour for internet access to billing monthly. The web browser was still a relatively new invention. PayPal and Google search were just two years old. Facebook and the smartphone had yet to be invented.

At the time, people were mostly thrilled just to be able to browse a new thing called the World Wide Web. Even the most casual computer user couldn't help but

be excited by the possibilities, which promised a new era of unlimited access to information, powerful new ways to communicate, and incredible opportunities to transform how people work, shop and play.

But for those of us who were paying closer attention, many of the potential perils were already apparent. From my vantage point working on consumer protection issues in the Office of the Vermont Attorney General, it quickly became obvious that all the personal data generated by internet searches, contained in emails and embedded in online shopping transactions, posed new threats to one of the core tenets



*The unprecedented speed and scale of technology innovation and progress in our era has meant new features and capabilities run ahead of the controls and laws we rely on to protect privacy.*

of society — the preservation of the right to reasonable levels of personal privacy.

In those days, online privacy was largely an afterthought. Based on an opt-out model that asked consumers to read long, impenetrable privacy statements, it was more about preventing litigation than preserving privacy. This placed the burden squarely — and unfairly — on consumers, who almost invariably accepted all the risks detailed in the documents they almost certainly didn't read.

I wasn't the only one who could see this model was inadequate to the task of protecting privacy. Across the world, a small but growing movement of consumer advocates, privacy experts, government regulators and technology leaders recognized a lot was at stake and the task of finding the right balance between technological progress and privacy

protection was going to require a lot of new thinking and hard work. One question many of us were asking in the late '90s was how we could turn this informal movement into something more organized and effective. It was clear we needed vigorous forums for our discussions, as well as a clearinghouse for information and a place where privacy professionals could develop their skills and advance their knowledge.

Since 2000, the International Association of Privacy Professionals has been a large part of the answer to this question. Through its training, certification programs, rich slate of conferences, comprehensive research and resources, the IAPP and its members have advanced privacy practices and protections around the globe. In addition to that important work, the IAPP has helped businesses and governments understand that protecting privacy is vital to

earning trust in technology and an essential foundation for thriving businesses, immersive consumer experiences and healthy economies.

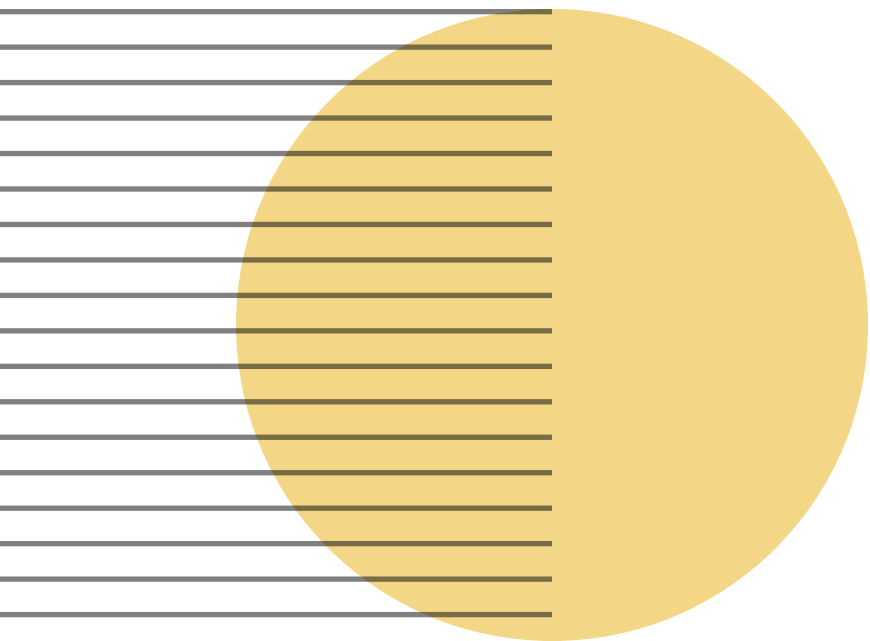
It hasn't always been easy. The unprecedented speed and scale of technology innovation and progress in our era has meant new features and capabilities run ahead of the controls and laws we rely on to protect privacy. So much of what we've been dealing with over the last decade or more simply didn't exist in 2000. Mobile phones, networks of sensors and smart devices generate once-unimaginable volumes of

data about who we are, what we like, where we go and what we do. With cloud computing and artificial intelligence, all that data can be stored, analyzed and used in myriad ways. Much of it is beneficial; some of it is not.

Along the way, we in the privacy world have found ourselves responding to seismic events, from the release of classified documents by Edward Snowden, to the decision invalidating Safe Harbor, to the Cambridge Analytica Scandal. There's a reason why we think of ourselves as being on the frontlines of privacy. At times, it feels like preserving the right to privacy



*Today, as the amount of personal data generated continues to grow exponentially and as AI continues to create new opportunities for progress (and raise new risks for privacy), the work of the IAPP is critical.*



is a series of rumbling tremors interrupted occasionally by much larger earthquakes.

But if it hasn't always been easy, it has always been deeply interesting and richly rewarding. Over the past two decades, I've been involved with the IAPP while working to promote privacy in the United States and internationally, through state governments, as a commissioner of the U.S. Federal Trade Commission, as a privacy lawyer in private practice, and now in my role as corporate vice president, deputy general counsel and chief privacy officer at Microsoft. I was fortunate to help lead the discussions that paved the way to the EU-U.S. Privacy Shield that replaced Safe Harbor and advocate for new ways for consumers to regain control of their privacy, like the "Reclaim Your Name" initiative to bring more transparency to the practices of data brokers. Every step of the way, my

colleagues at the IAPP have been an incredible source of insight, information and inspiration, and I have come to count many of them among my closest friends. It was an incredible honor to receive the Privacy Leadership Award in 2014.

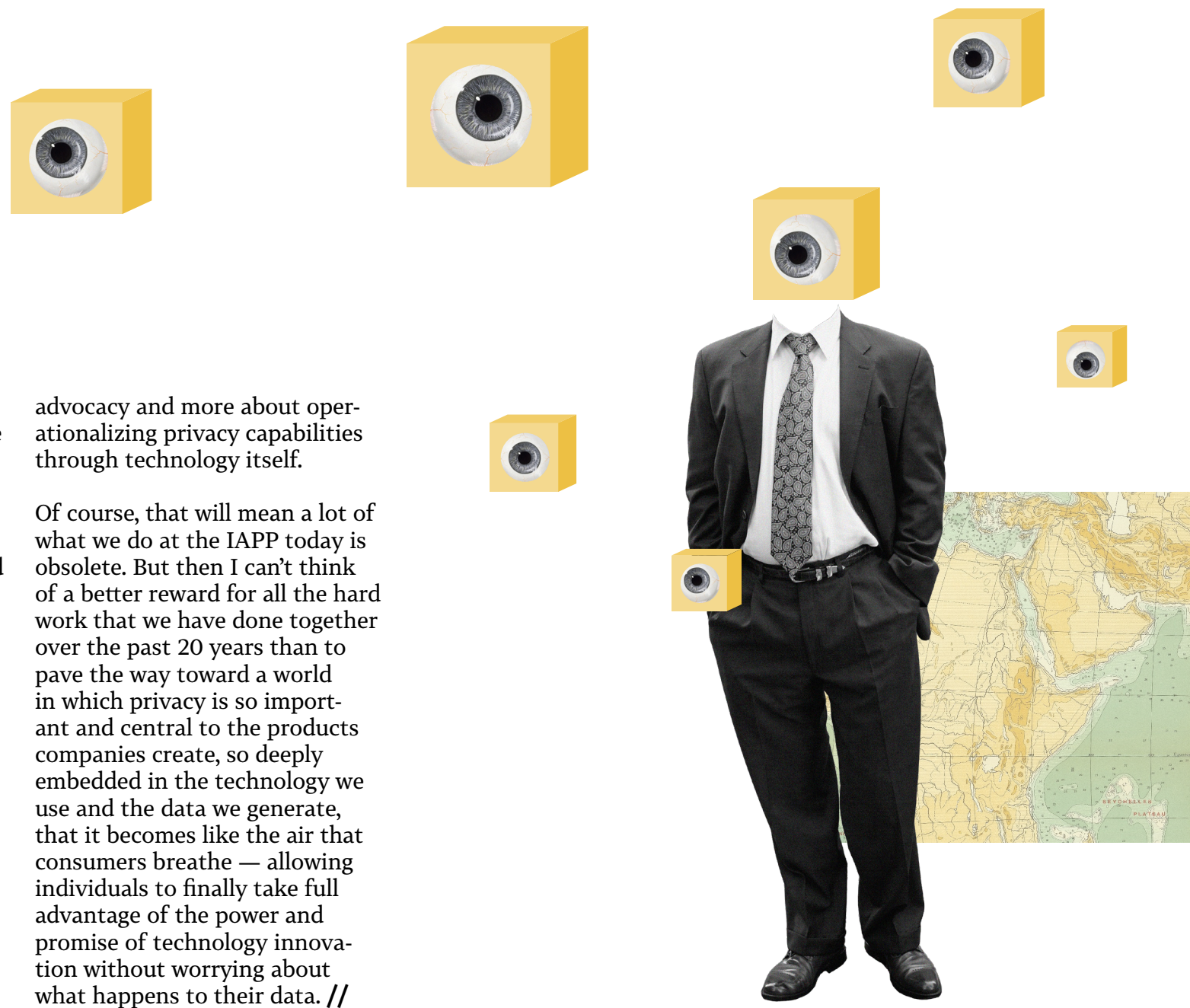
Today, as the amount of personal data generated continues to grow exponentially and as AI continues to create new opportunities for progress (and raise new risks for privacy), the work of the IAPP is critical. What I said five years ago when I accepted the Privacy Leadership Award is even more salient: "We need to do more. ... The potential benefits of our new technological age are clear, but so are the risks to our economic and social well-being if we cannot exercise appropriate control over our data."

I can already envision a different future for the world of privacy. Clearly, we still need new laws,

particularly in the U.S., where we have yet to establish baseline privacy protections at the federal level. But I believe that by 2030, it's possible that privacy will look a lot more like what security looks like today. Instead of trying to account for privacy through governance models — and asking consumers to read those hated privacy disclosure documents — privacy protections will be built into data and systems and managed automatically. By then, I expect more companies will see privacy as a critical competitive differentiator and privacy protection as an area of technical innovation in which they constantly strive to top each. In that world, the task for the IAPP and its members would be less about policy and

advocacy and more about operationalizing privacy capabilities through technology itself.

Of course, that will mean a lot of what we do at the IAPP today is obsolete. But then I can't think of a better reward for all the hard work that we have done together over the past 20 years than to pave the way toward a world in which privacy is so important and central to the products companies create, so deeply embedded in the technology we use and the data we generate, that it becomes like the air that consumers breathe — allowing individuals to finally take full advantage of the power and promise of technology innovation without worrying about what happens to their data. //





# A View from 2030

**John Edwards**  
New Zealand privacy  
commissioner

## Option A

*Some say it started with the EU General Data Protection Regulation, but in truth, the seeds were sown a decade before 2017.*

The tech companies had begun aggregating and monetizing personal information, habits and behaviors in stealth in the early part of the century. When consumers were given the chance and tools to own personal information, they leapt at it with no thought given to the consequences. How could they? They had no idea what was to come.

People invited eavesdropping devices into their houses and connected their toasters, cars and beds to the internet. They watched their local and central government, in collusion with the tech industry, attach sensors



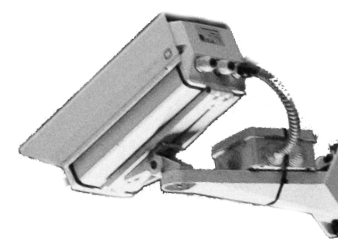
## Option B

*It was less of a “great awakening” than a gradual dawning.*

For years, consumers had seized the convenience and efficiencies the tech companies had offered. There was no question that the games, tools, networks and ability to communicate had improved lives and the economy. For a time, it seemed like these society-wide benefits came at little or no cost; it suited many to perpetuate a state of blissful ignorance.

The negative externalities of the attention economy, surveillance capitalism and digital dystopia (the headline writers were endlessly inventive) were obvious by the mid-2000s, but by 2020, there were few people left arguing that the market was capable of





# Option A

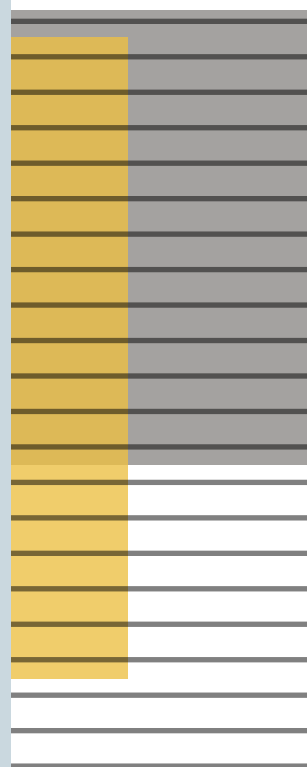
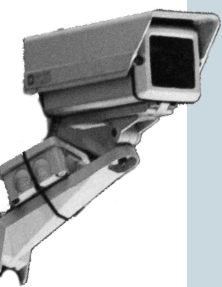
to everything — all under the vague promise that “data will make you free.”

The GDPR, California Consumer Privacy Act, U.S. Federal Privacy Protection Act and dozens of other regulations that sprung up around the world were reactions to the rapacity of the digital oligarchs and their, so far, successful strategy of playing nation states and regulators off against each other, all the while keeping consumers in the dark.

