



Privacy technology: What's next?

**The evolution of data-privacy
technology in the age of automation**

OneTrust
PRIVACY, SECURITY & GOVERNANCE

KPMG International

home.kpmg/cybersecurity



Executive
Summary

Change
drivers

Connecting
technology...

The changing
consumer...

The rise
of privacy...

What about
enterprise...

A plan
forward

About KPMG

Foreword



Costly data breaches. Ongoing security issues. Personalization of online services. Intrusive advertising tactics. Sharing of consumer data. Consumers are raising red flags about how today's businesses are using and protecting their personal data and their concerns are rapidly driving the issue of consumer data privacy up the boardroom agenda.

Consumers are not just concerned about data protection — they want greater control of access to their personal data and how it is ultimately used by businesses. Regulators are also paying close attention and continue to enact stringent laws aimed at 'bad' data gathering and sharing practices.

KPMG's *Me, my life, my wallet* study found that 55 percent of consumers cited data protection as their primary expectation of companies, with 47 percent also saying they expect companies to never sell or share their personal data.¹

At the same time, trust in businesses is suffering among dubious consumers. KPMG's *The new imperative for corporate data responsibility*² report found that 68 percent of consumers surveyed do not trust businesses to ethically sell their personal data. Fifty percent of consumers also said they do not wholly trust businesses to protect their data.

Ongoing consumer trends — from ubiquitous smartphones and social media channels to the massive shift to online shopping, personalized customer experiences and more — are driving an explosion of consumer data. Fast-emerging technologies such as 5G, the Internet of Things (IoT) and artificial intelligence, meanwhile, are poised to dramatically heighten both connectivity and the endless data wave — along with the complexity of data security and privacy protection.

Data-privacy technology will need to mature quickly to effectively manage today's endlessly expanding data universe. In this report, we examine where data-privacy technology and management are going — and needs to go — to effectively respond to a complex and fast-evolving environment.



Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International



Kabir Barday
President and CEO
OneTrust

[Executive Summary](#)[Change drivers](#)[Connecting technology...](#)[The changing consumer...](#)[The rise of privacy...](#)[What about enterprise...](#)[A plan forward](#)[About KPMG](#)

Contents





Executive
Summary

Change
drivers

Connecting
technology...

The changing
consumer...

The rise
of privacy...

What about
enterprise...

A plan
forward

About KPMG

06

Executive
Summary

08

Change
drivers

12

Connecting
technology
to privacy

16

The changing
consumer
technology
landscape

20

The rise of
privacy-centric
solutions

30

A plan
forward

24

What about
enterprise
technology?

34

About KPMG



Executive Summary



Consumer concerns about data privacy and security are rising up business agendas everywhere. As fast-evolving consumer technologies and applications proliferate, the need for enhanced controls and transparency regarding personal data use is unmistakable. And the picture is growing more complex against the backdrop of 5G, the Internet of Things (IoT) and other game-changing technology advances.

Nations around the globe are enacting new privacy laws while regulators are looking to new global regulations amid consumer concerns and trust issues over online tracking, unauthorized data sharing, consumer-targeted advertising, data breaches and more. The sheer volume of potential regulatory changes, combined with emerging technology, growing threats and rising public awareness, is creating unprecedented pressure on organizations to respond appropriately.

Today's data challenge can only be tackled with privacy technology that's designed for a bold new age of data use and management. Organizations are racing to create or expand data-privacy programs, systems and tools, and adhere to new privacy standards, in a bid to keep up with fast-changing perspectives and demands.

We are also seeing wary consumers turning to personal data vaults, data rights-as-a-service providers, data trusts and more to exert new controls over their data. Meanwhile, Privacy Enhancing Technologies, next generation privacy portals and other emerging capabilities will support the drive to appropriate data management. And not to be ignored along the way is the need for a trustworthy data-ethics framework.

Organizations ultimately must devise the perfect 'data compound' — the precise 'mix' of personal data elements that will unlock new opportunities for insight-based decision making, innovation and revenue growth, all while ensuring that privacy, security and ethics concerns are effectively managed.

"Technology and its accompanying data trails permeate so many aspects of our lives that organizations must earn and sustain trust, or wary consumers will be reluctant to share the critical data that businesses need to become data-driven and customer-centric," says Sylvia Klasovec Kingsmill, Global Cyber Privacy Leader, KPMG International.

"Trust in the digital era goes beyond the quality of an organization's brand, products, services and people. It's also about the trustworthiness of data use and management," he adds. "The challenge ahead is to prove that businesses are protecting the customer data they are using to create value and drive success. Privacy technology presents a huge opportunity in supporting organizations on this journey and those who get it right will have an advantage in demonstrating that they are protecting the customer data they are using to create value and drive success."



Executive
Summary

Change
drivers

Connecting
technology...

The changing
consumer...

The rise
of privacy...

What about
enterprise...

A plan
forward

About KPMG



Change drivers

**What's accelerating the
journey to automation?**



As technology makes data collection and processing pervasive, consumer concerns and awareness of privacy rights have moved into the spotlight among businesses and regulators, prompting organizations to change the structure and operations of their privacy programs. Whether creating or expanding a privacy program or adhering to a new privacy standard, organizations are pursuing strategic operational changes to keep up with changing perspectives on privacy protection.

As the scale of work required for privacy teams increases exponentially, and demand for new skills around privacy engineering and data evolve, privacy teams are at a crossroads: How can they be effective, efficient, consistent and timely at scale regarding necessary data security and protection?

More than 100 countries³ have now enacted privacy laws, while global regulations, combined with consumer outcries over online tracking and advertising, unauthorized data sharing, crippling data breaches and more, have heightened the need for an integrated approach to privacy compliance across all business activities.

While technology alone is not the answer to privacy and compliance challenges, it certainly plays a crucial role as businesses interact 24/7 with employees, customers, stakeholders and the consumer marketplace. The following infographic traces the evolution of privacy-protection measures for the public.

“Privacy technology has exploded over the last few years — and with good reason. The introduction of the GDPR, along with heightened awareness by consumers of the risks and their rights, has necessitated organizations shifting from inefficient manual processes to automated ones in order to keep up.”

Matthew Quick
Privacy Lead
KPMG Australia



Evolution of privacy protection

1361

England's Justices of the Peace Act criminalizes "peeping Toms" and eavesdroppers.⁴

1792

US Congress passes a law enforcing privacy of letters.⁵

1800s

Sealed envelopes are invented.

