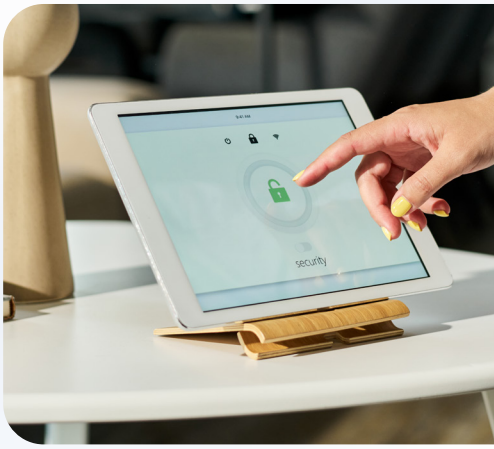
syrenis

GUIDE



The Future of Data Privacy: 2026 and Beyond

syrenis.com

> **“See things in the present, even if they are in the future.”**
>
> Larry Ellison, co-founder & Executive Chairman of Oracle

Introduction

The rate at which the world is evolving is unprecedented across pretty much every field. For centuries, arguably since the dawn of time, we’ve tried to predict the future. Both from a sense of practicality – it’s logical to try and be prepared for what’s next – but also, it’s exciting to wonder what might happen next.

Realistically, the future is often very unpredictable, in part because of how quickly things can change. We’re not living on Mars (yet), nor do we travel around in flying cars.

But on a smaller scale, particularly over the last decade or so, we’ve seen technology in particular make rapid advances that impact how we live our lives.

The field of privacy develops alongside technology; arguably the two are intrinsically linked.

Though there is no privacy magic 8-ball to give us insight into a guaranteed privacy future, it can be useful to consider what might lie ahead in the next 3-5 years on which to base strategy and infrastructure planning that aligns with tomorrow’s reality.

One way to categorize and understand the future of data privacy is to consider three crucial elements: **people**, **compliance** and **technology**.

These three components impact one another as well as drive each other forward.

After all, human attitudes motivate changes in regulations and technological developments. Innovative technologies impact human factors and regulations, and regulations impact human expectations and technological developments.

For instance, the rise of privacy-conscious consumers has led to stricter data protection laws like the GDPR and CCPA. These laws compel organizations to adopt advanced privacy-preserving technologies, such as encryption and anonymization. As these technologies become more sophisticated, they further shape public expectations and regulatory standards.

What Does The Future of Data Privacy Look Like?

People

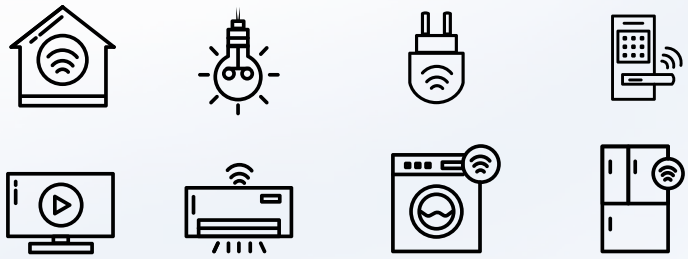
People and Devices
As technologies – and the long-prophesized Internet of Things (IoT) – advance, privacy increasingly becomes not just a matter of a personal identifier plus one or more data points about that person. It also becomes a combination of devices plus information about how humans (sometimes multiple humans, or households) use them.

The list of devices also expands. Mobile phones are not the only privacy-sensitive devices. Wearables, such as smart watches, present new privacy challenges now and in the future. Moreover, even smart connected home devices like light bulbs become part of the privacy picture.

Connected vehicles move into the list, as do medical devices and disability tools. In short, it is not hard to contemplate a future in which almost everything is a smart device, and there are privacy implications related to our interactions with them all. Additionally, given that people can share some devices like vehicles and household items, the notion of 1-1 notice and consent becomes increasingly complicated to implement.

Smart homes in the U.S. have an average of

8 smart devices



www.explodingtopics.com/blog/smart-home-stats

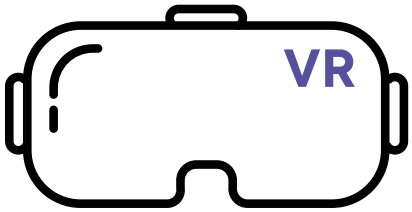
Picture this. Your smart fridge actively monitors what food is consumed on a weekly basis, under the remit of helping plan your weekly groceries shop. It collects data (from your entire household) on the types of food you're eating the most, which can easily be then used to send you personalized recommendations.

But how about when it starts to track how much wine you're drinking? When does it cross the line over helpful to encroaching? The data is then sold on to a third-party due to a vague privacy policy, ending up in the hands of your medical insurance... Without control, transparency and consent in place, vast amounts of personal data are at risk.

Digital Lives and Virtual Reality

Our online interactions are increasingly personal, complex, and satisfying. Online capabilities and platforms have transformed the way we play games, date, stay in touch, and advise one another.