But it was already too late. The tough regulations did more harm than good. We see that now, but at the time, politicians and regulators were desperate to shut the stable door behind an already-bolted wild stallion.

The regulations confused the public and locked in the monopoly status of the digital robber barons, who were the only ones who could afford the prohibitive compliance costs. The innovation needed to challenge them was choked out; their economic rents soared, and they paid their billion-dollar fines with loose change.

The politicians patted themselves on the back with each new “enforcement action,” and the companies continued to bankroll and “Astro-



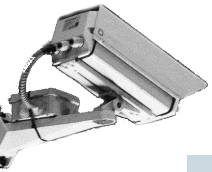
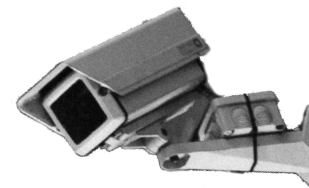
# Option B

correcting the excesses of digital industry without government intervention and tough regulatory action.

Those pushing for reform harkened back to the antitrust era in which the robber barons’ stranglehold on their monopolies was broken up with enormous, if belated, benefit to the economy. They needn’t have gone so far back. The IT industry had its own much more recent and equally successful example in the Microsoft antitrust actions of the 1990s.

The combination of increased regulatory action (from antitrust, consumer protection, data protection, electoral integrity authorities internationally) and heightened consumer awareness and demand led to a proliferation of privacy promoting technologies and business models.

The transparency imposed on platforms to account for their targeting and assumptions about the characteristics, traits and frailties of consumers exposed inherent biases and supported increasingly vocal calls for greater consumer protection. This feedback loop — resisted for years as companies sought to conceal their flawed proprietary algorithms — ultimately improved the quality of the



## Option A

## Option B

Turf feel” good nongovernmental organizations and policy shops to give the illusion of social responsibility.

What the companies didn’t already know about us, they could infer. What they didn’t fully understand was that much of what they thought they knew was a product of their own biased feedback loops. “You looked at this? Have some more of it, here; these guys are into that, too; you belong together. People like you also like this kind of stuff.” They were creating a society in their own image, but like Dorian Gray, it was the image in the attic, rather than the one in the parlour.

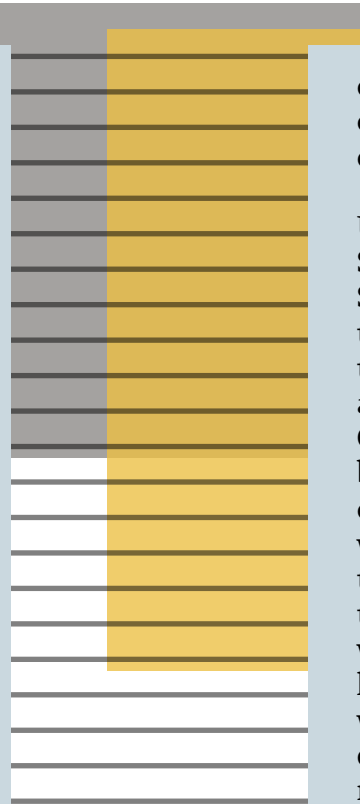
The election interference prototyped in 2016 in the U.K. and U.S. became standard operating procedure, despite efforts to enforce transparency and regulate political advertising. One study in 2025 showed that almost every voter in the 2024 U.S. elections received targeted political advertisements, and no two ads were the same!

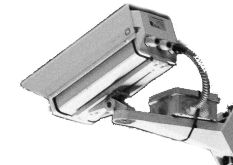
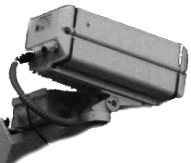
Democracies became marketplaces in which the ability to influence voters was optioned to the highest bidder. When prohibitions on targeting ethnic or economic microsegments

commercial offerings and reduced the harms caused by overconfident Silicon Valley snake-oil sales people.

Until the International Treaty on Privacy, Security, Consumer and Citizen Rights and State Responsibility was concluded in 2026, there remained a disparity in the application of privacy laws between holdouts China and Russia, and the Asia-Pacific Economic Cooperation, EU and Americas trading blocks. The international talks revealed all countries had far more in common than that which divided them. Each state committed to respect privacy and protect citizens’ data to a common standard, except where access was required for legitimate, proportionate, law enforcement and security purposes and was in accordance with recognized standards and the Rule of Law. Governments now submit audited annual reports demonstrating their conformance with their international obligations.

With access to quantum computing classified under international treaties as strategic technology and therefore restricted to governments and licenced researchers, secure encryption against government access was rendered a thing of the past. Even the most





## Option A

was outlawed, the artificial intelligence simply suggested proxies that enabled parties and hostile state actors to foment and exploit rivalries and discord.

It became impossible to know who was behind the advertisements. Ads purportedly promoting political candidates were sometimes produced by rivals, using “deepfakes” to suggest positions inconsistent with the views of the candidate’s base.

Governments, having half-heartedly attempted to slow the digital juggernauts, pivoted recognizing the value of the data stores and ability to monitor and anticipate the behaviors of the populace. Facial-, gait-, iris- and voice-recognition systems meant a handful of tech giants knew where each of us was at every moment. The existing datasets, combined with AI and the real-time floods of data gushing along the networks, meant they knew what we were doing, why and what we would do next. This became irresistible to law enforcement agencies and social engineers who forced the commercial operators of the surveillance infrastructure into a Faustian bargain. The social credit system trialled in China in the early 2020s became ubiquitous internationally.

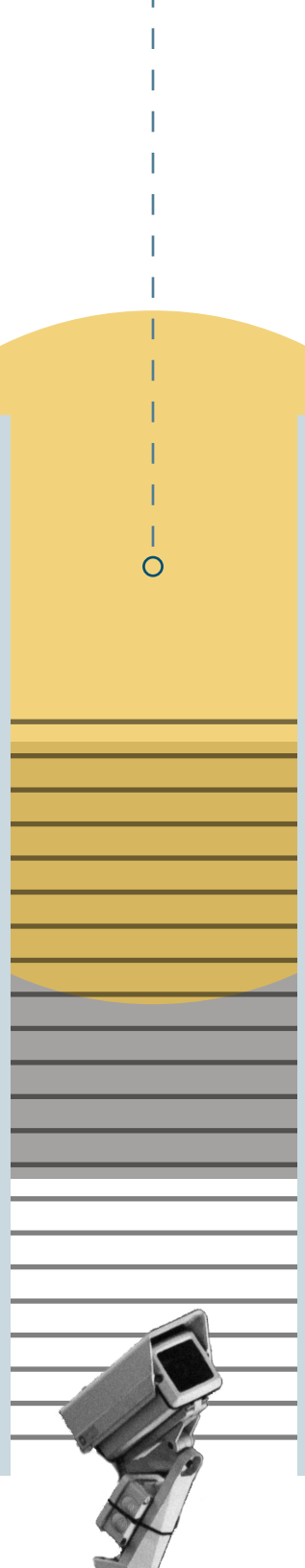
## Option B

libertarian of privacy advocates recognized the compromise of limited access, overseen by competent judicial authority and kept honest by regularly published reports and user access notifications, was better than the open slather that had operated in the pre-Snowden era and the cat-and-mouse chase of encryption technology and law enforcement that followed.

But the real change was the shift of power from those who offered services in exchange for data to the individual controlled, decentralized, self-sovereign ID. This allowed individual consumers to interact with a variety of providers without any one of those services aggregating data relating to all the others.

The shift led to a proliferation in the marketplace of consumer-oriented tools to securely manage the dissemination of a user’s identity.

With tech companies having to acknowledge the value of the data of which they were now being deprived, they were forced into a more open and transparent bargain with the consumers. They had to commit to a set of restrictions and benefits to have the opportunity to present more products or services to the





## Option A

Privacy had become a scarce commodity. A market of sorts developed, allowing those with the means and the wherewithal to protect what was left. But that was a chimera — the more they opted out, the more attention they drew to themselves. Law enforcement and intelligence agencies were suspicious, and industry was anxious to find ways of exploiting that market. There was no escape.

Which is how we got to where we are now, in 2030: open, surveilled, predicted, manipulated, anxious, vulnerable. //

## Option B

consumer. If they failed to honor that commitment, the consumer could, with a sequence of winks, delete all data the company held or move it to a more suitable provider.

With the data markets finally operating more efficiently and with entry and exit seamless and effortless for both consumers and suppliers, the need for the tough enforcement action required to reach this state has receded. The talk is once again, “Should industry be given a freer rein?” It will be interesting to see where this talk leaves us in 2040. //

**Choose One:**

**Future A**

**Future B**



# IAPP at 20:

## Expectations for Privacy in the Year 2030

**Elizabeth Denham**

*U.K. information commissioner*

Hover boards, flying cars and security cameras that instantly recognize your face. When we start to think about how the future might look, it's easy to stumble toward a vision that's half-Hollywood sci-fi and half-Orwellian nightmare.

The reality will be somewhat different. 2030 isn't all that far away, and if we reflect on the past decade of data protection, we see steady evolution rather than dramatic step-change.

History has shown us that the big questions we grapple with today will feel old fashioned 10

years from now. It often takes the passage of time to come to a realization that something we take for granted every day isn't, in fact, OK — single-use plastics being a recent example. I think we'll see something similar happen with how we protect children online.

The challenge regulators and lawmakers face today is how to change an internet built for adults but used by children. How to change a culture of online services and games that use sophisticated techniques to keep children hooked, of apps and websites that gather and share children's





data as a matter of course. But I think we'll see this very differently in 2030. We'll find it strange to imagine a time before design solutions to protect children and their data online. Online services will look very different for the children of 2030, and our expectations of what is normal and acceptable will have changed.

We'll have a similar view of advertising technology and real-time bidding. We'll look back at how strange it was that a system developed that involved sharing huge amounts of personal data with huge numbers of businesses, simply for the sake of a few extra pence on the sale of an ad. There are already ideas about how an alternative system could work, and I think a combination of the innovation the tech sector is known for, alongside a constructive regulatory approach, will lead to a far more efficient and proportionate approach to internet advertising.

More broadly, I think in 2030, we'll wonder if a time ever existed where organizations would decide to use systems, like facial-recognition cameras, without asking questions like, "Is this proportionate, is this legal, and is this going to upset a lot of my customers?" That last one is key. As much as regulation is driving improvements in legal compliance, so is the fear of reputational damage of mishandling people's personal data. People are increasingly aware of their information rights, and businesses are realizing the impact on their bottom line that upsetting customers can have.

What will undoubtedly continue is the pace of technological change over the next decade, and this will have a real impact on data protection. This isn't about the headline-grabbing new products, like driverless cars, but a refining and improving of

*Services could use inferences to predict people's needs and nudge them proactively, with an artificial intelligence system powered by massive invisible data collection and data sharing.*

technology that shifts services already available today into the mainstream.

For example, I think we can expect to see digital identity and authentication mechanisms become ubiquitous. Such systems exist already, and as they improve and develop inline with privacy principles, it isn't hard to imagine the idea of uploading photocopies of passports and utility bills to prove identity feeling positively old fashioned in a decade's time.

Similarly, we can easily imagine a world in which voice assistants, like Siri and Alexa,

become ubiquitous, embedded in our homes and our workplaces. This could spell the end of the "search engine" as we think of it, replaced by something providing personalized and intuitive content. Services could use inferences to predict people's needs and nudge them proactively, with an artificial intelligence system powered by massive invisible data collection and data sharing.

Such digital assistants will bring benefits, like empowerment and convenience, but will also have a significant impact on privacy rights and freedom of expression. Will consumers be clear



*Will consumers be clear how much their digital assistant has nudged them toward a product? How can people manage and delete data in such an AI-led system?*

how much their digital assistant has nudged them toward a product? How can people manage and delete data in such an AI-led system?

And what about an area where the future feels less certain? Could the right not to be subjected to an automated decision with significant/legal effects be looked back on as one of the most crucial — and forward-looking — aspects of data protection law? And how will this right evolve, as AI gets integrated into more and more real-world decisions, and people want to understand why “the computer” has decided yes or no?

But I think the area where we’ll see the most significant improvement by 2030 will be around international interoperability of data protection laws.

The borrowing of ideas, best practice and learning has defined data protection law across the 20

years I’ve worked in this sector. A decade ago, as assistant privacy commissioner of Canada, I oversaw the legal requirement for accountability as it entered privacy legislation for the first time. Organizations had to account for the risks they were creating for others and take steps to mitigate those risks. That principle now sits at the center of data protection laws around the world.

It’s a good example of one country’s work being developed and built on by other jurisdictions in the same way we’ve seen progress built on fair information practices from the U.S., Codes of Practice from the U.K. and New Zealand, and innovation measures from East Asia.

This is how data protection law evolves. New legislation stands on the shoulders of the successful laws that went before it, and I’d expect legislation in 2030 to reflect that.

*One thing's for sure: The next decade will continue to be an exciting time to work in data protection. The work we do has never been more relevant to people's lives or more important.*

This approach of new laws in one country reflecting existing ones in others is crucial. Not only because we benefit from the learning of others and ultimately from better drafted laws, but also because it starts a movement toward a global convergence of data protection principles and rights and a strengthening of protection and regulation. And shared legislative ground plays a key role in facilitating the data flows our stakeholders require.

This could be crucial in 2030. There are already danger signs of an increasingly politicised internet, as nations with vast populations and economic power, but with quite different legislative cultures, interact and overlap online. The risk here is one of geopolitical segregation and a tiered internet offering quite different services and standards in different countries.

That isn't great for consumers, and it's very challenging for businesses. International interoperability and collaboration around data protection can help to mitigate that risk, as well as ensuring a consistent minimum standard for personal data around the world.