1858

Attempts by newspapers to publish drawings of Elisabeth Félix on her deathbed lead to the development of Privacy laws in France.⁶

1888

Eastman Kodak invents the snapshot film camera, sparking alarm about privacy intrusion.⁷

1890

US lawyers Samuel D. Warren and Louis Brandeis publish 'The Right to Privacy' in the Harvard Law Review, prompting recognition of privacy as a legal right, after photos of Warren's dinner parties appeared in a gossip magazine.⁸

1907

World's first 'bugging device' — the dictograph — is invented.⁹

1928

US Supreme Court declares wiretapping private phone calls illegal.¹⁰

1948

UN Declaration of Human Rights establishes the right to privacy.¹¹

1994

Netscape releases browser that makes online tracking possible for the first time.¹²

1995

European Union adopts the Data Protection Directive.¹³

1997

Social media emerges with the launch of SixDegrees.com. LinkedIn follows in 2002, Facebook in 2004 and Twitter in 2006. SixDegrees — based on the idea that everyone is connected to everyone else in six steps — closes in 2001.¹⁴

1999

Sun Microsystems CEO Scott McNealy declares: "You have zero privacy anyway — get over it."¹⁵

2000

US and EU sign the Safe Harbor agreement allowing the transfer of European citizens' data to the US.¹⁶

2000

Ericsson releases the first device marketed as a 'smartphone' — combining a mobile phone, a PDA, limited web browsing and touchscreen.¹⁷

2008

App Store is launched. The use of data-driven mobile apps transforms the mobile device into an immensely powerful personal information processing and sharing device.¹⁸

2010

Facebook changes the default setting for user profiles from 'private' to 'public'.¹⁹

**2010**

Facebook CEO Mark Zuckerberg declares: "Privacy is no longer a social norm."²⁰

2011

Latest smartphone releases include features to track users.²¹

2012

Facebook users increase shared content to seven billion pieces a week. A US survey shows 70 percent of customers don't trust social media with their data.²²

2012

For the first time, more people use mobile apps than mobile internet. Meanwhile, the makers of 'Girls Around Me' are forced to withdraw their app. It allowed users to identify girls near their location, based on publicly available data.²³

2012

The New York Times declares the "Age of Big Data" amid the proliferation of sensors, new forms of data and increasing storage capacity.²⁴

2013

WikiLeaks helps Edward Snowden release classified information showing widespread surveillance by Western intelligence agencies. The revelations spark a global debate about national security versus individual privacy.²⁵

2014

Tech publications declare 2014 "The Year of the Wearable." Sales of smartwatches and smart wristbands hit five million and 15 million respectively.²⁶

2015

Humans create 2.5 quintillion bytes of data a day, equivalent to 625 million DVDs.²⁷

2015

European Court of Justice says Safe Harbor is no longer a valid way of transferring data between Europe and the US.²⁸

2015

The Internet of Things take off, 16 years after the term was coined. Among the milestones this year: Amazon launches a service offering voice control over home systems. Cisco estimates 15 billion IoT devices.²⁹

2016

'Dark Patterns' emerge where algorithms use data to predict future behavior.³⁰

2016

The EU enacts the *General Data Protection Regulation* (GDPR) — the biggest change in data-protection laws in more than 20 years, imposing a single set of rules and tougher penalties across the EU.³¹

2018

After the GDPR goes live, the EC issues several multi-billion-Euro fines.³²

2019

A number of high profile organizations are fined for GDPR breaches.³³

2020

Covid-19 pandemic has a worldwide impact on everyday life and livelihoods.

2020

CJEU decision on Schrems II lands ruling that the EU-US Privacy Shield is invalid.³⁴

2020

Data Protection Authorities levy further fines on organizations for GDPR breaches.

2021

Council of the European Union agrees on negotiating mandate for ePrivacy regulation allowing for start of dialogue between the Council, the European Parliament and the EC.³⁵

2021

Virginia's Consumer Data Protection Act is signed into law, joining the California Privacy Rights Act (CPRA) as the second state-wide US privacy bill.³⁶

2021

Fines continue, with organizations being fined tens of millions of dollars by the State Commissioner for Data Protection in Lower Saxony³⁷ and by the AEPD in Spain.³⁸

The Future

Technology is eroding consumer privacy at an unprecedented rate. Will it have disappeared altogether by 2050 — or will consumers take it back?



Executive
Summary

Change
drivers

Connecting
technology...

The changing
consumer...

The rise
of privacy...

What about
enterprise...

A plan
forward

About KPMG



Connecting technology to privacy

**Leveraging privacy tech to cover the
full scope of privacy**



While businesses increasingly rely on powerful new technologies and tools to unite disparate systems and automate operations, today's new age of privacy awareness is also forcing organizations to evolve privacy systems and programs. In the race to enhance data security and privacy protection, technology continues to replace manual processes and ultimately help businesses meet global privacy laws.

As we move into the next generation of privacy technology, we are seeing privacy technology generally aligned to three key areas: *process orchestration, personal data management and governance, risk management and compliance (GRC)*.

“Privacy technology has rapidly evolved into a mature industry and is front and center on the Chief Privacy Officer's agenda for many of our clients. It's important to approach this space through an ecosystem lens as opposed to siloes: the art of privacy automation is very much a function of weaving together complementary technology for the various facets of data management, protection, and privacy to help streamline and drive efficiency and cost effectiveness in privacy program management.”

Orson Lucas
Privacy Lead
KPMG in the US



Process Orchestration

Process orchestration is the standardization of a process to improve operations and efficiency. By utilizing process orchestration, including the use of automation, organizations can reduce the time, money and resources needed to ensure that tasks and processes are completed consistently and continually improved.

This can be critical for privacy teams in meeting obligations to consumers and regulators. But what could process orchestration look like in a privacy-tech solution — for example in responding to an individual's request for access to their personal data? In a manual approach, responses are likely to be inconsistent or inadequate, take longer than needed and require dedicated teams project managing complex responses.

Process orchestration manages such requests in a structured format that heightens efficiency and reduces cost. The benefits of process orchestration can also be aligned to KPMG's Six Pillars of customer experience excellence³⁹. Organizations that understand and deliver against the Six Pillars enhance outcomes, grow more quickly and increase shareholder value.

Personal Data Management

Personal data management at its core is the practice of collecting, retaining and using data effectively and securely. Organizations do this in many ways, whether a retailer dealing with payment and shipping information or an organization maintaining sensitive contractual information for a client.

Organizations need to know where all the personal data collected is going and exactly what is being done with it. Beyond meeting consumers' privacy demands and expectations, mapping and managing data is particularly critical amid privacy

The Six Pillars of experience excellence





“Privacy technology brings automation, scalability and innovation to the forefront when implementing privacy frameworks and controls. It’s crucial to the success of large-scale privacy transformation programs, reducing costs, and accelerating lead time to deploy privacy processes, so that privacy practitioners can focus on driving change rather than on mundane operational tasks.”

Maliha Rashid

Privacy Lead
KPMG in the Lower Gulf Region

regulations governing storage, retention and usage. This also plays into compliance regarding the sharing, localization or deletion of data.

Privacy-tech solutions can raise personal data management and record keeping to new levels of speed, accuracy and efficiency. Solutions offering automated data discovery can accelerate identification of personal data sources and effective fulfilment of consumer requests. These solutions may also offer delivery of additional data protection requirements via automation of encryption, masking and access control.

GRC

Governance, risk management and compliance (GRC) spans a wide range of responsibilities and can take on many different forms. At the heart of effective GRC is a connected data model that links privacy-related risks and compliance controls to enterprise risk categories such as reputational risk and regulatory compliance.