Since the person behind the online profile can be anonymous, pseudonymous, or fictitious, an increasing gap appears between the human being behind the online curtain and the persona that the human being presents online. At some point, privacy may need to consider whether digital, virtual lives have the same value and privacy risks as our physical lives.



The number of VR users is expected to reach **300.8m** by **2029**

People are also beginning to express different privacy preferences depending on the persona they have adopted within a particular context. For example, an individual may have privacy sensitivity on a professional social media platform more intricately linked to their 'real' personal identity, but they may have a different set of privacy expectations for personas they create on gaming sites or other social media platforms in other contexts.

In the future, privacy may even have to consider whether a person is a physical, single human being, or whether a person instead can be a loosely connected set of personas, each with different privacy perspectives.

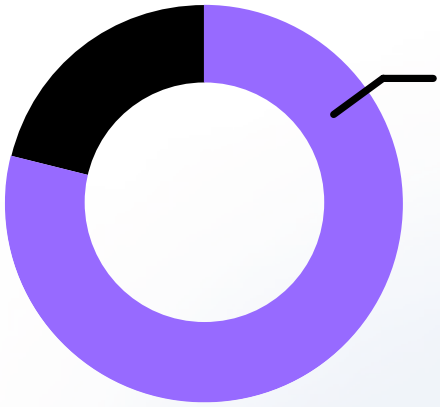
Compliance

Global Privacy Standards

Increasingly, privacy laws around the world are moving closer and closer to one another. Each subsequent privacy law picks up components of the privacy laws that came before. As a result, it is not hard to imagine a world where most privacy laws eventually resemble each other to such an extent that a global privacy law, or at least a global privacy standard, is a possibility.

We have seen this phenomenon as the GDPR influenced subsequent laws, such as the LGPD in Brazil. In the United States, California's privacy law influenced subsequent state laws, each of which pick up components of preceding ones. Provincial Canadian privacy laws are also similar, even down to the name of the law.

There are non-trivial obstacles to implementing a global privacy law, such as enforcement, but a global privacy standard could be a near-term reality if these trends continue. Though today's privacy office may handle privacy on a jurisdiction basis, tomorrow's privacy office may be able to set minimum standards globally without losing any significant flexibility or competitive advantage with personal data.



79.3%

of the world's population is covered by some form of national data privacy law

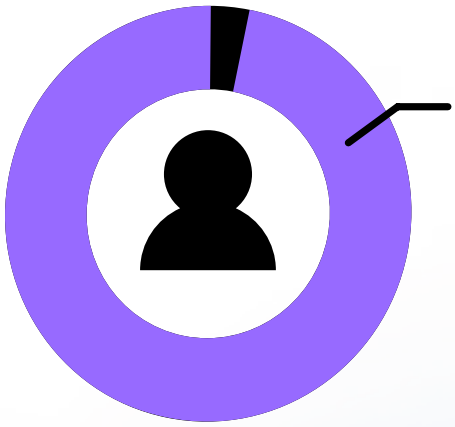
https://www.iapp.org/news/a/identifying-global-privacy-laws-relevant-dpas

Reglatory Enforcement

There is no need for a palm reading to predict that enforcement will only increase in the short term. A combination of new laws, which bring new enforcement opportunities, and increased regulatory attention to privacy enforcement of legacy laws, means that privacy regulatory risks continue to rise.

Plus, regulators are thinking about how to use AI and other technologies to help make enforcement more efficient, so that the data protection authority of the future may be able to investigate and act against many, many more organizations while not increasing staff.

Whilst it might seem like only large companies are being fined at the moment, this is likely to change as enforcement ramps up. Consider the likes of Meta and TikTok enforcement actions as cautionary tales of what not to do. But the reality is, particularly for any enterprise-scale organization, the eyes of the regulators will be on you to set an example.



97%

of US consumers believe there should be **stricter penalties for companies** that violate data privacy regulations

Technologies

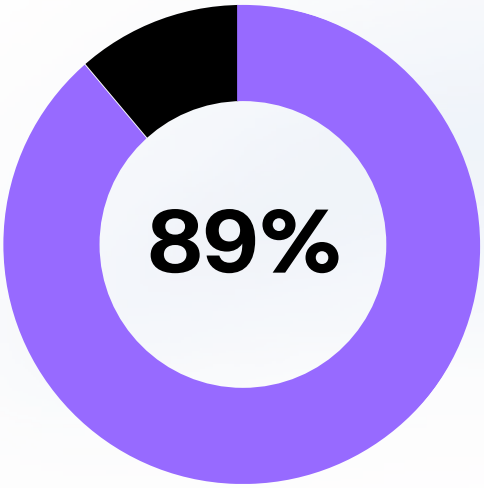
Artificial Intelligence

We can't talk about the future (or pretty much any topic these days) without mentioning Artificial Intelligence (AI). The reason for that is easy to see. Though AI has been around for a while, recent advancements in technology have pushed AI into a new era of possibilities. One of the likely future outcomes resulting from AI is the democratization of data and knowledge.