One thing's for sure: The next decade will continue to be an exciting time to work in data protection. The work we do has never been more relevant to people's lives or more important. Data-driven innovation has changed the world dramatically across the past decade and will continue to do so. Whether it's driverless cars and hover boards or digital identification verification and AI-powered assistants, the data protection community must continue to work together to encourage such innovation while protecting privacy rights. //



# 2030: The Decade of Individual Control and Choice

***Teki Akuetteh Falconer***

*Nsiah Akuetteh senior partner*

One major change that we might see in the year 2030 is more individual control over the use of personal data.

Big data, artificial intelligence and the internet of things will continue to challenge the issues of privacy. It will be invariably impossible to live outside of the technological ecosystem. Technology will become more invasive and control most aspects of our lives as human beings. It will play a significant role in the provision of and access to basic needs. This means individuals will be required to share more and more critical personal data to get access to basic needs, such as food and water, shelter, security, and physical, emotional and intellectual growth and development. With significant advancement in technology, as well as increases in personal datasets and points, the ability to predict and deter-

mine human behavior will also increase. This will also increase automated decision-making in many critical areas of human life, such as health care.

The institutions/countries/corporations with control over large datasets will control the world. This will significantly intensify the struggle for control over personal data by technology corporations, organizations, governments and individuals.

There will be a call for stronger privacy laws that give more control and choice to individuals. Regulators and lawmakers will be called upon to institute more stringent mechanisms that guarantee the right to privacy and provide more control and choice to individuals. The developed countries and economies will step up to the plate, while small or developing economies

may not be able to adequately address these challenges. Generally, there will be the need for more industry and technology expertise on the issues of privacy since the issues will now be synonymous with the growing complexities of the technologies themselves. We will, therefore, see an increase in privacy laws and regulations with more investments in technologies and skill sets that will address such issues. This will also lead to the growth of technologies that support the call for individual control over their personal data by providing platforms that enable individuals to achieve this end. We may also see the development and growth of platforms that allow individuals to trade their privacy at a price.

At the center of the privacy struggle in 2030 will be individual control and choice. //



# The Universe of the Privacy Professional: Star Date 2030

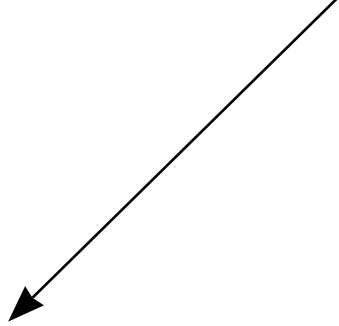
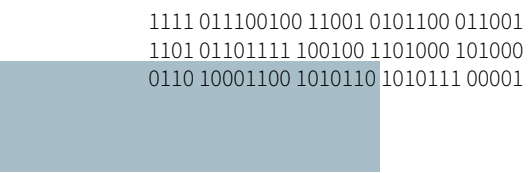
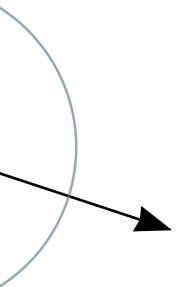
## **Genie Barton**

*PrivacyGenie president and CEO*

The universe of the privacy professional has continued to expand. As predicted by President and CEO J. Trevor Hughes, membership at the International Association of Privacy Professionals has doubled every 10 years. Membership has spiked as new laws and regulations have been enacted in diverse industries, from automobiles to smart wearables and, in various parts of the world, including the majority of countries in Latin America, Asia and the Indian subcontinent. Now, 30 years after the creation of the IAPP, membership has long surpassed the predicted 100,000.

There was a notable spike five years ago with the unexpected

passage of a comprehensive U.S. privacy law — Privacy for the American People — which mirrored the EU General Data Protection Regulation in many respects. The PAP included a cookie consent notice operating through a series of checkboxes; a Do Not Track Registry; the right of consumers registered on DoNT to equal access to all ad-supported platforms, media and other services; and fines for violations of the statute that are, in the regulator’s sole discretion, “commensurate” with the nature and extent of the violations. The Congress also created a new independent agency, the Privacy Commission, with rulemaking authority to implement and enforce the PAP.



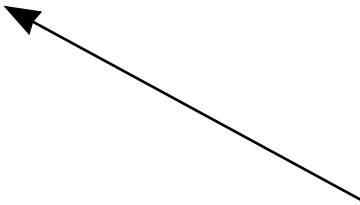
In addition, the PAP required covered companies hire an in-house certified privacy professional or work with an outside certified privacy consultant, depending on company size and the pervasiveness of its data usage, to oversee compliance. To qualify under the statute, the privacy professional's certification was required to meet American National Standards Institute/International Organization for Standardization standards, which provided another boost to the IAPP's ANSI/ISO-approved certification programs. The PAP also required that publicly owned companies with an annual gross revenue of more than 1 billion dollars create a privacy committee on its board of directors. The IAPP developed and won approval for a certification program for individuals who serve on such board privacy review committees.

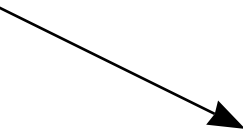
The federal framework replaced the patchwork of state privacy laws, while preserving the ability of state attorneys general to bring actions for violation of the federal statute, although a private right of action was not included in the PAP. Work for privacy professionals at the federal and state level and in the private and public sectors, as well as the academy, has been robust. Like a handful of other independent agencies with high private sector demand for staff, the pay scale of PC employees was roughly pegged to privacy sector salaries, which allowed many privacy professionals in high-pressure positions in law firms and technology companies to enter federal service without selling their homes.

The PC levied a series of fines in the billion-dollar-plus range against major tech, credit rating, data broker, credit card, bank

and insurance companies, which the U.S. Treasury Department has used to pay interest on the national debt. The threat of astronomical fines has boosted law firm privacy practices to previously unimagined heights, and many firms have added in-house tech labs. In 2030, hiring is at an all-time high. To meet this demand, law schools have added a host of privacy courses, providing new opportunities for privacy professionals to enter academia.

Companies had hoped the PAP would lead to a declaration of adequacy for the United States, particularly since there was no cap on the fines the PC or state attorneys general could levy for violations of the statute and the PC has been an active enforcer of the statute. Sadly, however, the Supreme Court struck down several key provisions of the PAP on constitutional grounds. While upholding consumers'





right to opt out of companies' collection, retention and resale of consumers' data to unrelated parties, the court ruled that the requirement that ad-supported services be offered free to consumers who opted out of the sale of their data violated the Takings Clause, a provision of the Fifth Amendment. This opened a new privacy role for economists who were hired to create a pricing system for consumers' data in each ad-supported company to set subscription fees for DoNT-registered consumers to access ad-supported companies. This was a boon for PayPal and other payment services that handled the payment for consumers who opted to subscribe or pay on a per use basis, rather than allow the collection, use and sale of their data. The Supreme Court stayed an immediate challenge to the PAP's offensive content prohibition pending the com-

pletion of the PC's rulemaking to create guidelines on offensive content as directed by Congress. After two years, 17 hearings and 6.4 million comments, the PC completed its rulemaking. The Supreme Court unanimously declared many of the rules were void for vagueness and that many prohibitions violated the First Amendment.

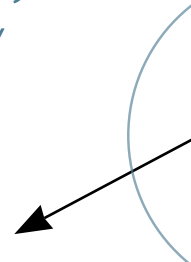
With these two key provisions stripped from the PAP, the EU refused to entertain the United States' petition for an adequacy determination, despite the PC's vigorous enforcement of the remaining provisions of the PAP. As a further blow, after winding through the EU justice system for the past 10 years, the European Court of Justice ruled the Privacy Shield failed to protect EU citizens. Members of the EU trading block, which now includes Scotland, the United Irish Republic and California,

also rejected the U.S. petition. The U.S.-England Privacy Shield agreement remains in place.

As we look forward to the next 20 years, we see a rosy future for privacy professionals. In the U.S., privacy advocates are shifting their focus from data-collection prohibitions to restrictions of various kinds of data usage, in light of the ability of algorithms to make highly sensitive

*As we look forward to the next 20 years, we see a rosy future for privacy professionals. In the U.S., privacy advocates are shifting their focus from data-collection prohibitions to restrictions of various kinds of data usage, in light of the ability of algorithms to make highly sensitive risk predictions from publicly available and seemingly benign data.*

risk predictions from publicly available and seemingly benign data. Civil society and many computer scientists are pushing for new legislation governing the use of algorithms for risk assessments and rate setting by health, life, auto and home insurance companies, credit agencies, banks and the pharmaceutical industry. Stay tuned, and take courses in machine learning and data ethics. //





# The Demand to be Forgotten and Its Associated Challenges



**Heather Dean Bennington, CIPP/US**

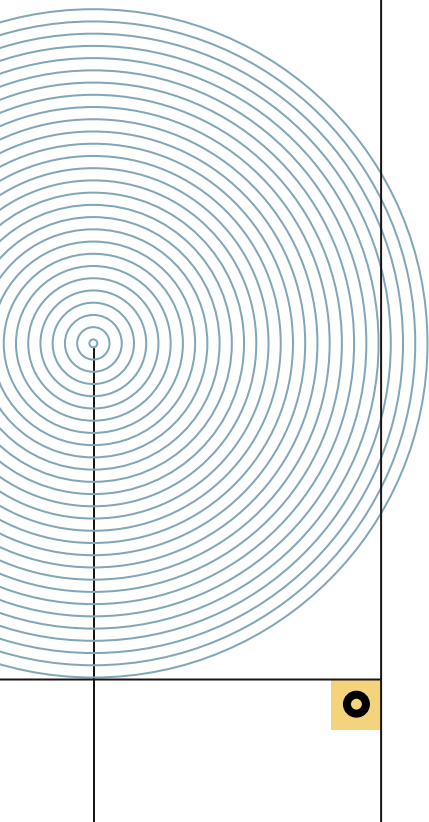
*BNY Mellon privacy compliance vice president*

We have all had an image or a video of us posted by a friend, family member or acquaintance that we preferred to keep private. Maybe a photo with an unflattering angle or a video of you enjoying an activity where you'd rather have a more limited audience than most social media accounts offer. Or it may have even been content shared by you in a conscious yet regrettable moment or inadvertently by way of an accidental "pocket post." You may have asked the poster to remove their media, or if it was accidentally posted by you, you probably deleted it hoping no one noticed.

In 2030, Generation Z will have expansive digital footprints, more so than any prior generation. Some of the information that comprises these footprints

will have been created and digitally shared by a parent without the consent of the individual, by a friend unbeknownst to them, or by the individual themselves as this generation is very digitally connected due to the increasing availability and types of data-capturing devices.

The vast amount of content will be a problem for individuals who want to limit or even eliminate the personal information associated with this footprint. Whether it be a photo or voice in a video or text where one can draw inferences about sensitive information, such as religious or political affiliation, the request by these individuals to exercise what is known as the "right to be forgotten" will be a heavy ask for companies that host this data, and will become the demand to be forgotten.



Although the right to be forgotten does not currently exist in many jurisdictions, I anticipate the desire for this will be great enough to widely change legal requirements within the coming years. Businesses will need to adapt to be able to comply with the new demand to be forgotten. As the continually shifting belief that a company owns the data it holds on individuals versus the individual owns the data that the company holds on them, individuals will feel more empowered to make deletion requests. There are several challenges that businesses will need to overcome to be able to comply, including finding the content, deleting the content and maintaining the request going forward.

Let's start with finding the content. Perhaps an individual wants all videos of themselves that they are captured in removed from a particular social media website. Not just ones they posted, but all videos — for example, as a participant in a

school concert or their presence in a crowd at a professional sporting event. Facial-recognition technologies would be a start to identify where the data subject exists; however, what if their facial structure significantly changed for whatever reason? A business's ability to identify all video content of an individual seems insurmountable today, and although will continuously improve as technology does, I do not anticipate this being at an absolute achievable level in 2030.

Moving on, let's say all the video content has been accurately found. However, much of the content was uploaded by a user other than the individual who has requested they be deleted from videos on the site. What approach will the business take? Will they simply remove the content, regardless of who posted it? Will they anonymize the individual by pixelating the face or modifying the integrity of the video? Will there be a legal basis to have the

user who posted the video comply with the deletion request?

Lastly, we will pretend whatever approach the business took, they were successful. However, how will this request be maintained? Will the site perform continuous monitoring to identify this individual and remove the content in the instance that a video they are in is uploaded back to the site? Better yet, will the site scan each user's request to add content and block the upload when this individual appears in a video? Even if the above controls are implemented, we must remember there is still the challenge of accurately identifying the individual in all instances.

Wherever the future of privacy takes us, businesses will need to have the ability to honor right-to-be-forgotten requests to keep up with legal requirements and, most of all, the demands of an increasingly privacy-sensitive society. //

# Privacy in 2030 Means Hitting the Off Button

**John Bowman, CIPP/E, CIPM, FIP**  
*Promontory senior principal*

One of the great experiences of my early life was studying in the United States from 1987 to 1988. My one-year exchange student adventure took me all the way from Essex, a county to the east of London, to Minneapolis and the University of Minnesota.

Looking back, I have two enduring memories from that time. The first is the sheer cold of a Minnesotan winter, unlike anything I had ever experienced before or since. The other is the complete sense of being cut off from home. The weather may have been a shock, but the isolation was something I relished. I had left my old world behind and was able to embrace the new without hindrance from those who remained in the United Kingdom.