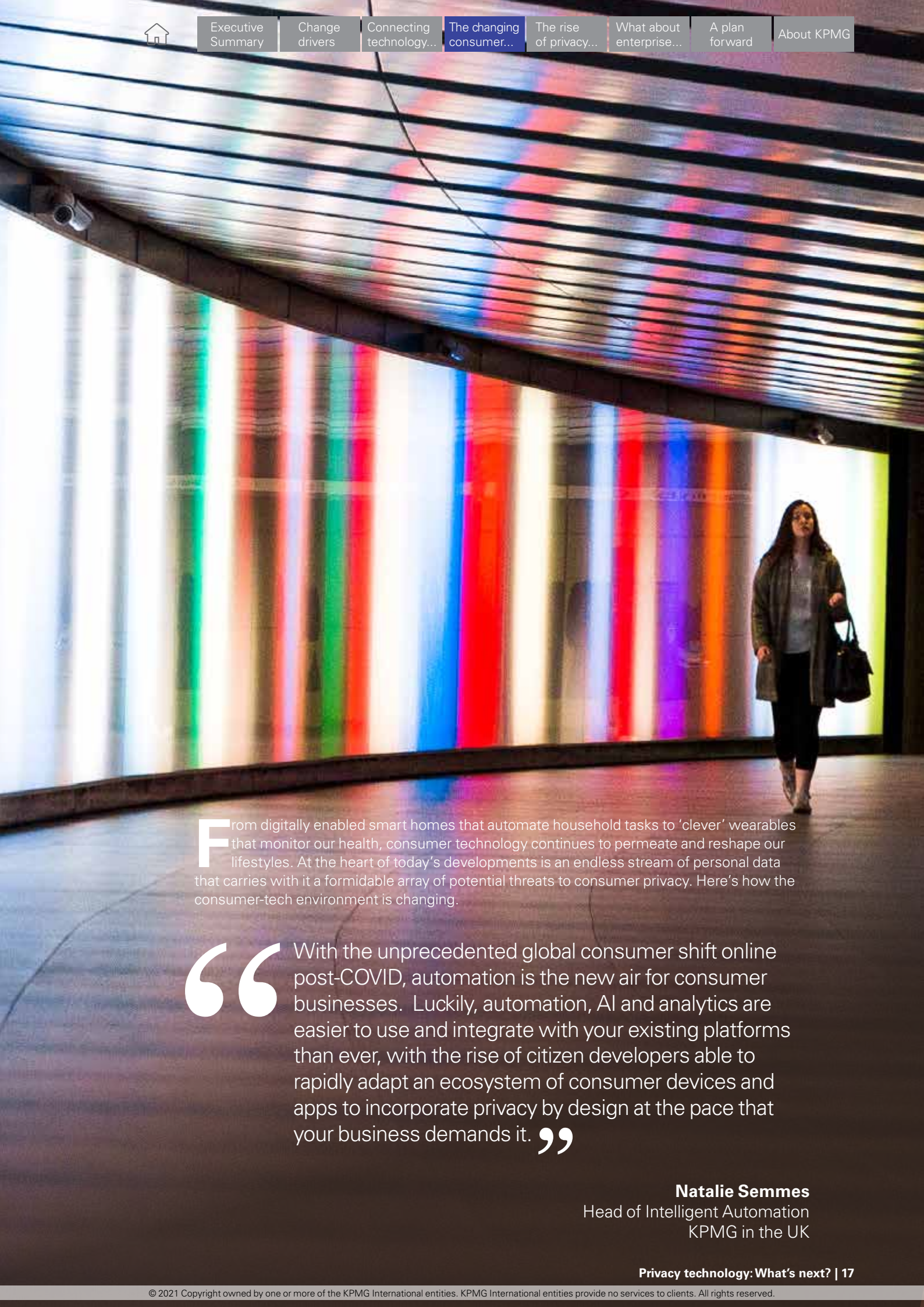
Smart businesses are increasingly looking at GRC more broadly to include a customer lens and this is driving more-trusted outcomes. We are now seeing a move toward Integrated GRC or Integrated Risk Management to gain a connected view of risk across all lines of defense and all risk types, including technology, conduct and privacy. From a GRC technology perspective, a ‘risk ecosystem’ is an important trend.

For enhanced privacy, you will see process orchestration and GRC management processes integrating with best-of-breed privacy-tech capabilities to offer end-to-end, holistic management of privacy risks. Looking ahead, data-driven GRC to drive real-time insights will soon become the norm and transform how we understand and manage privacy risk.



The changing consumer technology landscape

The continuing impact of consumer technology on our lives



From digitally enabled smart homes that automate household tasks to ‘clever’ wearables that monitor our health, consumer technology continues to permeate and reshape our lifestyles. At the heart of today’s developments is an endless stream of personal data that carries with it a formidable array of potential threats to consumer privacy. Here’s how the consumer-tech environment is changing.

“With the unprecedented global consumer shift online post-COVID, automation is the new air for consumer businesses. Luckily, automation, AI and analytics are easier to use and integrate with your existing platforms than ever, with the rise of citizen developers able to rapidly adapt an ecosystem of consumer devices and apps to incorporate privacy by design at the pace that your business demands it.”

Natalie Semmes

Head of Intelligent Automation
KPMG in the UK



IoT, 5G and edge computing

As the Internet of Things (IoT) expands — with estimates of IoT-connected devices (11.7 billion) outnumbering non-IoT connected devices (10 billion)⁴⁰ by the end of 2020 — so do related privacy challenges.

While these have the potential to deliver significant new customer experiences and services, personal to our every need, want and desire, the data which they will be processing is increasing exponentially. Looking ahead, a key driver for continued IoT growth will be the successful roll out of 5G technology, and the ongoing development of edge computing. 5G offers higher speed, lower latency and increased bandwidth to support billions of connected devices transmitting unprecedented data volumes. Edge computing will enable data processing near the data source, reducing the amount of data that must be transported centrally.

As these developments promise to dramatically improve the speed, scalability and efficiency of business interconnectivity, they pose new privacy concerns as technology providers collect increasingly granular data points to create a rich digital footprint.

If privacy and security considerations do not keep up, then it is almost inevitable that personal data will be leaked, revealing more and more about our personal habits.



“5G and edge computing represent the platform on which the next industrial revolution will be delivered. The organizations that will thrive are those with ambitious visions and disruptive models that seem to glide effortlessly through the digital economy, achieving astounding earnings, customer growth rates and market share targets time and time again.”

Alex Holt

Global Head of Telecoms & Media
KPMG in the US



Artificial Intelligence (AI)

AI continues to evolve and is magnifying the ability to use personal data in ways that threaten privacy. The reliance on using personal data to generate insights can clash with individual's expectations of privacy when their data is used in unexpected or potentially unauthorized ways or where results are generated that harm individuals' interests. Concerns over AI use include emerging use cases of facial-data recognition that can be considered invasive or the use of AI and machine learning algorithms to infer or predict sensitive information from non-sensitive forms of data.

There are strong arguments around algorithm bias and how technology inadvertently amplifies systemic discrimination and the inherent privacy challenges with consent, choice and automated decision making.

As AI initiatives move from machine learning to deep learning, with artificial neural networks that can learn and make intelligent decisions on their own, AI is starting to also play a bigger role in how organizations interact with consumers for example via AI-driven digital assistants.⁴¹

What's clear is that as AI and machine learning capabilities advance, organizations will likely need to keep consumers informed about how their data is being used to drive business insights and automated decision making.



Augmented and virtual reality

Virtual reality, augmented reality and mixed reality blur the edges between real and digital worlds. Mixed reality sits between a fully immersive virtual-reality experience and a digitally enhanced augmented reality experience by combining real and digital experiences.

The potential in these technologies have been spotted by many. Non-profit organization Charity:Water took 400 guests from their seats at The Metropolitan Museum of Art to Ethiopia to follow 13 year old Selam⁴² as she went on her daily journey to bring water to her family.⁴³ In the gaming world, Pokemon Go remains a long-lasting example of the power of augmented reality.

As COVID-19 reshapes working environments, attention is turning to these systems to provide virtual interactions, plus enhanced customer experiences. However, at the heart of these technologies lies the constant collection of biometric data and information from consumer apps. Developments in the technology could further increase privacy concerns — data collected through the tracking sensors could be used to create more convincing deepfakes and while improvements in eye tracking may be used to improve the user experience it also offers advertisers the chance to measure interaction with targeted advertising with unerring accuracy.

As new virtual and augmented-reality systems are being rushed to market, appropriate privacy considerations cannot be overlooked.



Social networking, collaboration and technologies

Social media users' concerns about privacy have spiked in recent years. Repeated data leaks, the potential misuse of profile data and security issues have caused users to rethink their relationships to social media and the security of their data.

Privacy concerns continue unabated and we have seen as a result an explosion in consumers' adoption of privacy-protecting technology.⁴⁴ At the same time, however, only one third of consumers have updated their social media privacy settings in the past 12 months, while only 24 percent have created stronger passwords.⁴⁵ The global pandemic's impact on remote working and the proliferation of online virtual meetings, meanwhile, has been fraught with security and privacy issues.

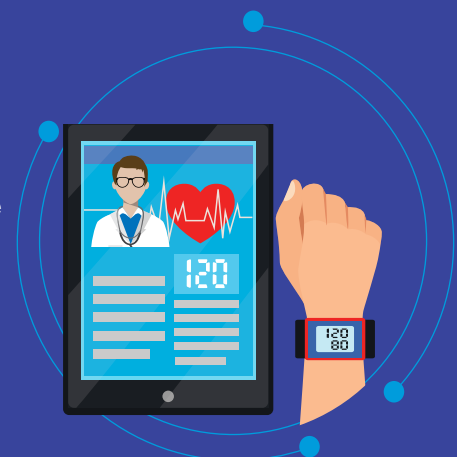
Consumers are becoming more aware of the privacy implications related to social media sites and collaboration technologies and we hope to see more secure systems emerging.

Healthcare technology

Cutting edge technology developments have long been adopted by the healthcare industry and applied to patient settings — from the application of IT to patient records to create electronic health records in the 1970s, the use of personal digital assistants for daily clinical practice in the 2000s to the use of virtual reality to create 3D models for surgeons to practice before a surgery in the present day.

More recently the growth in IoT has been reflected in the development of consumer medical devices. An example of this includes Medtronic partnering with Fitbit to integrate data collected from continuous glucose monitors with Fitbit activity trackers.⁴⁶ Looking ahead, the development of 5G's increased connectivity will advance health monitoring capabilities and enable more rapid responses by healthcare providers.


However, these advancements also raise questions about sensitive personal data. According to a recent Kantar study, just 38 percent of surveyed consumers believed that today's healthcare technology is providing adequate data security.⁴⁷



[Executive Summary](#)[Change drivers](#)[Connecting technology...](#)[The changing consumer...](#)[The rise of privacy...](#)[What about enterprise...](#)[A plan forward](#)[About KPMG](#)

The rise of privacy-centric solutions

How privacy technology is evolving



As consumer technologies evolve, so do privacy-centric solutions designed to help consumers manage their data and privacy rights.

Personal data stores and data privacy vaults

Personal data stores offer consumers a centralized location to safeguard personal data. Typically, solutions allow individuals to create and manage an inventory of personal data and choose how it can be shared.

However, many of these solutions are yet to become mainstream. And while a centralized store of personal data offers a simple way to manage data and act as the single source of truth should that copy be stolen the impact on an individual's privacy can be amplified. At the same time, consumer demand for greater data control may serve to incentivize development and adoption of personal data stores, while the potential for insights from personalized dashboards could prove enticing for some.

Data too may continue to be the allure for organizations with the potential to access accurate 'zero-party data' — data that has intentionally been created and kept up to date by the individual. However, in the absence of mass adoption by individuals, organizations are unlikely to see the benefits of introducing frictions into existing processes to collect data.



Data trusts

The principle of centralized management of personal data offered by personal data stores can also be seen with data trusts. Defined by The Open Data Institute as ‘a legal structure that provides independent, fiduciary stewardship of data,’⁴⁸ individuals give control of their data to a trustee who decides, on behalf of the individuals, who is able to access and use that personal data, and for what purposes.

Should an organization using personal data provided by the trust fail to comply with privacy requirements, data access can be revoked. The data trusts also prioritize the maintenance of data interoperability while also seeking to ensure that users fully understand the use of their data and have consented to its use.

Data trust development remains nascent, however, with several challenges to overcome, including the need for universal standards for the development of data trusts and the applicability of trust law. Examples such as John Hopkins⁴⁹ development of a data trust for medical research show the potential, while the identification of trusts as method to empower individuals to exercise their rights by the European Commission’s ‘A European Strategy for Data’⁵⁰ suggests that data trusts warrant further investigation.

The development, and widespread adoption, of Privacy Enhancing Technologies may further encourage the growth of data trusts via a federated approach, ideally reducing a trust deficit and encouraging more organizations to sign up.

Data rights-as-a-service

The EU’s General Data Protection Regulation (GDPR) and the development of other privacy regulations globally has helped to formalize data-subject rights, enshrining into law several rights for individuals. Alongside this, the growing number of publicized data breaches and fines have increased consumers’ focus on data privacy.

As such, consumers are becoming more aware of how to exercise their data-subject rights. In response, the data rights-as-a-service industry is allowing individuals to automate their subject access rights, reduce their digital footprint and remove personal data from search engines and other data aggregators, or mask their email identities online.

As emerging technologies pervade into our lives, data rights-as-a-service, offer consumers the chance to exercise their rights in an efficient and automated way.

Privacy-centric browsers

Browsers have long been a battleground for privacy rights, with browser services facing off against privacy advocates. Consumer adoption of privacy-centric browsers, meanwhile, has shown that consumers are joining the battle over privacy rights.

In the absence of appropriate configuration, usually requiring positive actions from the consumers to do so, most browsers typically collect vast amounts of personal data as you browse the internet — browsing history, login credentials, data collected by cookies or tracking mechanisms, autofill information and more.

Third-party cookies facilitating sharing of this personal data with a vast chain of third parties have recently come under the microscope with several larger browser makers announcing plans to remove or replace third party cookie collection. While several solutions have been proposed by major browser makers, more privacy-centric browsers have entered the battle late on offering to keep data about online consumer activity on their device and block trackers embedded into websites.



Global Privacy Control

The Do Not Track mechanism, originally proposed in 2009, was intended to act as a signal for users to opt-out of tracking by websites. However, a lack of widespread adoption by industry meant that even if individuals enabled the Do Not Track feature within their browsers, there was no guarantee that this signal would be respected. As such, the W3C disbanded its working group in January 2019.⁵¹

Picking up where Do Not Track left off, the Global Privacy Control (GPC) is a new browser mechanism designed to send a Do Not Sell (or Do Not Share) signal to a participating company's website. The GPC is also intended to signal when consumers do not want to share data with third-party data brokers. A number of browsers have announced plans to send the GPC signal by default, with a growing number of publishers and other online organizations signing up.⁵²

“Technical capabilities are a must in privacy management. Technology facilitates the management of privacy obligations and requirements throughout the whole lifecycle of information, from simple functionalities such as data categorization, PIAs and rights to more advanced measures such as anonymization, encryption and data deletion.