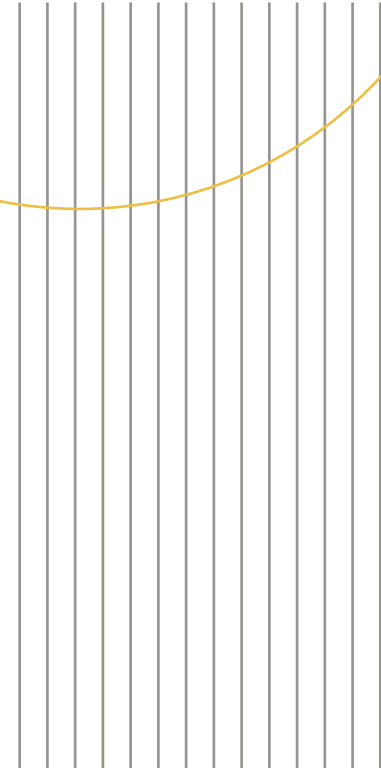
Before the age of instant messaging, social media and always-on news, the ways I kept in touch were a once-a-month phone call with my parents and letters to friends, usually written on wafer-thin “aerograms.” These aerograms combined writing paper and an envelope in a portable, lightweight format that kept the cost of airmail down. It usually took about five days for letters to arrive, but I valued them more than anything else.

My newsfeed was a week-old copy of the Sunday Times of London that the university library fortunately kept in stock and listening to the BBC World Service on my Sony shortwave radio. It was reassuring to hear the dulcet tones of London calling across the airwaves, partic-

ularly as American media barely reported on Europe.

“Fake news” was around, though the old Communist regimes still dominated the shortwave bands. There was a certain fascination in hearing a view of the world from Radio Moscow or an even harder line from Radio Tirana in Albania, however fantastic the claims of these regimes were.

My interaction with the world during my year abroad was therefore truly analog. This even extended to my university work, which I prepared on an IBM Selectric typewriter with golf ball typehead. I remember thinking at the time that using the backspace button to erase a typo was the most amazing function I had come across.







I cannot imagine there is much trace of my time at the university beyond a registration form, my essays, letters, photos and some faded memories. I realize now I could have been as private as I wanted to be, gone anywhere I wanted to, and no one would have been much the wiser. I can now see how all-enveloping digital society is compared to those times. There are some things we cannot control any more, particularly when we are forced to engage with the machinery of the state, our employers and the commercial institutions that enable us to exist and function in the modern world.

We may also feel that we are compelled to interact with information society services as there are no other choices in the marketplace. Or maybe we have just become addicted to the perceived value and convenience that such services offer. But are

we willing to compromise our privacy for all this?

Views are changing, and perhaps we can take back some control of our personal lives. In the next 10 years, we may see the growth of grassroots movements advocating simpler ways of living that aim to disentangle us from our digital dependencies.

In the late 1980s, I cannot recall privacy being a topic that people were unduly concerned about. In the U.K., we did not have the experience of oppressive regimes that many of our European counterparts had during the Cold War so our sensibility about privacy rights was undoubtedly different.

Things have changed, though, and with a global consensus emerging about privacy rights, maybe it is time to look back on the analog era, not only with a sense of nostalgic fondness (at

least for those of us old enough to have compiled mixtapes on actual cassette tapes), but also as an alternative way of living for those who grew or are growing up during the digital age.

So, what could privacy look like in 10 years' time? It could mean dusting off those typewriters, handwriting those letters to friends, navigating using paper maps and enjoying entertainment on physical formats.

By dispensing with the multitude of electronic devices that track everything we do, we may gradually reveal less about ourselves to the world, or at least limit what is available. But that is a choice we must make ourselves. This may seem like a crazy dream, but privacy in 2030 probably means having to hit the off button on all those devices that tie us to the world that we live in. //

# An Idea Whose Time Has (Finally) Come

**Lorrie Faith Cranor, CIPT**

*Carnegie Mellon University professor of computer science, engineering and public policy and CyLab director*

It's 2030, and the vision of seamless privacy notice and choice, first proposed in the mid-1990s, has finally been realized. No longer are consumers expected to read 20-page privacy policies full of legalese that neither humans nor artificial intelligence systems can comprehend. The presumption that companies can use data unless a data subject opts out has become obsolete. Those annoying cookie banners that consumers swatted away without reading in the late 2010s and their successors, the audio privacy banners that consumers yelled at to make them stop whispering in their ears in the 2020s, are all a thing of the past. Instead, consumers have a single conversation with their digital assistants about their preferences for data sharing

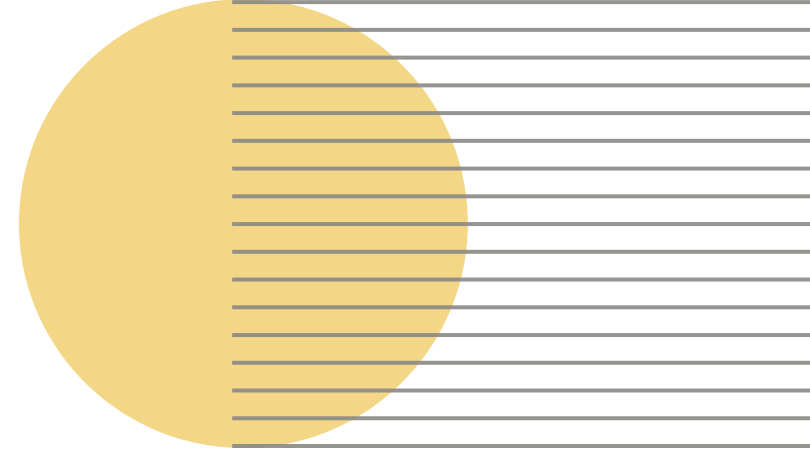
and are confident their data will be transmitted and used only according to their desires. Of course, consumers can ask their digital assistants to tell them about how a particular company is using their data any time they want and can make adjustments if they change their preferences. However, most people set up their privacy preferences once and rarely worry about it again.

The seamless privacy notice and choice system is a new high-tech system based on old tech. In the mid-1990s, the World Wide Web Consortium began developing a privacy standard called the "Platform for Privacy Preferences" that allowed websites to communicate about their privacy practices in a format that could be read and acted on automati-

cally by web browsers. Although it was built into the Microsoft web browser when it became an official standard in 2002, it never saw [widespread adoption](#). In the 2010s, W3C developed a standard called "Do Not Track" to allow web browsers to automatically communicate to websites their users' desire not to

be tracked. While a number of web browsers included a button to send Do Not Track signals to websites, few websites honored these requests, and the standard was [ultimately abandoned](#).

The new seamless privacy notice and choice system works with all the devices and services that



*Data is flowing again but only with data subject consent.*

now collect and use personal data. This idea goes back to the early 2000s when academic privacy researchers began proposing privacy awareness systems for “ubiquitous computing” environments. In the 2010s, academic research on “personalized privacy assistants” demonstrated prototype systems in which internet-of-things devices broadcast their privacy policies in computer-readable format so apps running on smartphones and smartwatches could **notify their users**.

Today, laws around the world mandate data about an identifiable person be considered

private and used only with that person’s consent with some exceptions. As these laws were enacted, businesses struggled to adjust to the new regulation. The online advertising industry bombarded users with so many requests to opt in to tracking that most people installed cookie-banner blockers so they didn’t have to keep swatting away requests. Smart thermostats, smart speakers and even smart toothbrushes read privacy policies out loud and begged people to allow data collection. People were so overwhelmed with constant requests for their data they could no longer find the requests they wanted to

permit and just denied them all. Pundits predicted that with personal data no longer freely flowing, economies around the world would soon collapse.

Fortunately, technologists had a solution. Reaching back into their archives and pulling out research prototypes and web standards that were 10 to 30 years ahead of their time, they proposed a seamless privacy notice and choice system. This new system makes use of computer-readable privacy policies and user-consent statements that are seamlessly exchanged between a user’s privacy assistant and the devices and services the user interacts with. Data is not collected or used until an appropriate consent statement is received, and consent statements are only sent in circumstances that match a user’s privacy preferences. An audit trail showing all data flows is available to users, as well as

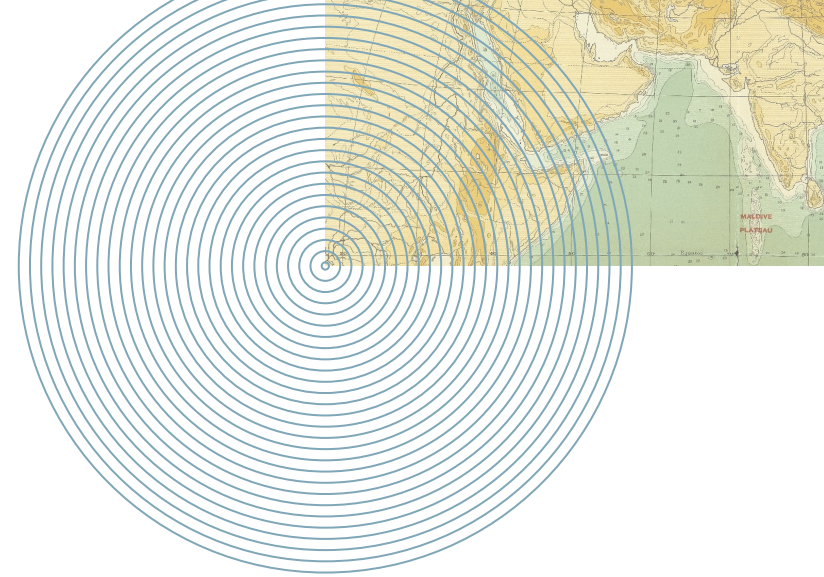
to help companies track onward sharing of data they collected. Best of all, users can set their preferences up front and are rarely interrupted to make privacy decisions.

As a result of the seamless privacy notice and choice system, new business models and services have emerged. People who want to be the first to know about new products are receiving ads, precisely targeted to the interests they have granted permission to share. But now these ads are better targeted than ever before, and they are sent only at the time and location designated by users. New privacy-enhancing technologies allow consumers to share data anonymously so they can take advantage of customized services that used to require the use of detailed personal information. Data is flowing again but only with data subject consent. //



# In Hindsight:

## The Global Impact of the GDPR



**Andrew Clearwater, CIPP/US**  
*OneTrust chief privacy officer*

On May 25, 2018, the EU General Data Protection Regulation entered into force. To privacy professionals working in the field, it was clear that the reform to EU data protection legislation marked a turning point, not only in the way in which data would be viewed and regulated from that moment on, but also in the way that society, business and nations interacted with each other.

### **The domino effect**

It's now 2030. In the years that followed the entry into force of the GDPR, countries all around the world began to adopt new privacy and data protection laws or update existing frameworks. California and Brazil were among the first to enact legislation in the wake of the

GDPR, with other jurisdictions, such as Argentina, Chile, Dubai International Financial Centre, India, Nigeria and Pakistan, all following suit.

The United States, in particular, saw a rapid succession of state privacy laws being passed not long after the California Consumer Privacy Act, culminating in the first comprehensive federal privacy law in 2022, the Personal Information Privacy Protection Act. As with other federal privacy legislation, PIPPA was drafted to include narrow preemption provisions of state law in certain circumstances. While PIPPA was meant to alleviate the concerns with dealing with differing state requirements, arguably challenges continue when attempt-

ing to address PIPPA alongside more than 20 general state privacy laws.

### **Global trade**

Common among these frameworks, of course, was the pursuit of better safeguards and protection for residents' personal information and inclusion of generally accepted privacy principles and concepts relating to data accuracy, data minimization, accountability, legal bases for processing and data subject rights. Though such concepts have long been discussed and included in part within legislation, the impact of the GDPR's approach to such provisions on other jurisdictions' legislation can be seen from the similarity of wording and drafting in these laws.





*Privacy could continue to be undermined under the banner of safety if we don't see new actions taken. There is a long road ahead for settling these issues.*

In addition to this, the GDPR was the first major data protection law that extended its requirements across borders outside the European Union. This extraterritorial scope marked a big step in escalating the global shift toward digital protectionism and even stoked a “global trade war” of sorts that caused a worldwide impact. In a bid to ensure other jurisdictions preserve the protection of their residents, the majority of privacy laws that have emerged since the adoption of the GDPR have also sought to enact obligations that stretch out extraterritorially, binding any company in the world

that does or targets business in that jurisdiction.

Moreover, data localization requirements have continued to be included in both general data protection and sectoral laws and regulations. For example, the Indian Data Protection Act 2020, much like the Russian data localization law before it, continues to require companies to keep and maintain a copy of personal data in a local data center. Such provisions continue to add to the myriad complexities that organizations face when doing business internationally.

### **Technology that required more changes**

When cars first took to the streets in the 1890s, there was confusion about roles and responsibility. When the first person in New York City died due to being struck by an automobile, there were two reactions: One that it was an accident, and another summed up by the Evening Telegraph in their opening line, “The automobile has tasted blood.” So, with that history as context, when the first driverless cars took to the streets, we all wondered about roles and responsibility. Privacy and security issues around automated and connected vehicles took center stage for data protection regulators that took interest in the wide array of equipment and features that rely on the collection and use of data about people and their vehicles. Should we prevent people from opting out of sharing safety data to the cloud in the name of safety? The Fair Driving Reporting Act was a

good first step to give consumers access to information about their history so they can see it and correct it. But privacy could continue to be undermined under the banner of safety if we don't see new actions taken. There is a long road ahead for settling these issues.