In the digital world, privacy is alive more than ever. Recently, we have seen in the European Data Strategy that measures for protecting the processing of personal data and increasing customer trust have become the norm for AI and large-scale data usage in analytics. Technology solutions could help in this process by enabling the implementation of mature privacy processes.”

Javier Aznar Garcia
Privacy Lead
KPMG in Spain



Executive
Summary

Change
drivers

Connecting
technology...

The changing
consumer...

The rise
of privacy...

What about
enterprise...

A plan
forward

About KPMG



What about enterprise technology?

The need for enterprise technology to keep pace



As consumer technologies quickly evolve, along with consumer-privacy tech, organizations themselves need to respond to the key drivers of change impacting their privacy-technology landscape.

Regulatory drivers of technological change

As with the Data Protection Directive 95/46/EC, the GDPR has ultimately set a foundation for global privacy regulations that have forced organizations to re-evaluate their privacy-compliance practices and move to a higher baseline of standards.

However, this represents just the start of the regulatory evolution, as countries such as China, Brazil, Thailand, India and others increasingly look to enact their own transformative privacy regulations.

While enhanced privacy regulations present benefits, the sheer volume of potential regulatory changes increases pressure on organizations to keep track of, understand and meet these requirements.



The hurdles presented by the patchwork of regulations can only be tackled and scaled with privacy technology. Smart companies will lean on advanced technology to handle cross-channel privacy compliance strategy and implementation. This technology allows for a convergence of different types of technology into one holistic platform within a streamlined privacy-management system.

From data as a liability to value creator

Many organizations see data as a liability in the absence of sufficient controls. This is no personal data ‘catch 22’ but if privacy requirements are addressed appropriately, organizations can meet privacy obligations while also creating value from data.

Consumers want the right to control their data. New privacy regulations present challenges with consent management, while creating the opportunity for unique personalized user experiences across multiple channels. Technology solutions allow marketing teams to create a single source of truth across multiple systems and manage consent across various collection points.

A transparent approach to customer data use builds trust. Organizations can collect and sync preferences across various channels and drive better opt-ins and marketing results. Marketing compliance can be automated by integrating privacy into existing marketing technology to sync preferences throughout marketing and sales.

Ultimately, privacy experts can’t be the only ones championing the privacy agenda. Organizations must also protect consumers, prioritize client engagement and preferences around data management, and integrate customer privacy journeys to create a positive experience.

Balancing identifiability and usability

Balancing identifiability and usability have long been a conundrum for organizations. While regulations such as the GDPR make it clear that the principles of data protection do not apply to anonymous information, organizations must ensure that anonymization truly removes any chance that the individual can be re-identified. Merely trying to



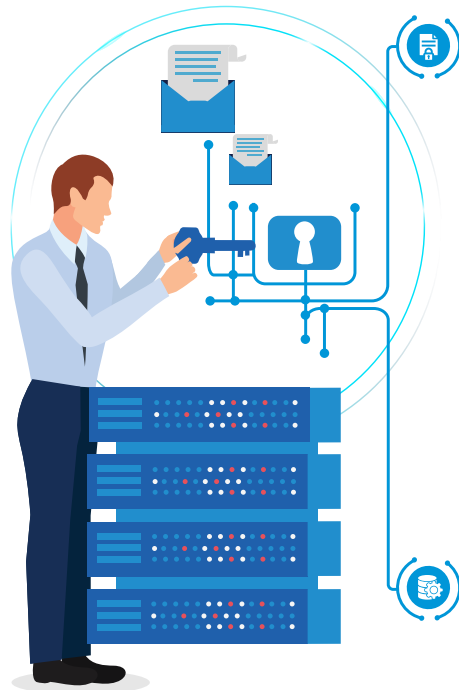
There’s a big trend we’re seeing in the market and that’s the importance of trust. Trust has become a significant factor in how companies compete and differentiate today. Studies show modern organizations, consumers and the employees of today want to buy from, work for, and be associated with brands that are aligned to their own values. The trustworthiness of your brand is now becoming equal to, if not more important, than your products and services.”

Kabir Barday
CEO
OneTrust



remove identifiers from data sets may not be enough. Indeed, guidance from regulators (such as the ICO⁵³) and well-publicized examples of re-identification occurring following release of so-called anonymized data sets point to the need for caution.

So, what can organizations do when there's a need to share large datasets containing personal data, while also preserving privacy? Useful approaches include:



Differential privacy: While not strictly a technology, it seeks to manage privacy risks amid data sharing. The core idea is that when looking at the output of data analysis, there is no way to tell whether an individual's personal data was included within the original dataset. Differential privacy adds a 'statistical noise' layer to the dataset, revealing patterns of groups within the dataset while maintaining privacy. It also articulates privacy as a measure that can be quantified and understood in terms of accumulated risk and sets a 'privacy budget,' beyond which any more queries of that dataset will result in identification of the individual.

Synthetic data: Creating synthetic data involves machine learning to create new datasets containing no personal data while maintaining some similarity (in mathematical and statistical form) to the original dataset containing personal data. The aim is to create a synthetic dataset that can be shared more broadly.

While both methods let organizations manage privacy risks when sharing data, neither solution alone may fully eliminate risk. As a result, organizations employing these techniques should continue to assess the likelihood of personal data leakage.

Next-generation automation using AI and more

AI has a role to play in the future of privacy tech. In fact, it's the foundation on which everything will operate while also providing a barrier to unethical data practices.

AI can be used to enhance privacy-protecting automation. From vendor management, to monitoring cookies and consent, to managing data, AI will operate within a privacy-compliance tool to complete human tasks more quickly and accurately within ethical boundaries. AI can be used to support more-effective data discovery, to classify data, identify risks and suggest appropriate next steps based on the identified context.

When deploying AI, however, organizations need to ensure ethical and safe practices. AI and machine-learning systems operate by analyzing existing datasets, but bias or discrimination may be reinforced or even amplified through their application: for instance, if data fails to accurately represent the broader population from which it draws inferences. Inherent bias among developers can also be reflected in algorithms.



Next-generation privacy portals

As emerging technologies continue to influence lifestyles, consumers will likely expect privacy transparency tools provided by organizations to keep up. Privacy dashboards, or centralized preference management tools, let individuals manage privacy preferences from one central location. Regulators also highlight the benefits of using a dashboard (e.g. the ICO⁵⁴), suggesting that it can be linked at each data-collection touchpoint.

What might consumers expect when looking to understand how their personal data is used and when exercising their data subject rights? Current tools and dashboards might allow individuals to understand the personal data gathered on them and exercise some form of control by updating or deleting information. However, many are static and provide read-only extracts of personal data held rather than a real-time basis on which they can amend and delete personal data on a granular basis.

Looking ahead, should personal data stores and data privacy vaults increase in use, consumer control of personal data may shift from an organization-by-organization approach to being centralized in a consumer-managed vault. A next-generation privacy portal may let consumers understand the exact personal data fields being used by each organization, provide a visual dashboard as their data is shared, and offer enhanced controls over data use.

Privacy Enhancing Technologies (PETs)

PETs can make a difference in the future of privacy technology by minimizing personal data use, maximizing data security and empowering individuals to protect their privacy rights. The promise of PETs is that the underlying personal data can remain protected, while still allowing data analysis. Common examples of PETS include:

Homomorphic encryption: Encryption has long been a go-to solution to secure personal data. However, the risks arise when it's time to access necessary data, as the decrypted data must be stored and processed securely. Enter homomorphic encryption — it bypasses the need to decrypt data, instead allowing for computational operations on encrypted data as if they were performed on plaintext data. Types of homomorphic encryption include Partial (PHE), Somewhat (SHE) and Fully Homomorphic Encryption (FHE) all offering a different scope over the computation that can be performed. However, the maturity of solutions varies with PHE solutions more readily available while FHE is still at the proof of concept phase⁵⁵.

Secure multi-party computation (SMPC): A subfield of cryptography, SMPC seeks to enable joint analysis of data held in multiple encrypted data sources owned by different parties, without each party revealing their own input.

However, PETS are still nascent, with barriers such as costs and complexity in adoption meaning that the landscape of PETs is constantly changing.

Data Access Control

Organizations face increasing challenges amid the proliferation of sensitive data being handled and in turn, the rapidly evolving ethical and legal privacy obligations that must be met. Simply accessing a website can generate personal data such as email addresses or physical location, often gathered and stored without consumer knowledge or consent.

In the last 15 years or so, Role-Based Access Control (RBAC) has been the preferred method to manage access to personal data, replacing individualized user access rights with an approach that manages access based on a user's role within the organization. It is often referred to as static-based access control as it requires administrators to implicitly predetermine the parameters of what access a role should have to fulfill their job function alongside which users are assigned to which role. However, modern data access control requirements are increasingly more complex and difficult to meet using a single attribute such as user role, especially in heavily regulated industries or global organizations.



Building upon this foundation, proposed multi-dimensional and dynamic access control models include privacy protection as a key component. In these Data Access Control models, the notion of purpose is fundamental to how access decisions are made. Data Access Control specifies the intended usage of personal data alongside the purposes for which a given data element is accessed.

Additionally, it can support purpose compliance and explicit prohibitions, allowing administrators to verify that the purpose for accessing personal data complies with the intended purposes of data use and to specify that data should not be used for a given set of incompatible purposes. For example, a receptionist working at a hospital should only be able to see the patient's name and contact details, whereas doctors and nurses are able to access complete patient records. In this example, it may be appropriate that a radiographer should only get access to the record to add completed scans and notes without being able to access specific medical notes about the patient that is out of scope of their role requirement.

All of this can happen in real-time based on the metadata and policy and compliance rule sets which the organization has set, without administrators needing to create separate roles within each system and data store. This dynamic and multi-dimensional approach allows organizations to keep pace more effectively with real-time changes and reduce challenges, compared to role-based access controls.

So, what about data ethics?

The ongoing rapid adoption of increasingly sophisticated technologies to enhance customer experiences and insights requires endless data collection. As a result, there is the increased likelihood of breaches regarding the ethical collection, processing and management of personal data.

Because regulations do not always keep up with technological advances, organizations should embed a data-ethics framework that maintains fair and trustworthy outcomes for all data subjects. A data-ethics framework can help organizations maintain consumer and employee trust by embedding rights into automated decision making, supporting fair decision making that is explainable to the data subject, and ensuring that innovation occurs in a safe and trusted manner.

Ethics will likely play a major role in the future of privacy technology, with ethics principles considering the broad societal implications, combined with appropriate planning for Privacy by Design principles. Not getting this right will make it challenging to implement effective data-management practices while still delivering on the opportunities presented by disruptive technologies.

“Organizations consistently strive to be trusted by their customers and compliant with privacy rules and regulations. Having privacy technology that is agile, nimble, user friendly and effective to meet growing privacy demands is important to support organizations ability to consistently demonstrate compliance in offering trusted, secure and compliant products and services.”

Tom Hyland
Privacy Lead
KPMG in Ireland

[Executive Summary](#)[Change drivers](#)[Connecting technology...](#)[The changing consumer...](#)[The rise of privacy...](#)[What about enterprise...](#)[A plan forward](#)[About KPMG](#)

A plan forward

Key considerations for selecting privacy-tech solutions





[Executive Summary](#)

[Change drivers](#)

[Connecting technology...](#)

[The changing consumer...](#)

[The rise of privacy...](#)

[What about enterprise...](#)

[A plan forward](#)

[About KPMG](#)





Assessing the 'now' and identifying requirements

Before seriously considering any privacy-tech solutions, know the specific needs that a solution must address. Discuss your obligations with privacy, compliance and legal teams to assess how your organization is currently meeting its diverse needs. Explore manual processes that can be automated and be very clear on what a potential solution needs to deliver both today and in the future.

Also, consider the technical specs. Involving your technical staff early in the process can provide a better sense of which specific solutions are viable options. This input can also indicate what other departments and teams would prefer in a privacy-tech solution and will enhance its integration and organization-wide use.

What to look for in a privacy-tech solution

The future of data in organizations will rely on privacy tech and organizations must be careful and diligent when choosing a solution. Marketing by privacy-tech vendors — and in some cases, their oversold promises — will only increase as organizations realize the competitive edge of privacy best practices.

As with any new solution, understand the essential features and technical specifications needed to fully support privacy, security and best-practice requirements. Above all, the solution should be able to grow with your organization amid technological and regulatory changes. Some traits to look for in a solution include ease of use, suite of available products and services, and long-term sustainability.

Ease of use

As more organizations build internal privacy teams, a privacy-tech solution should be easy to build upon existing privacy and compliance processes. The more difficult a solution is to implement and employ daily, the less useful it will be. Focus on compliance, not software implementation.



Privacy technology is everything that empowers individuals to strengthen their personal privacy. Providing those solutions is fundamental for data-driven organization models. Companies need to win back trust and reliability. Showing the added value of data-driven services is my interpretation of the transparency requirement in regulations.

Processing personal data should be reviewed: with a clear focus on a customer-centric journey, including all interfaces and other “sensors” collecting data and the value-add we provide based on that. If personal data is part of your organization model — treat the individual as a long-term organization partner.

It's time to digitalize privacy management and make it more flexible and user focused. This does include customers as well as stakeholders.”

Michael Falk
Privacy Lead
KPMG in Germany



In Japan, market trading and monetization of IoT data from private devices have become a critical concern in various organization communities. We believe that privacy technology would be the key to manage this risk.”

Kenjiro Obora
Privacy Lead
KPMG in Japan



The solution should be sufficiently simple to integrate existing business workflows with the solution's workflows, such as automated API workflows and manual user-assigned tasks. Whatever the solution, a significant amount of architecture, process redesign, configuration and tuning will often be required to deliver on required benefits. This can often be multiples of the costs associated with the purchase of the technology solutions.

Suite of available products and services

Another aspect to consider is the solution's suite of services and products. Determine if a single platform can cover your needs, as that can enable collaboration across teams within a single platform to simplify privacy management. A consistently updated suite of services and products can grow with your organization.

Privacy tech should be highly modular, particularly for smaller organizations, in order to provide the features that matter most. Some privacy regulations have thresholds based on size. By using a modular privacy-tech solution, you can add new modules as needed. Modularity, along with a suite of services that stay up to date with changing regulations, will be invaluable.