### **Who is a privacy professional?**

Looking back, it's funny to think that in the early 2000s, privacy was a challenge faced predominantly by lawyers. How the times have changed! Privacy engineers ushered in an era of greater technical focus, and the role of unforeseen role of privacy ethicist formed to ensure the ethical collection and use of data. Today, the job of chief privacy officer has turned into a much larger enterprise, reporting directly into the CEO at most Fortune 500 companies with a team interwoven into every facet of the organization. It's hard to look back and imagine the task of going in alone — good thing that's not the case today in 2030. //

# Seen But Not Herded

**Ian Cooke, CIPP/E, CIPM, CIPT, FIP**  
*An Post Group IT audit manager*

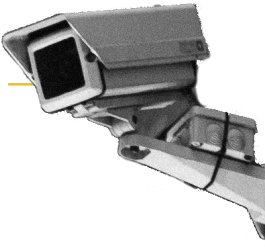
In April 2019, I went on vacation to China. Being a privacy technologist, I am aware that many western social media and news sites are blocked in China so I prepared well, installing a virtual private network on my iPhone and that of my wife so that we could keep in touch with events and family back home. This later proved to be invaluable as many of our fellow travelers (it was a guided tour) or their family members back home were forced off the WeChat platform (a Chinese messaging, social media and mobile payment app developed by Tencent) for discussing our visit to Tiananmen square (WeChat does not employ end-to-end encryption and, as such, is monitored by the Chinese state).

Entering China is much like entering the United States for a European citizen. We were

required to provide fingerprints and a facial shot. However, once through border control, I was not in any way prepared for the number of cameras, although I had read about them — there are cameras everywhere! Besides being on every major street corner or intersection, they were in the subway, in the corner of practically every room you entered, and even hang from trees.

In China, the cameras are an accepted part of daily life. For instance, facial recognition is an accepted form of identification. One of our hotels allowed check-in via facial recognition; on an internal flight from Beijing to Xi'an, there was a facility to check your flight status via facial recognition; and finally, when exiting China, the same border routine with facial scanning and fingerprinting was required again. My wife went





through first and waited for me on the other side of the border control. When I approached the console and my face was recognized, she could see what the guard could see — pictures of me from different angles from, we assume, the various locations we visited throughout China.

Given [reported](#) misuse of the technology, this was a somewhat disconcerting experience, and my concern is the situation is only likely to get worse. China is already selling this technology to countries, such as [Ecuador](#), while in the west, for every positive story, such as [San Francisco](#) banning facial recognition or [Axon](#) admitting the technology is not yet ready, there are negative ones, such as the [U.K. watchdog](#) criticizing the “chaotic” police use of facial recognition or the [Danish data protection authority](#), the Datatilsynet, approving the use of the technology at a football club.

Given these stories, there is likely to be some sort of moratorium until the biases are removed and the accuracy improves. There is also likely to be legislation, but I have no doubt the technology will be deployed on a massive scale long before that happens. In addition, as the internet of things continues its expansion, consumer use of the technology will explode. There will be no escaping a camera or facial recognition in 2030.

So, what can be done? How will I, as a privacy technologist, prepare for a trip to Ecuador in 2030? I could try [occlusion techniques](#), which work by physically hiding facial features so the camera simply can't see them. I suspect instead I will pack anti-surveillance clothing. This will involve [printing](#) patterns on clothing or textiles that computers interpret as a face, the idea being to overwhelm and confuse the facial-recognition systems

by presenting them with thousands of false hits so they can't tell which faces are real. One example of this technology is [HyperFace](#), which works by providing maximally activated false faces based on ideal algorithmic representations of a human face. I will also pack my privacy-protecting eyeglasses. Such [technology](#) already exists and [works](#) by using carefully crafted lenses that reflect, refract and absorb light in different ways or by reflecting both infrared light and visible light. Both claim to block facial recognition. By 2030, [Apple](#) will likely be marketing augmented reality glasses. Given their current focus on privacy, I would not be surprised if I pack privacy-protecting, augmented-reality glasses with an Apple logo on them.

What is the major change we might expect with regards to privacy in the year 2030? We will “opt out” of facial recognition using wearables. //



# Privacy, Evolved.

**Barbara Cosgrove**

*Workday vice president and chief privacy officer*

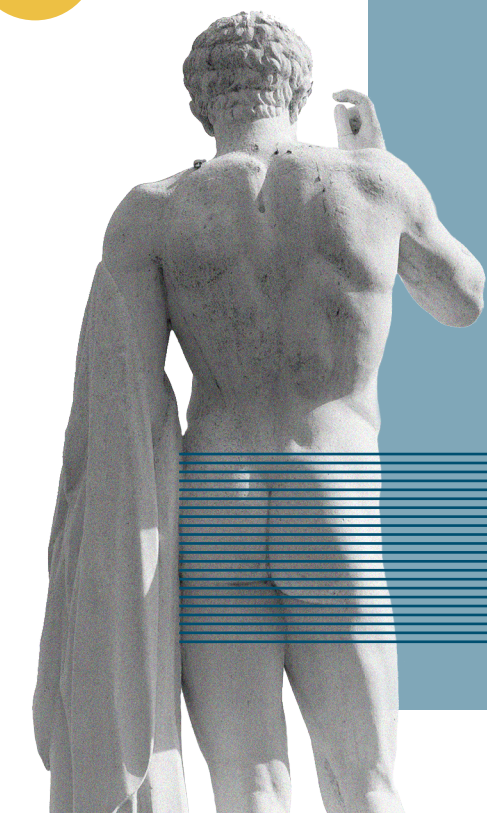
Leaders from both the public and private sectors have called for an increase in the role governments play in ensuring citizens and their data receive adequate protection in recent years. Two factors have fueled this trend: 1) a massive shift to digital transfer of data; and 2) proven business and consumer benefits resulting from the adoption of privacy frameworks around the world. As we pair these insights with developments like the lightspeed maturation of emerging technologies, like artificial intelligence and machine learning, the continued evolution of privacy — from the way we define it to how its upheld and protected — is the one constant we can expect to see in 2030.

Let's get a bit more specific about how continued technological advances and regulatory

change will influence the evolution of privacy within each of those categories on a global scale and envision what it might look like for businesses, governments, citizens and other stakeholders in 2030.

## **Privacy, defined.**

Until recently, the term “privacy” at organizations was synonymous with “compliance.” And, in many cases, ensuring that a company’s products, services and practices maintain compliance with evolving regulations is a responsibility owned by the same team that manages data privacy operations. Although compliance will continue to be a core component of the privacy function, most organizations will broaden the roles and responsibilities of internal privacy teams to include business ethics and trust.



*We can expect to see a continued influx of content that clearly states corporate values, guidelines and/or corporate stance not only from a general standpoint, but on specific issues, as well.*

**Privacy, upheld.**

The way businesses and their customers evaluate privacy and ethics will also evolve. While certifications and standards will continue to be helpful in ensuring regulatory compliance, the corporate ethos, mission or purpose that inspires organizations and employees to maintain ethical business practices will become more critical to internal and external company stakeholders. We can expect to see a continued influx of content that clearly states corporate values, guidelines and/or corporate stance not only from a general standpoint, but on specific issues, as well. Operationalizing those

values and guidelines in a meaningful and verifiable way will be key. From there, companies will align their use of data and access to data with these frameworks.

**Privacy, protected.**

As governments grapple with this complex topic, we can expect to see legislation across the globe align more closely with the Organisation for Economic Co-operation and Development's Fair Information Principles. This legislation will include broad yet robust U.S. national legislation that protects citizens' privacy in an adaptable way so that as technology evolves, our regulatory structure is able

to adapt and scale without overhauling the laws themselves. By aligning privacy laws with the Organisation for Economic Co-operation and Development Fair Information Principles on a global scale, we'll have enabled the continued free flow of personal data across borders and protection of individuals, regardless of where they're located.

As we've seen in recent years, transparency and trust will continue to remain a top priority for major corporations and their customers. Hopefully, we'll reach a point at which the protection of privacy and data is perceived the same way a seatbelt and car safety ratings are today, in that consumers, companies and government agree on and mutually benefit from the imperative nature of protection, and everybody does their part to support it. //



# Human Rights Coupled with Fiduciary Duties

**Christopher Hart, CIPP/E, CIPP/US, CIPM**  
*Foley Hoag counsel*

In 2030, we will see the full fruition of the revolution that the EU General Data Protection Regulation began: the transition from a business-centric balancing approach to privacy interests, to one that puts the individual's interest in privacy as a right at the center of the legal structure. Moreover, this transition will go hand in hand with a transition from a business-centric notice-and-consent system to a set of legal regimes that take rights seriously and shift the burden of protecting privacy to entities processing information, rather than placing it on consumers themselves.

To say that, in the United States, there is a balance between consumer and business interests in personal data would be generous to consumer rights. In actuality,

there are very few protections that consumers have relative to the amount of data they provide businesses, outside of any obligations that organizations might bind themselves to through their privacy policies. Even in states where they do or will have greater rights, there is usually a massive burden placed on consumers to exercise their rights rather on business to protect those rights. The California Consumer Privacy Act is a good example of this tendency. The CCPA gives people real rights, such as the right to delete information, but forces consumers to be the ones who are vigilant about those rights.

While the GDPR is, in fact, no different in this respect — it is in significant measure a notice-and-consent statute that forces

individuals to exercise the rights they have — nevertheless, it moves the bar significantly toward defining concrete rights and toward favoring entity protection over consumer vigilance. Therefore, the GDPR requires notice of rights that individuals already have rather than notice of rights a company deigns to give them but need not (as in the U.S.).

Granting rights, however, is a one-way ratchet. Once people have rights, it is very difficult to have them give up those same rights. The GDPR has defined privacy rights in concrete and important ways and codified the longstanding EU view that they are human rights; moreover, the GDPR makes such rights a vital part of a significant set of legislation that is now entrenched in

1111 011100100 11001 0101100 011001  
1101 01101111 100100 1101000 101000  
0110 10001100 1010110 1010111 00001



*As data breaches continue and become more dangerous with the ubiquity of facial recognition and artificial intelligence, it will become clear that a burden shift toward companies will be the only way to preserve well-accepted privacy rights.*

a vastly important sector of the world economy, forcing companies and legal systems around the world to react. National legislatures in other parts of the world, such as Brazil, have reacted, expanding the scope of the new rights-based world. The CCPA is only the first step in a larger and inevitable march in the U.S. toward a rights-based privacy system — and once rights are defined in one jurisdiction, such as the enormous California economy, there is no going back. Other states, such as Washington, New York and Massachusetts, have already tried to pass laws privacy laws that define rights. While these efforts have not yet been met with success, their time will come. And that time will come regardless of what the federal government does.

When rights are universal, expected and clearly defined, company behavior too will have

to change. Rather than place the burden on consumer, the burden will be placed on companies to act as fiduciaries of data. It will soon become clear the notice-and-consent model is not compatible with a rights-based model because one undercuts the other. As data breaches continue and become more dangerous with the ubiquity of facial recognition and artificial intelligence, it will become clear that a burden shift toward companies will be the only way to preserve well-accepted privacy rights.

In short, by 2030, we will look back at 2020 as a unenlightened time, when there were no well-defined privacy rights in the U.S. and businesses held all the bytes. Privacy rights will be an entrenched part of culture, and companies holding personal data will be expected to act with care. And we will look back at the GDPR and CCPA as the footholds for this new and sensible future. //

# The Range of Responsibility

**Peter Hustinx**

*Former European data protection supervisor and IAPP board member*

My favorite provision in the EU General Data Protection Regulation is Article 24 about “responsibility.” It is arguably the most central provision of the regulation, which is now influencing developments globally. That influence is likely to increase — possibly exponentially — with ongoing innovation. No wonder by 2030 the “range of responsibility” will have emerged as a crucial factor for all stakeholders to observe very closely.

There is much to say about the nitty-gritty of data protection — e.g., the requirements for lawful processing, requirements for valid consent, and rights of the persons involved — but without “responsibility,” it all amounts to very little. Without a clear definition of who is responsible for the delivery of all that beauty,

and what it actually means to be responsible, it is all only a castle in the sky. Make no mistake, it is not the individual or regulator that can provide effective protection but rather a responsible controller that understands their role and acts in a proper manner so that data protection can do its work in practice.

The GDPR has made significant steps in the right direction on this point. In the old law, “responsibility” was not entirely absent, but the relevant provisions were largely invisible or came into practice only when the question arose of who should be liable if something had gone wrong. The new law makes “responsibility” prominent from the very beginning. A controller must adopt all appropriate technical and organizational

measures to ensure compliance with the legal requirements. He needs to periodically review such measures and adjust them, if necessary. He must be able to demonstrate compliance with these obligations. This threefold mission is dependent on the circumstances and risks of the case. That forces the responsible controller and the persons acting on his behalf to watch out and act from the start to avoid unpleasant developments.

This approach to “responsibility” is no longer a formality but an issue that requires constant care and attention. The obligation to take “all appropriate measures to ensure compliance with the legal requirements” will inevitably bring in all other relevant requirements of the GDPR at an early stage and a thorough

analysis of their impact before data processing has started. To underscore this, the GDPR also provides for data protection by design and default for which responsible controllers will be equally accountable.

Within organizations, this should be organized in a proper manner to ensure they are not missing it. Hence, there is now a clear trend toward the “professionalization of data protection.” There is also a growing profession with the right expertise to give “responsibility” substance in practice. Going forward, it is







likely the present tensions in the market for privacy professionals will cool down and a workable balance be reached.

Regulators have now also received the effective tools to keep responsible controllers on track. That need not be so complicated; they can choose to control with simple actions whether relevant organizations are on the right path. Insiders know there is much low-hanging fruit in this space; an organization that has no clear overview of the processing for which it is responsible, after all, seems bound to fail. A supervisory authority may in such cases impose a fine or also decide to set a time limit within which the necessary measures must be taken. Appropriate publicity surrounding such actions can further stimulate laggards to do their best.