Long-term sustainability

Finally, ensure that the privacy-tech solution has signs of long-term sustainability, and accounts for common scenarios like turnover, mergers and acquisitions, company growth, changes to the technology environment, or changes to privacy regulations. This allows your organization to remain ahead of the curve regarding both privacy obligations and meeting the needs of clients and customers.

“Choosing the right software solution for your company is hard. There's a lot riding on the decision, particularly since in many cases, your selection will not only be attributed to you; the usage of the software will be an extension of working with you. Make sure that software represents you well.”

Andrew Clearwater
CPO
OneTrust

“Privacy technology is no longer an after-thought as to what you build and how it integrates into what you're doing. Privacy is becoming a part of businesses' critical infrastructure. Investing in the wrong company or technology stack or choosing not to build privacy into your business and then attempting to fix it later is like trying to put the toothpaste back in the tube.”

Blake Brannon
CTO
OneTrust



About KPMG

At KPMG, our global organization of cyber security professionals offers a multidisciplinary view of risk to help you address your privacy challenges. Our unwavering commitment to precision, quality, and objectivity can help you embed protection and trust into all your activities, not just your technology, to create a security culture.

No matter where you are on your privacy and cyber security journey, KPMG firms have expertise across the continuum — from the boardroom to the data center. In addition to assessing your privacy posture and aligning it to your business priorities, we help you develop advanced solutions, implement them, monitor ongoing risks and help you respond effectively to incidents. Helping you carry privacy compliance throughout your organization, so you can anticipate tomorrow, move faster, and get an edge with secure and trusted technology.

KPMG brings an uncommon combination of deep technical expertise, strong business insights and creative professionals who can help you to manage regulatory obligations and enables you to leverage personal information to create value and increase revenue while meeting the expectations of your customers, employees and vendors.

Together, let's create a trusted digital world, so we can push the limits of what's possible.



OneTrust

OneTrust is the #1 fastest-growing company on Inc. 500 and the category-defining enterprise platform to operationalize trust. More than 9,000 customers, including half of the Fortune 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across privacy, security, data governance, GRC, third-party risk, ethics and compliance, and ESG programs.

The OneTrust platform is backed by 150 patents and powered by the OneTrust Athena™ AI and robotic automation engine. Our offerings include OneTrust Privacy Management Software, OneTrust DataDiscovery™ AI-powered discovery and classification, OneTrust Data Governance™ data intelligence software, OneTrust Vendorpedia™ third-party risk exchange, OneTrust GRC integrated risk management, OneTrust Ethics ethics and compliance software, OneTrust PreferenceChoice™ consent and preference management, OneTrust ESG environmental, social and governance software, and OneTrust DataGuidance™ regulatory research.

According to the IDC Worldwide Data Privacy Management Software Market Shares Report, 2020, "OneTrust is leading the market outright and showing no signs of slowing down or stopping."

OneTrust has raised a total of USD920 million in funding at a USD5.3 billion valuation from Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, and Franklin Templeton.

OneTrust's fast-growing team of 2,000 employees is co-headquartered in Atlanta and London with additional offices in Bangalore, Melbourne, Denver, Seattle, San Francisco, New York, São Paulo, Munich, Paris, Hong Kong, and Bangkok.

To learn more, visit OneTrust.com or connect on [LinkedIn](#), [Twitter](#), and [YouTube](#).

[Executive Summary](#)[Change drivers](#)[Connecting technology...](#)[The changing consumer...](#)[The rise of privacy...](#)[What about enterprise...](#)[A plan forward](#)[About KPMG](#)

Our contacts

Sylvia Klasovec Kingsmill
Global Cyber Privacy Leader
KPMG International and Partner
KPMG in Canada
E: skingsmill@kpmg.ca

Kabir Barday
Chief Executive Officer,
OneTrust
E: kbarday@onetrust.com

Andrew Clearwater
Chief Privacy Officer,
OneTrust
E: aclearwater@onetrust.com

Blake Brannon
Chief Strategy Officer,
OneTrust
E: bbrannon@onetrust.com

Walter Risi
KPMG in Argentina
E: wrisi@kpmg.com.ar

Matthew Quick
KPMG Australia
E: mquick@kpmg.com.au

Andreas Tomek
KPMG in Austria
E: atomek@kpmg.at

Benny Bogaerts
KPMG in Belgium
E: bbogaerts@kpmg.com

Leandro Augusto M Antonio
KPMG in Brazil
E: lantonio@kpmg.com.br

Sylvia Kingsmill
KPMG in Canada
E: skingsmill@kpmg.ca

Tamara Agnic
KPMG in Chile
E: tagnic@kpmg.com

Henry Shek
KPMG China
E: henry.shek@kpmg.com

Pavel Kliment
KPMG in the Czech Republic
E: pkliment@kpmg.cz

Teet Raidma
KPMG in Estonia
E: traidma@kpmg.com

Juha Karilo
KPMG in Finland
E: juha.karilo@kpmg.fi

Vincent Maret
KPMG in France
E: vmaret@kpmg.fr

Jaba Gvelebiani
KPMG in Georgia
E: jgvelebiani@kpmg.com

Michael Falk
KPMG in Germany
E: mfalk@kpmg.com

Efthymia Katsouli
KPMG in Greece
E: ekatsouli@kpmg.gr

László Hargitai
KPMG in Hungary
E: laszlohargitai@kpmg.com

Mayuran Palanisamy
KPMG in India
E: mpalanisamy@kpmg.com

Freddie Mulyadi
KPMG in Indonesia
E: freddie.mulyadi@kpmg.co.id

Tom Hyland
KPMG in Ireland
E: tom.hyland@kpmg.ie

Bryan Beesley
KPMG Isle of Man,
Guernsey, Jersey
E: bbeesley@kpmg.co.im

Jonathan Brera
KPMG in Italy
E: jbrera@kpmg.it

Kenjiro Obora
KPMG in Japan
E: kenjiro.obora@jp.kpmg.com

Min Soo Kim
KPMG in Korea
E: mkim9@kr.kpmg.com

Sanita Petersone
KPMG in Latvia
E: spetersone@kpmglaw.lv

Estefania Rizzo
KPMG in Luxembourg
E: estefania.rizzo@kpmg.lu

Albert Lim
KPMG in Malaysia
E: hockenglim@kpmg.com.my

Rommel Garcia
KPMG in Mexico
E: rommelgarcia@kpmg.com.mx

Ronald Koorn
KPMG in the Netherlands
E: koorn.ronald@kpmg.nl

Souella Cumming
KPMG in New Zealand
E: smcumming@kpmg.co.nz

John Anyanwu
KPMG in Nigeria
E: john.anyanwu@ng.kpmg.com

Arne Helme
KPMG in Norway
E: arne.helme@kpmg.no

Glenn Tjon
KPMG in Panama
E: gtjon@kpmg.com

Jallain Manrique
KPMG in the Philippines
E: jsmanrique@kpmg.com

Krzysztof Radziwon
KPMG in Poland
E: kradziwon@kpmg.pl

Tiago Reis
KPMG in Portugal
E: treis@kpmg.com

Mihai Gabriel Tanase
KPMG in Romania
E: mtanase@kpmg.com

Ilya Shalenkov
KPMG in Russia
E: ishalenkov@kpmg.ru

Daryl Pereira
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Finn Elliot
KPMG in South Africa
E: finn.elliott@kpmg.co.za

Javier Aznar Garcia
KPMG in Spain
E: jaznar@kpmg.es

Anders Sederholm
KPMG in Sweden
E: anders.sederholm@kpmg.se

Thomas Bolliger
KPMG in Switzerland
E: tbolliger@kpmg.com

Jason Y.T. Hsieh
KPMG in Taiwan
E: jasonhsieh@kpmg.com.tw

Chris Saunders
KPMG in Thailand
E: csaunders2@kpmg.co.th

Maliha Rashid
KPMG in the UAE
E: mrashid5@kpmg.com

Julia Spain
KPMG in the UK
E: julia.spain@kpmg.co.uk

Rodrigo Ribeiro
KPMG in Uruguay
E: rribeiro@kpmg.com

Orson Lucas
KPMG in the USA
E: olucas@kpmg.com

Will Nguyen
KPMG in Vietnam and
Cambodia
E: williamnguyen@kpmg.com.vn



[Executive Summary](#)

[Change drivers](#)

[Connecting technology...](#)

[The changing consumer...](#)

[The rise of privacy...](#)

[What about enterprise...](#)

[A plan forward](#)

[About KPMG](#)





References

- ¹ KPMG's Me my life my wallet, 2021.
- ² KPMG's The New Imperative for Corporate Data Responsibility, 2020.
- ³ OneTrust Data Guidance, 2021, <https://platform.dataguidance.com/>
- ⁴ Justices of the Peace Act, 1361 (Eng.), 34 Edw. 3, c. 1.
- ⁵ Second Congress. Sess. 1, Chapter 7, 1792.
- ⁶ Félix v. O'Connell, Trib. Civ de la Seine, 16 juin 1858.
- ⁷ Mia Fineman, "Kodak and the Rise of Amateur Photography," metmuseum.org, October 2004.
- ⁸ The Right to Privacy, Samuel D. Warren; Louis D. Brandeis, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.
- ⁹ K.M Turner & W.F.H. Germer, Telephone Dictating Machine or Apparatus, Patent No. 843,186, Patented Feb, 5, 1907.
- ¹⁰ Olmstead v. United States, 277 U.S. 438, 1928.
- ¹¹ United Nations Declaration of Human Rights (UDHR), Article 12, 1948.
- ¹² "Netscape 1.0 Released," thisdayintechhistory.com, 2015.
- ¹³ The History of the General Data Protection Regulation, European Data Protection Supervisor.
- ¹⁴ SixDegrees.com, wikipedia.org, 2021.
- ¹⁵ Polly Sprenger, "Sun on Privacy: 'Get Over It'," Wired.com, January 26, 1999.
- ¹⁶ 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council, August 25, 2000.
- ¹⁷ Adam Pothitos, "The History of the Smartphone," Mobile Industry Review, October 31, 2016.
- ¹⁸ The App Store turns 10, Apple Newsroom, July 5, 2018.
- ¹⁹ Sarah Perez, "The 3 Facebook Settings Every User Should Check Now," The New York Times, January 20, 2010.
- ²⁰ Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder," The Gaurdian, January 11, 2010.
- ²¹ Charles Arthur, "iPhone keeps record of everywhere you go," The Guardian, April 20, 2011.
- ²² Emil Protalinski, "70% don't trust Facebook with their personal information," ZDNet.com, May 9, 2012.
- ²³ "Girls Around Me app 'like looking in the window': developer," securitybrief.co.nz, April 2, 2012.
- ²⁴ Steve Lohr, "The Age of Big Data," The New York Times, Feb. 11, 2012.
- ²⁵ Becky Branford, "Snowden affair puts Wikileaks back into spotlight," BBC News, June 28, 2013.
- ²⁶ Joe Svetlik, "2014: Wearable tech review of the year," Wearable.com, December 22, 2014.
- ²⁷ James Connington, "It's time to make sure research is understandable to all," The Telegraph, July 27, 2015.
- ²⁸ Samuel Gibbs, "What is 'safe harbour' and why did the EUCJ just declare it invalid?" The Guardian, October 6, 2015.



²⁹ “Internet of Things Will Deliver \$1.9 Trillion Boost To Supply Chain And Logistics Operations,” Cisco Newsroom, April 15, 2015.

³⁰ Natasha Singer, “When Websites Won’t Take No for an Answer,” The New York Times, May 14, 2016.

³¹ “Data protection in the EU,” ec.europa.eu, 2021.

³² GDPR Enforcement Tracker, enforcementtracker.com, 2021.

³³ “Provvedimento correttivo e sanzionatorio nei confronti di Eni Gas e luce S.p.A.,” gdpd.it, December 11, 2019.

³⁴ Court of Justice of the European Union, Press Release No 91/20, July 16, 2020.

³⁵ “Confidentiality of electronic communications: Council agrees its position on ePrivacy rules,” Press release: European Council of the European Union, February 10, 2021.

³⁶ Sarah Rippy, “Virginia passes the Consumer Data Protection Act,” iapp.org, 2021.

³⁷ LfD Niedersachsen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de, lfd.niedersachsen.de, January 8, 2021.

³⁸ “Resolución De Procedimiento Sancionador,” Procedimiento N°: PS/00477/2019, www.aepd.es.

³⁹ KPMG’s Six Pillars, <https://home.kpmg/xx/en/home/insights/2020/01/six-pillars.html>.

⁴⁰ Knud Lasse Lueth, “State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time,” iot-analytics.com, November 19, 2020.

⁴¹ KPMG’s COVID-19 and the future of digital assistants, kpmg.us, 2020.

⁴² Charity: Water, The Source, 2015, <https://www.with.in/watch/the-source/>

⁴³ J. Volpe, “The 21st-century charity that puts Google and VR to good use,” engadget.com, March 3, 2016.

⁴⁴ Queenie Wong, “Why WhatsApp users are pushing family members to Signal,” cnet.com, Feb. 5, 2021.

⁴⁵ KPMG’s Me my life my wallet, 2021.

⁴⁶ Press release : Medtronic and Fitbit Partner to Integrate Health and Activity Data Into New CGM Solution for Simplified Type 2 Diabetes Management, Medtronic Newsroom, December 7, 2016.

⁴⁷ Jessica Davis, “Consumer Adoption of Health Tech Slowed by Privacy, Security Concerns,” healthitsecurity.com, January 7, 2020.

⁴⁸ Jack Hardinges, “Data trusts in 2020,” theodi.org, March 17, 2020.

⁴⁹ Data Trust, ictr.johnshopkins.edu, 2021.

⁵⁰ A European strategy for data, ec.europa.eu, February 2020.

⁵¹ WG closed, github.com, January 2019.

⁵² GPC Privacy Browser Signal Now Used by Millions and Honored By Major Publishers, Global Privacy Control, January 28, 2021.

⁵³ What is personal data? ico.org.uk, 2021.

⁵⁴ How can dashboards help? ico.org.uk, 2021.

⁵⁵ Protecting privacy in practice, The Royal Society, 2019.

Acknowledgments

Our sincere thanks to those who contributed their time and insights in the planning, analysis, writing and production of the report itself. With a special thank you to Saz Kanthasamy (KPMG), Tess Macapinlac (OneTrust) and Kadi Coult Wharton (OneTrust), who generously contributed their support, knowledge and insights.

home.kpmg/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Designed by Evalueserve.

Publication name: Privacy Technology: What's next?

Publication number: 137417-G | Publication date: May 2021