In recent months, such and other enforcement activities have increased, and we are not likely to see the end of that line very

soon. To the contrary, the scope, diversity and impact of enforcement activities will gradually increase, in parallel with technological developments involving or affecting the use of personal data. The wide territorial scope of the GDPR — also covering companies with activities but no other presence in the European Economic Area — is an important factor to be reckoned with in this context.

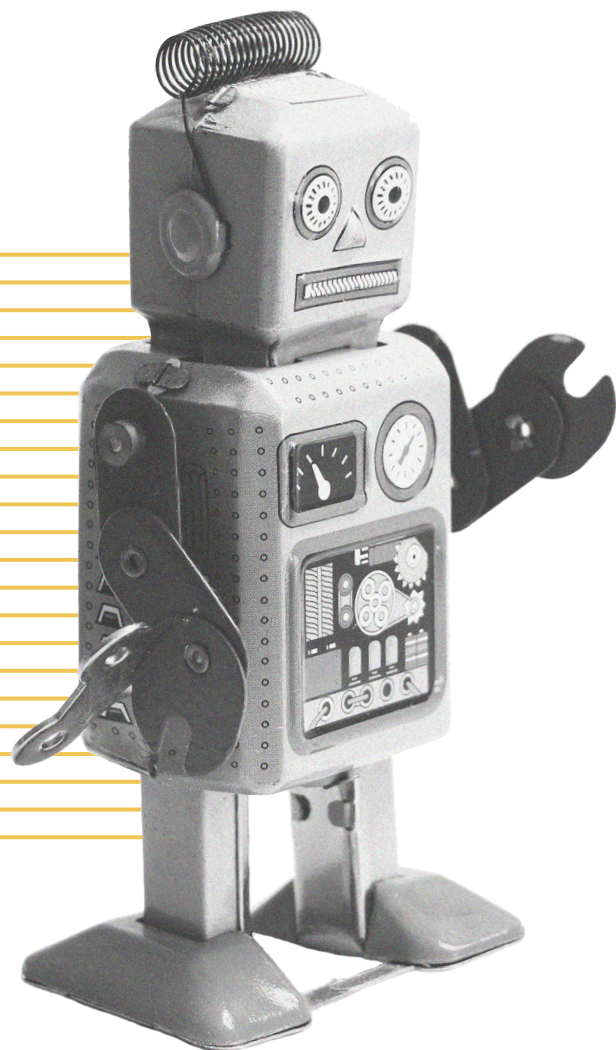
Let me mention a few other dimensions that also need to be considered. First — and this is already happening at some scale — organizations cannot limit their attention to internal developments but need to consider data relations with their partners, vendors and clients. Increasingly, these other parties may turn out to have a shared responsibility for certain parts of their operations with all important consequences flowing from it. The Court of Justice of the European Union has recently dealt with such cases involving both Face-

book and third-party websites featuring Facebook “like” buttons (CJEU, case C-210/16, Wirtschaftsakademie Schleswig-Holstein, and case C-40-17, Fashion ID). More of those cases will undoubtedly follow.

Second, in a now-famous decision about the “right to be forgotten,” the CJEU decided Google is responsible for what its algorithms do in searching across the internet (CJEU, case C-131/12, Google Spain ). This part of the decision and its emphasis on the need to ensure effective protection of personal data suggest controllers will also be held responsible for the use of artificial intelligence in their operations. The argument that such use is not fully predictable will probably not hold sufficient water.

Privacy professionals are, therefore, advised to further explore this “range of responsibility” or ignore it at their peril. There will no doubt still be interesting times for them by 2030. //

# My Privacy Robot



```
1111 011100100 11001 0101100 011001  
1101 01101111 100100 1101000 101000  
0110 10001100 1010110 1010111 00001
```

**Jules Polonetsky, CIPP/US**  
*Future of Privacy Forum CEO*

By 2030, I expect artificial intelligence to help us manage our personal privacy choices in ways that reflect our true preferences without requiring us to constantly update our privacy settings manually. I'm fascinated by Carnegie Mellon University Professor Norman Sadeh's work on [personalized privacy assistants](#). He envisions "intelligent agents capable of learning the privacy preferences of their users over time, semi-automatically configuring many settings, and making many privacy decisions on their behalf."

AI can be used to manage your interactions with all the different technologies and companies that are using or tracking your data.

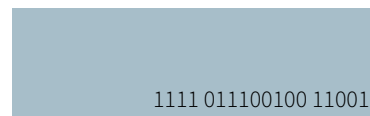
There are literally hundreds of options on a phone that affect your privacy, not just the clear privacy options in your settings, but also hundreds of decisions you could be making. That's far more than any human can handle, and that's where AI on behalf of the user would come in very handy. Intelligent agents can learn and actually know your true preferences, your actual intentions about how you share data, and with whom you share and for what purposes.

Today, we have a focus on AI primarily to help organizations act more wisely on you for the organization's benefit, hopefully for purposes that are valuable to



1111 011100100 11001 0101100 0111001  
1101 01101111 100100 1101000 101000  
0110 10001100 1010110 1010111 00001

you and society, but not necessarily driven by what your core interests are. In the future, Sadeh and others will develop AI that lives on your phone or your computer. It watches and it learns, and it tries to see what you end up doing or not doing over time. That agent reflects your priorities and goals and maybe knows you better than you even know yourself — because sometimes



1111 011100100 11001 0101100 011001  
1101 01101111 100100 1101000 101000  
0110 10001100 1010110 1010111 00001

you try to use a certain setting to accomplish a certain purpose, but you may not appreciate that you are under-sharing or over-sharing. You may misunderstand the setting or just not want to be bothered at the time you are presented with the choice.

In fact, manually taking time to set, update and tweak your preferences on the computer, mobile or TV for every different company for every different technology is going to be impossible. Nobody will actually be able to spend the amount of time and energy that requires.

We know from Carnegie Mellon University Professor Alessandro Acquisti’s research that people are so complex that their actual attitudes about privacy can vary at different times of day or can be altered based on what they’ve recently heard, seen or read. Given the incredible complexi-

ties, making selections reflecting your true desire at any given point is infeasible.

However, AI will have people managing their true privacy preferences in a sophisticated way without them having to spend a lot of time and energy to train the mechanism. So, machine learning can work for you over time.

I anticipate smart technologists driven by a notion that we can use AI on behalf of the individual will build those sorts of AI tools to protect privacy according to learned personal preferences. Users may even be able to train browsers and other operating systems to act on their behalf. I can even imagine a situation in which my AI “robot” could “match wits” with commercial AI tools attempting to manage data on others’ behalf. But perhaps that is best left to science fiction. //



# Making the Grade: Privacy as Core Curriculum

**Alexandra Ross, CIPP/E, CIPP/US, CIPM, CIPT, FIP, PLS**  
*Autodesk global privacy and data security counsel director*

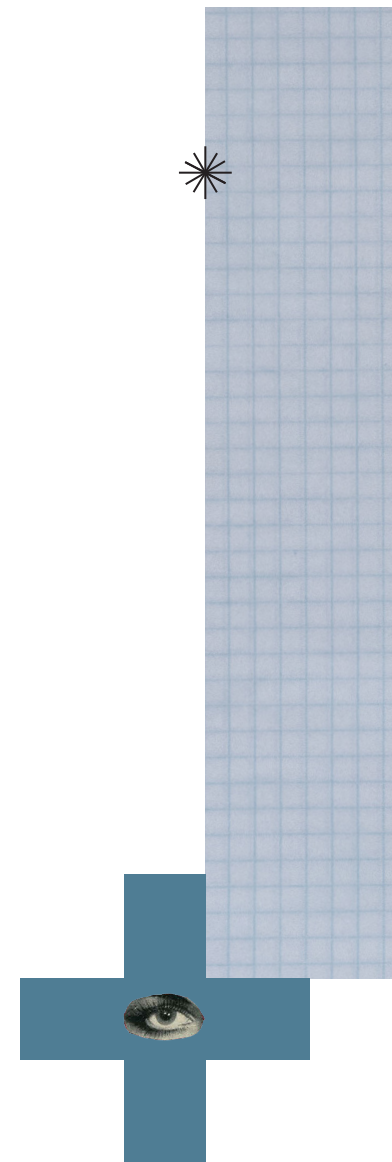
When I was in law school, there were no dedicated courses in privacy or data security. Certain intellectual property survey courses may have touched on technology and data-related concepts, but nothing that could be considered a “course” on privacy, let alone a certificate program dedicated to the topics of privacy and data security existed. The world was about as different in 2000 as 2030 will be from 2020. By 2030, privacy will be more than just something that might come up in a general survey course. With any luck, privacy will become core curriculum, part and parcel of what it means to get an education, on the same level of importance as reading, writing and arithmetic.

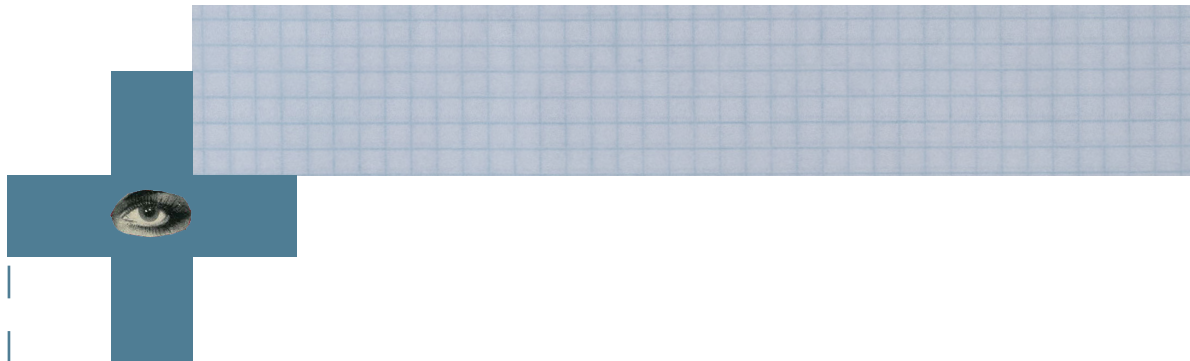
The educational landscape is changing. High-profile data breaches have prodded a sleep-

ing giant, raising our collective awareness about the precarity of privacy, particularly as our personal data is distributed across an increasingly digitally connected society. In response, universities have begun to take privacy seriously. [Dozens of schools](#) across the United States, Canada, Asia-Pacific region and EU have instituted some form of privacy curriculum. Most major law schools have significant offerings around privacy, security and tech law, with some even courting legal scholars who focus their studies on privacy. Santa Clara University has [developed certificate programs](#) around privacy law, while others, like [New York University](#) and [Carnegie Mellon](#), have entire institutes dedicated to the study of issues related to security and privacy — everything from biometrics to blockchain, cryptography to

the internet of things. Programs such as these will become more common as data and privacy landscapes grow more complex.

By 2030, though, privacy and data security will be more than topics for the classrooms, ivory towers of law schools and other institutions of higher education. With K-12 schools relying on digital tools for classroom management, digital record keeping and school surveillance and with children now getting their first cellphones [by age 10](#), privacy and data security skills will be part of a well-rounded primary and secondary education. In much the same way kids from earlier generations might have been taught to avoid talking to strangers and look both ways before they cross the street, the kids of 2030 will learn digital literacy skills, password hygiene and encryp-





tion. They'll learn about avoiding phishing emails, identity theft and algorithmic discrimination. They'll learn about closing their browsers when they're finished with them, using a virtual private network and the dangers of unsecured Wi-Fi networks.

But privacy and online safety can't fall solely on the shoulders of parents. Schools, after-school programs and public service media will have their own roles to play in making sure privacy takes priority. And it's not a huge leap to get there. [Girls Scouts of America](#) already issue badges for cybersecurity — from the basics of staying safe online to cracking cipher codes, analyzing log files to solving fictional cybercrimes. Right there, alongside more traditional outdoor skills, like archery, camping, first-aid and woodworking, sit badges honoring the mastery of making informed online choices

and tracing the steps of a ransomware attack. In a sense, data security and privacy protections are becoming new life skills — ones that should be taught at younger and younger ages. Like the civics classes of yesterday, privacy and data security will become part of what it means to be a person in a connected and complicated digital world.

Privacy and data security are about more than just protecting one's own personal data. We need trained privacy professionals, privacy attorneys and data protection officers — individuals with a deep and broad knowledge of data policy, program management and ethics to take the lead on these educational efforts. Beyond privacy as core curriculum in schools, privacy-by-design trainings will evolve with the landscape, making clear current legal requirements and best practices to

ensure an informed workforce. According to a [recent survey](#), 60% rated their company's privacy knowledge as "moderate to low." By 2030, we'll make progress toward bridging this privacy compliance education gap.

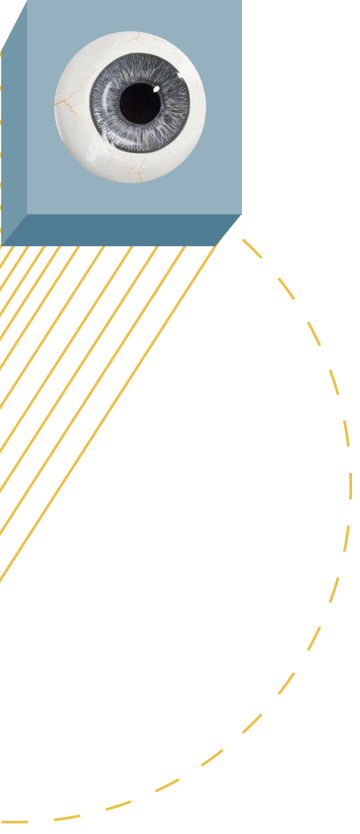
To drive home the importance of a privacy culture, these kinds of trainings should be relevant, engaging, interactive and include data governance stakeholders at the helm. They should cover key concepts of global privacy laws and best practices for identifying personal data, individual rights regarding their personal data and the responsibilities that organizations have when collecting, processing or sharing data.

2020's demand for privacy training and awareness isn't going away. By 2030, it will be part of what it means to make the grade. //

# No Hiding:

## When Personal Data Becomes Identified

**Laura Tarhonen, CIPP/E**  
*IKEA Group data privacy leader*



Until recently, the most important concept in data protection law has been the notion of “personal data.” If data is not qualified as personal data, data protection laws are not applicable. Within the next 10 years, we will have less and less discussion about whether certain data is personal or not and more and more processing of data directly connected to a specific person. The main drivers for this are the definition of personal data in the EU General Data Protection Regulation, the perceived value of data for businesses, rise of biometric identification, and development of more personal devices and technologies.

The GDPR tried to close the gap between the definition of personal data and reality of digital technology by explicitly

mentioning online identifiers as personal data and emphasizing personal data can also be indirectly identifiable. Simplistically put, this means the creation of profiles around a specific identifier will make the data personal regardless of whether the exact person the profile relates to is known. The possibility to directly identify an individual with reasonable effort is enough.

Since there is no difference in how directly and indirectly identifiable personal data is treated under the GDPR, there are no real incentives for data collectors to avoid processing directly identifiable personal data. This is further reinforced by the “data craving” that most companies suffer from. It is widely accepted that personal data is valuable for creating and optimizing business activi-

ties and deciding not to leverage the possibility for personal data processing is like not believing in computers or using email.

There used to be a time when it was justifiable to claim browser cookies were not linked to only one specific person. We regularly used devices that were shared with family members, friends and even colleagues. There is no going back to that time. The devices we are using are mostly personal and soon also physically part of us in the form of chips or other insertables. Even the internet-of-things devices that are used in households need someone with an app, account or other adjacent device to control them. The use of biometric identifiers and facial recognition will become (and already are) part of our everyday life. These technologies, although

*It is already necessary to stop the discussion on what is personal data and start to plan how privacy by design, consent and choice will be implemented in a world where there is no hiding.*



prone to deception, are going to be accurate and always linked to “that one” specific person. The selling point for the individuals is compelling: Biometric identification is convenient — no remembering passwords, no typing, no active measures needed to access services.

You might be thinking, does it really make a difference if data will be more identifiable? Already today when we use online services, identifiable data is necessary for finalizing almost

any the transaction. One clear difference will be that when the identification of data becomes more precise, like with biometric identifiers, it will be much easier to match and combine different data sources reliably and also without the knowledge or participation of the individual. Today, you might still be using different email addresses as your identifier, but using a different face will be much more difficult. From an individual’s point of view, this will lead to even more intrusion of their privacy, when data

breaches have a bigger impact and it is easier to create all-encompassing profiles by combining data from different contexts and use data for new purposes. Instead of being someone with characteristics X, Y and Z, you are always you.

It is already necessary to stop the discussion on what is personal data and start to plan how privacy by design, consent and choice will be implemented in a world where there is no hiding. The shift to more identifiable data could lead to harmful data sharing and combination, but it could also open a possibility for more control for individuals as there is less data that can be excluded from data subject rights. To be able to fully leverage the data subject rights, it should be easy for the individuals to manage their rights to the data.

We must start the development of central privacy rights man-

agement for individuals — a one-stop shop for controlling data connected to you and the purposes that it can be used for. Optimally, these services will not process any data themselves to avoid conflict of interest but only interpret the individual’s will toward the parties processing personal data. The initial steps to get individuals engaged with such services will be difficult, but the development of standardized consent and individual rights management should be a priority for all data privacy professionals. It could be a solution for compliance issues, like conditions of consent and transparency, that many are already struggling with. But even more importantly, it is needed to balance the power between individuals and technology by equipping individuals with tools they can efficiently use to fight disproportionate intrusion and unnecessary or harmful data combination. //



# Privacy Assistance

## Beyond the Speed of Thought

**Alexander White, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPM, CIPT, FIP**  
*Bermuda privacy commissioner*

As a science-fiction fan, I relish the idea of imagining the future but have read enough to know the folly of writing it down. After all, by now we should have had flying cars, Jupiter colonies and all other manner of wonders (or horrors). With this risk in mind, I will nevertheless hazard a guess. By 2030, a technology just over today's horizon will be adopted for widespread use, empowering individuals to take control over their data and how it is used in a way that is simply beyond the capacities of mere mortals: an intelligent, artificial agent able to act on behalf of its individual human's personalized preferences.

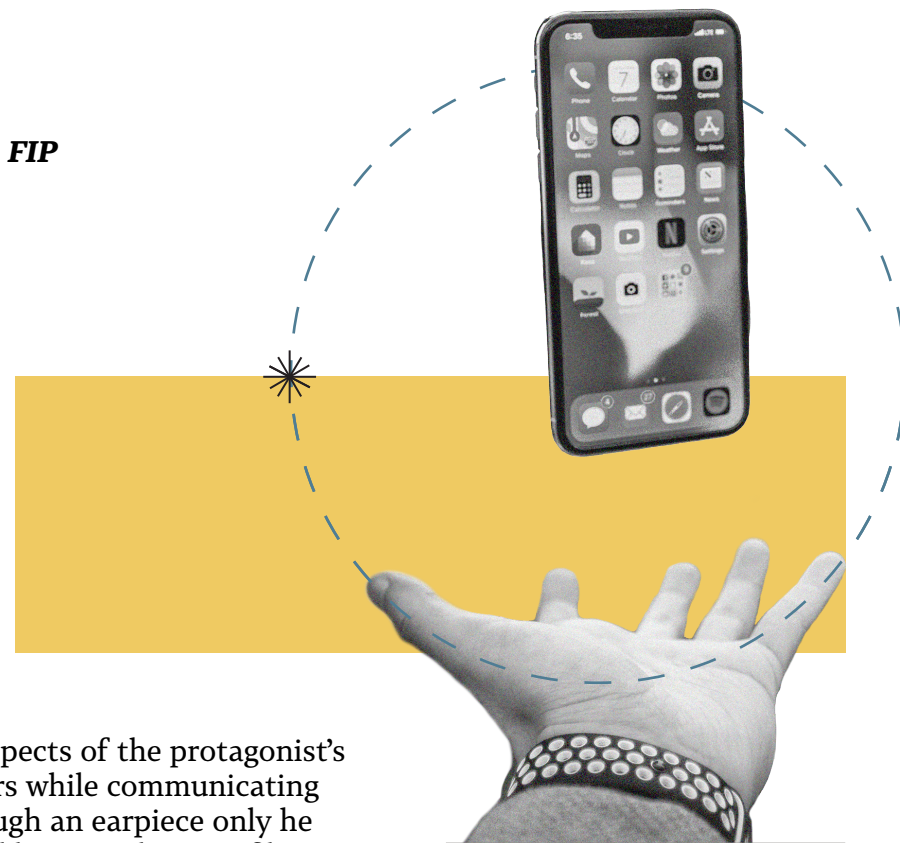
We've seen our fictional heroes and protagonists speaking to computers for decades, since at least HAL 9000 and the Starship Enterprise computer of the 1960s. Artificial assistants have

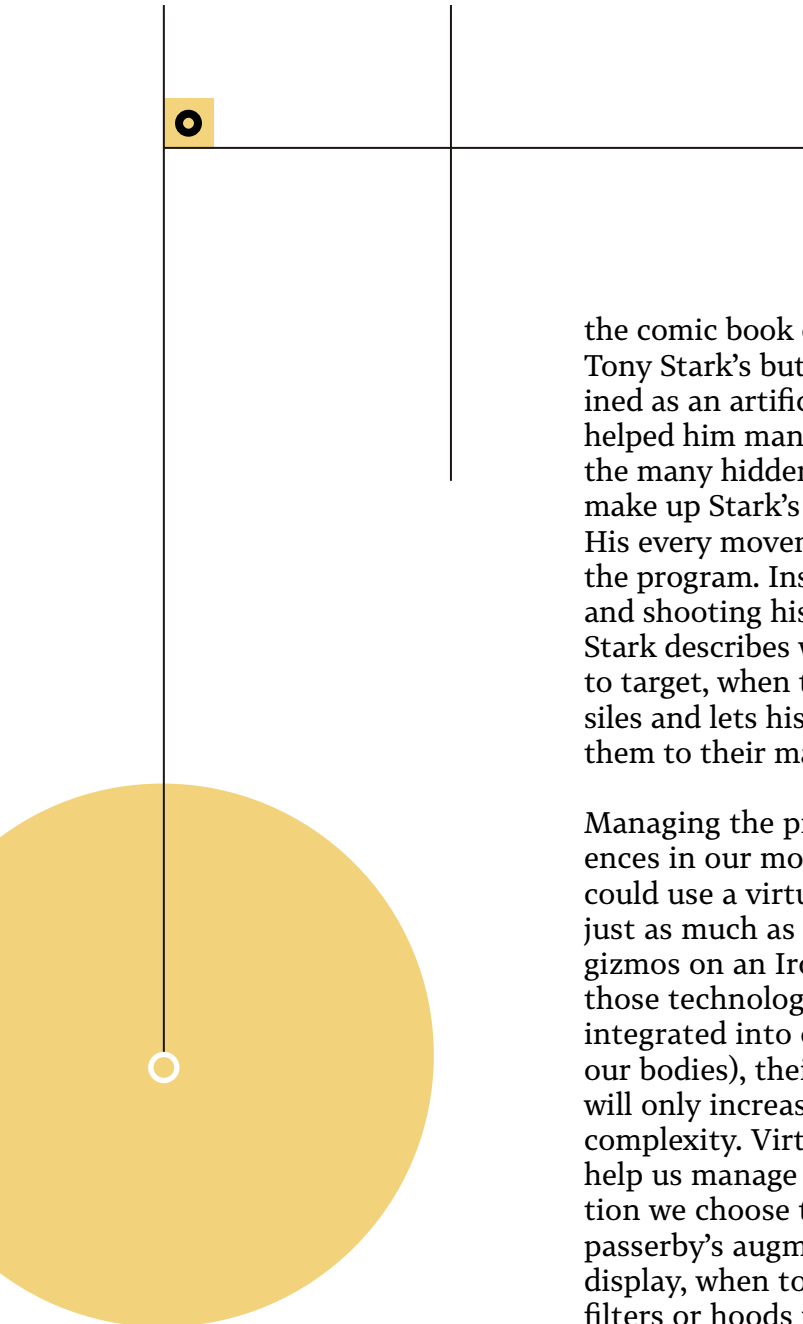
been tasked with handling the at-times unfathomably complex jobs of maintaining warp engines, fighting super villainous crime (KITT, "Knight Rider" and the Batcomputer, "Batman") or even traveling in time (Ziggy, "Quantum Leap") — while also serving as a convenient tool for exposition and to move the plot along. When things get complicated, just let the (super)computer do it.

More recently, in parallel with the concept of a computer itself shifting from a warehouse to a jacket pocket, we have seen a shift from thinking of artificial intelligence as a monolithic entity managing a vast enterprise to thinking of them as personal, customized for each individual user. In the 1986 novel "Speaker for the Dead," an "artificial sentient" named Jane ran

all aspects of the protagonist's affairs while communicating through an earpiece only he could hear. In the 2013 film "Her," virtual assistant Samantha was programmed to adapt to her user's personality, creating an intense bond between the two.

Perhaps the most famous modern example comes from the 2008 film "Iron Man," in which





the comic book character of Tony Stark's butler was reimagined as an artificial assistant that helped him manage and execute the many hidden gadgets that make up Stark's armored suit. His every movement is aided by the program. Instead of pointing and shooting his rocket launcher, Stark describes which bad guys to target, when to launch missiles and lets his assistant guide them to their mark.

Managing the privacy preferences in our modern technology could use a virtual assistant just as much as managing the gizmos on an Iron Man suit. As those technologies become more integrated into our lives (and our bodies), their interactions will only increase in number and complexity. Virtual agents will help us manage what information we choose to share with a passerby's augmented reality display, when to enable clothing filters or hoods to distort our

participation in public facial recognition, what data will be transmitted outside our bodies from our biological or medical implant, and any number of varied tasks.

Today, in our increasingly sci-fi world, we can now speak to our computers to request they conduct an internet search, execute a program command or, as their creators hope, buy stuff. While these assistants are responsive and draw from our profiles and history of commands to create customized search results or pre-load likely choices, they are certainly not an individual's agent empowered to act on our behalf. While many of us own a device that allows us to access the service, there is no such thing as "my" Alexa or "your" Siri — only Amazon's Alexa and Apple's Siri. (In another example of life imitating art, Microsoft chose to name their virtual assistant Cortana, due to the popularity of the

2001 video game "Halo" and the artificial intelligence character who guides the player.)

Once the day arrives that AI can act on our behalf as a true agent, solely answerable to the individual, such programs will revolutionize, among many other things, how individuals express their privacy rights and preferences. Like their fictional counterparts, they will learn our personalities, assist us in using complex technological tools and manage our larger affairs. These agents will empower all individuals to respond to the complex, fast-moving challenges presented by even the simplest online interactions.

For example, much has been made about the intricacies of privacy notices, which are often written at a reading level beyond that of the average individual, if not in full legalese. Even when a reader can parse the language,

*With the ability to update an individual's virtual agent at any time, organizations no longer need the foresight of an oracle. They simply must keep the dialogue open and respond to individuals' preferences.*



the notice may include vague wording that does not go into detail about specific uses, circumstances or contexts of which there could be an infinite variety. And, of course, there are hundreds, if not thousands, of organizations that collect or process an individual's personal data, each with their own policies.

The use of virtual agents could upend the model for how we learn of data practices and express our preferences. Recent head-to-head tests have shown algorithms can read contracts better than a team of lawyers

and in a fraction of a second. Virtual agents could inform the individual of what is really happening with their data in a way they can understand, to a level of detail they would prefer and at the times of their convenience. Then, and on an ongoing basis, agents could monitor organizations for changes to their policies or even to audit their practices.

Privacy is intensely personal, varying by individual. Once the agent has developed a personalized model for the preferences of its user, it could engage in real-time discussions with organizations that use personal data to grant or deny permission to proceed. At the time of data collection, when notice of practices should be provided, organizations may not be able to foresee the variety of circumstances, contexts or potential complications of processing personal data. With the ability to update an individual's virtual

agent at any time, organizations no longer need the foresight of an oracle. They simply must keep the dialogue open and respond to individuals' preferences. In other words, engage in good customer service with the added benefit of having a direct line to the customer's representative available at any time and for any length.

Virtual agents will represent an incredible leap forward in democratization of privacy rights, extending the reach and capability of the individual to express themselves and inform others of their preferences. The ability to protect privacy will no longer be limited to those who understand the technology or the time to pursue complaints. In an increasingly complex and interconnected world, we will increasingly rely on our virtual partners who can work beyond the speed of thought and may just know us better than any living being. //

# Privacy Law Will Become More Specialized in 2030

**Christopher Wolf**

*Hogan Lovells senior counsel and Future of Privacy Forum founder and board chair*

My prediction: By the year 2030, privacy law will become more specialized. Lawyers will no longer hold themselves out as “privacy lawyers” generally but rather will focus on particular statutes, technologies or industries resulting in many sub-specialties of privacy law.

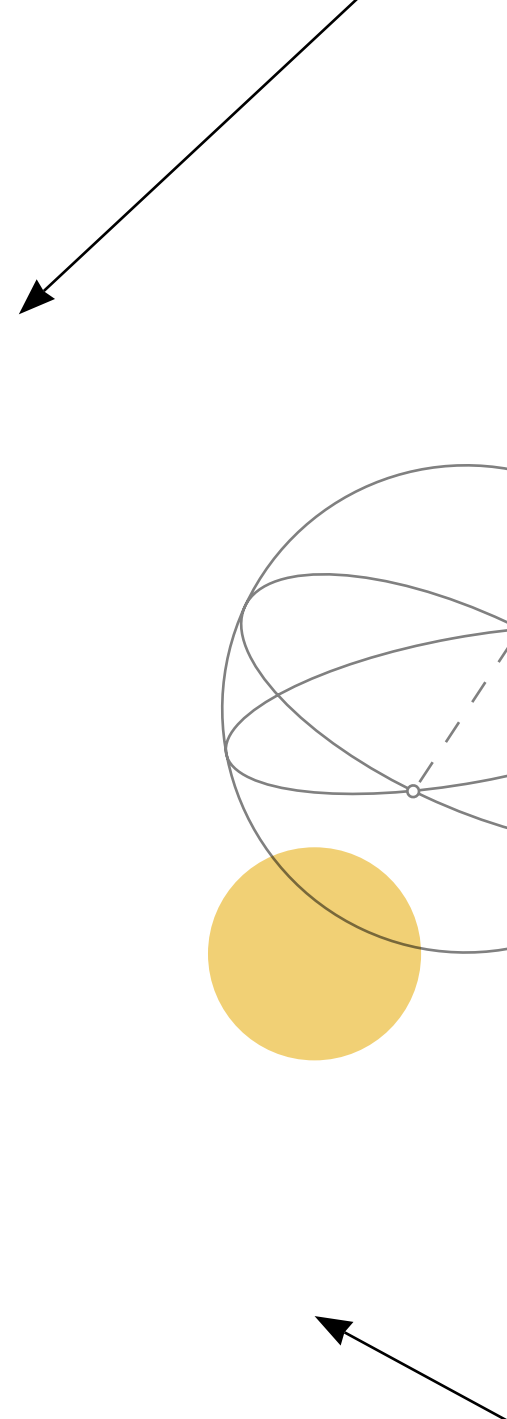
Thirty-nine years ago, I became a lawyer. For the first decade or so, following a judicial clerkship, I was a “generalist litigator.” Like so many litigators, my mildly arrogant philosophy was, “It’s a law; I’m a lawyer; I can handle it.” As a result, I tried cases involving international trade, antitrust, employment discrimination, intellectual property and more. I even represented the government of El Salvador in the International Court of Justice.

A case involving an early internet technology sent me to Silicon Valley for weeks and months at a time in the early-1990s, culminating in a long jury trial (we won; I try not to mention the cases I lost). That experience signaled to me this “internet thing” was going to be significant, so, I came home to Washington and declared myself an internet lawyer. I read and wrote as much as I could, attended and spoke at conferences, and stayed current with technological and legal developments. I was lucky enough to get some of the earliest internet-related cases. Thus, my transition away from being a generalist litigator began.

In 1998, Marc Rotenberg of the Electronic Privacy Information Center, whom I got to know in Washington charitable circles,

referred a pro bono case to me concerning violations of the Electronic Communications Privacy Act by the U.S. Navy. At the time, the Navy was accused of illegally obtaining information about a sailor to eject him from the service under the now-repealed “Don’t Ask, Don’t Tell.” We won that case (again, I only mention the winners), and the case made news since it was one of the rare times the military lost under “Don’t Ask, Don’t Tell.” A neighbor of mine in D.C. reached out to me to say how pleased he was with the result and to say a company he was advising was looking for outside privacy counsel. He connected us, and I had my first paying privacy client.

My early forays into privacy law reminded me of my first







exposure to the internet — “this area is also likely to grow and be significant,” I said to myself. And like the path I followed to earn my internet law bona fides, I set out to immerse myself in privacy law and policy. With substantial help from friends, I organized the first Practising Law Institute treatise on privacy law. I was a regular talking head at conferences, including early IAPP conferences. I developed a full-fledged privacy law practice. In 2008, I came up with the idea for the Future of Privacy Forum and joined forces with Jules Polonetsky to execute my dream.

In 2009, I fully abandoned the idea of being a generalist litigator and left the law firm that judged my value by the number of jury trials I first-chaired. I joined Hogan & Hartson (now Hogan Lovells), a firm well known for its regulatory practices, and had the honor of helping to lead what now has become one of the largest (if not the largest) privacy and

cybersecurity practices among global law firms.

My privacy law practice was much like my litigation practice I started in the 1980s. I was a generalist. I handled many varieties of privacy matters for many types of business and institutions: Federal Trade Commission and attorney general investigations, government and law enforcement access to data, assessments and compliance reviews, matters involving children’s privacy, cross-border transfers, data security and breaches, big data, internet-of-things and connected-car privacy, education privacy, location and advertising practices, mobile location analytics, and much more.

Fast forward to 2020, and I am retired. I no longer practice privacy law daily, although I still am engaged with Hogan Lovells as a senior counsel, and I still lead the Future of Privacy Forum board. My retirement provides a good

time to reflect on the future of the privacy law profession.

While it still may be possible for those who litigate to remain generalists, taking all comers, I have come to the conclusion that it soon will not be prudent or perhaps even possible for there to be a species of generalist privacy lawyers. As the recently enacted EU General Data Protection Regulation and California Consumer Privacy Act reflect, privacy laws are becoming more and more complex. And they are proliferating. Thus, practitioners advising or litigating under such laws need to be statutory experts. Case law will embroider the meaning of those statutes, requiring vast and in-depth knowledge.

Likewise, technology continues to develop rapidly. Although I still believe one does not have to be a computer scientist to practice privacy law (although it surely helps), you do have

to understand the technology and, at the very least, be able to interact with the experts. But even with expert help, it would be arrogant for privacy lawyers to claim working knowledge of all technologies affecting personal data.

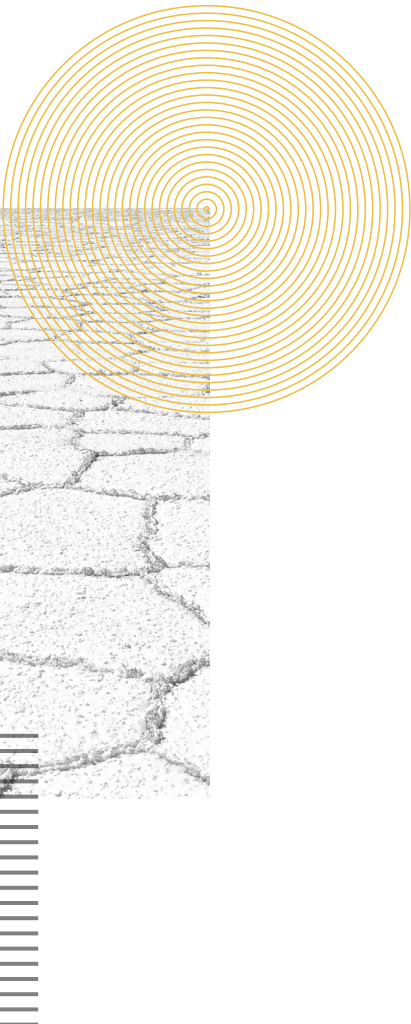
Just as health privacy lawyers and financial privacy lawyers have focused on discrete laws and technologies, the trend toward specialization will continue. I can see a day when there are recognized areas of privacy law specialization beyond health and finance.

While privacy law may not become as specialized as securities law, where practitioners are known to specialize even in one or two sections of the code, the growth in law and technology suggest that hanging out a proverbial shingle as a privacy lawyer generalist soon no longer will be viable. Privacy law specialization is coming. //

# An Anthology of Privacy Predictions

**Stephen Kai-yi Wong**

*Hong Kong privacy commissioner for personal data*



In this day and age, extensive and ubiquitous collection of personal data, both online and offline, together with the unpredictable use, transfer and breach of data, has posed unprecedented challenges to the data privacy frameworks around the globe. Worse still, individuals may not even be aware their data has been collected or shared. This makes exercising control over their data and objecting to unfair or discriminatory use of it next to impossible, even though personal data does not belong to any organizations but rather to the individuals from whom the data is collected. It being their own data, individuals would expect they are entitled to have the legitimate control or self-determination over it. On the other hand, in this data-driven economy that keeps growing in parallel with big data and information and communications

technology developments from which individuals benefit tremendously, particularly in relation to scientific advancement and social interactions, it would not be in the interest of the community at large to have data locked up. Regulators worldwide are seeking to strike a balance between data protection and a variety of competing interests and rights.

Fragmented regulatory frameworks around the world — in Asia, in particular — have been a major concern for organizations having international or inter-regional operations. Fraudsters and cyber-bullying activists, for example, may find them a blessing, though. Naturally, individuals would look up to regulators. In the pursuit of effective data protection addressing, in particular, the sans frontiers nature of digital data flow, there is no

justification for regulators not to put their heads together for a de-fragmented regulatory framework, if not a harmonized one. Similarly, international internet-related organizations will have all the reasons to reach a consensus on how best personal privacy and security with popular content and services could be balanced.

Compliance with the law is but part of the data ecosystem. While resonance of accountability has started to tune up, complementing compliance with the law by adopting data ethics will form the bedrock for nurturing and flourishing data protection in times of change. Data ethical values typically center on fairness, respect and mutual benefits. In practical terms, they involve genuine choices, meaningful consent, transparency, no

*It is almost inevitable that much of the information or behavior we consider private today will not be so as time goes on.*

bias or discrimination, and fair negotiation or exchange on a level playing field between organizations and individuals.

By adopting an ethical data stewardship framework, an organization is expected to consider the rights, interests and freedoms of all stakeholders in planning and conducting its data-processing activities. The stakeholders do not only include the clients and customers of the organization but also other individuals who may be impacted by the data-processing activities, as well as society as a whole.

Essentially, individuals expect no surprises when they deal with organizations in relation to their personal data. Individuals'

expectations, alongside their behavioral profiling, will become a constant in the organizations' demand function, and the equilibrium against their supply of products or services will need to be adjusted from time to time.

So will the regulators. One of the challenges regulators have to continue to meet will be how they could help unlock and share personal data within the legal and ethical frameworks in the midst of widely applied sensory ability, cognition, robotics, machine learning and cloud services, etcetera, with a view to maximizing the benefits of data in a sustainable way, minimizing the risks and harms, creating healthy synergy with economic growth, and identifying and

securing the innovative use of personal data in a post-data-driven economy. It is almost inevitable that much of the information or behavior we consider private today will not be so as time goes on.

Data protection policies, regulations and practices are invariably lagging behind ICT developments. While privacy-protective technology will continue to grow in power and magnitude, so will privacy-intrusive technology. We have never had ubiquitous surveillance before. Nor have we had internet social platforms or applications capable of influencing political results. That said, individuals will tend to give up more and more of their personal data than before for ease and convenience, if not to be trendy, especially in the emerging economies. The balancing exercise, whether on the part of regulators or organizations, that is working today may not be seen as workable in the year 2030.

While the balance will need to be adjusted constantly, a common denominator will ultimately be acted upon (i.e., respect and trust), which is being built among all stakeholders and will be pivotal to the balancing exercise. Notwithstanding the nature of privacy right being a fundamental human right, encroachment of the right may be justifiable, such as for the purposes of detection and investigation of crimes, or where public interests dictate. Organizations, public or private, will have to respect individuals' privacy right to win their trust. Individuals will continue to expect organizations to do not only what they are required to do by the law, but also what they ought to do ethically. Regulators will need to play the roles of law enforcers, educators and facilitators in a respectable way. The evolution from an established privacy structure to a practicable privacy culture will probably take 10 years, if not more. //