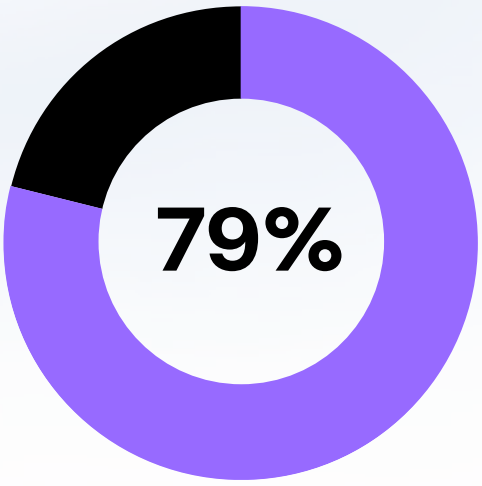
In the 1980s, to answer a question about how to construct a bridge, the individual would need to find a book or a subject matter expert to explain the process. In the 2000s, the individual just turns to his or her phone for the answer. Progressively, in the 2020s, AI makes natural language requests possible for the average Joe or Jane wanting to find an answer or generate something new based on existing information.

There is no doubt that the privacy professional of the future – and even today – must understand and plan to address privacy challenges of AI, including but not limited to deep fakes, bias, automated decisions, legal basis, consent, and notice.

On the other side, AI is already an asset to complex privacy management activities, including but not limited to third party management, individual rights, data inventories, data protection impact assessments, and consent and preference management.



of US consumers agree that **AI isn't bad**, it just needs more regulations



of US consumers say they would be more likely to **opt-in to data sharing** if this was the case

Privacy Enabling Technologies

There is plenty of good news in the privacy future, and one part of that good news is the ongoing development of Privacy Enabling Technologies, or PETs.

According to the **US Federal Trade Commission**, PETs, "such as end-to-end encryption, are a broad set of tools and methods aimed at providing ways to build products and functionality while protecting the privacy of users' data." It's likely that privacy regulations will mandate the continued adoption and enhancement of PETs.

The PETs of today can help organizations fulfil obligations or conduct business activities such as analytics that would ordinarily require access to personal data without gaining actual, free access They also serve to help protect and control personal data.

Tomorrow's PETs may allow organizations to conduct business while eliminating the need to access personal data altogether.

Voice Controls and Natural Language Processing

As technology continues to improve its ability to recognize and process voice and natural language, privacy may become both easier and more complicated to manage.

These abilities can help to democratize data, allowing non-programmers to more easily access information, control applications, and take advantage of the power of computers.

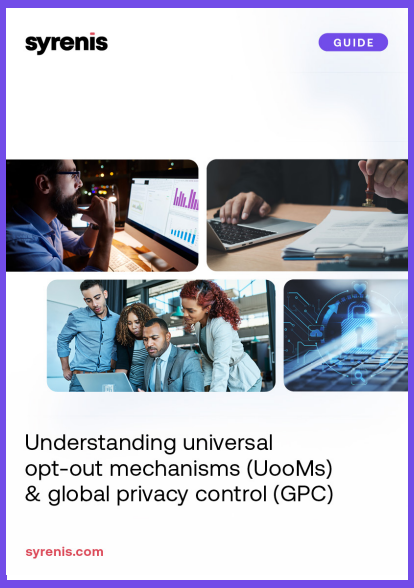
More data users and more data can make managing privacy even more complicated. On the other hand, these technologies also may help individuals exert more, easier control over their own data.

Who knows – the privacy novice and individual rights process of the future may rely less on text and more on real-time voice information and commands. Natural language processing may also help individuals ask for and receive information about how an organization collects and uses information without the human involvement of the privacy office.

Universal Privacy Signals

Already a reality in the online world related to cookies and other online trackers, the idea here is that an individual can set preferences, such as rejecting third party advertising cookies, once in a browser and then the browser passes on instructions to every web domain it visits.

More privacy laws require some sort of acceptance of these types of signals. For example, in the United States, Colorado and Connecticut privacy laws require that relevant companies recognize and act on Global Privacy Control (GPC) signals, one example of a universal privacy signal to opt out of some third-party cookies.



Understanding Universal Opt-out Mechanisms (UooMs) & Global Privacy Control (GPC)

DOWNLOAD NOW

There are also similar rumblings from Google that they may implement a browser-level consent option into Chrome, however they face stiff resistance on the grounds of monopolization and controlling too much data.

In the future, it is conceivable that technology could enable a define-once, implement-everywhere approach to consent and preferences. That is, a consumer could set preferences and give general consents in a single location, and organizations would implement those preferences (online and offline) without interacting directly with that individual.

Bioengineering

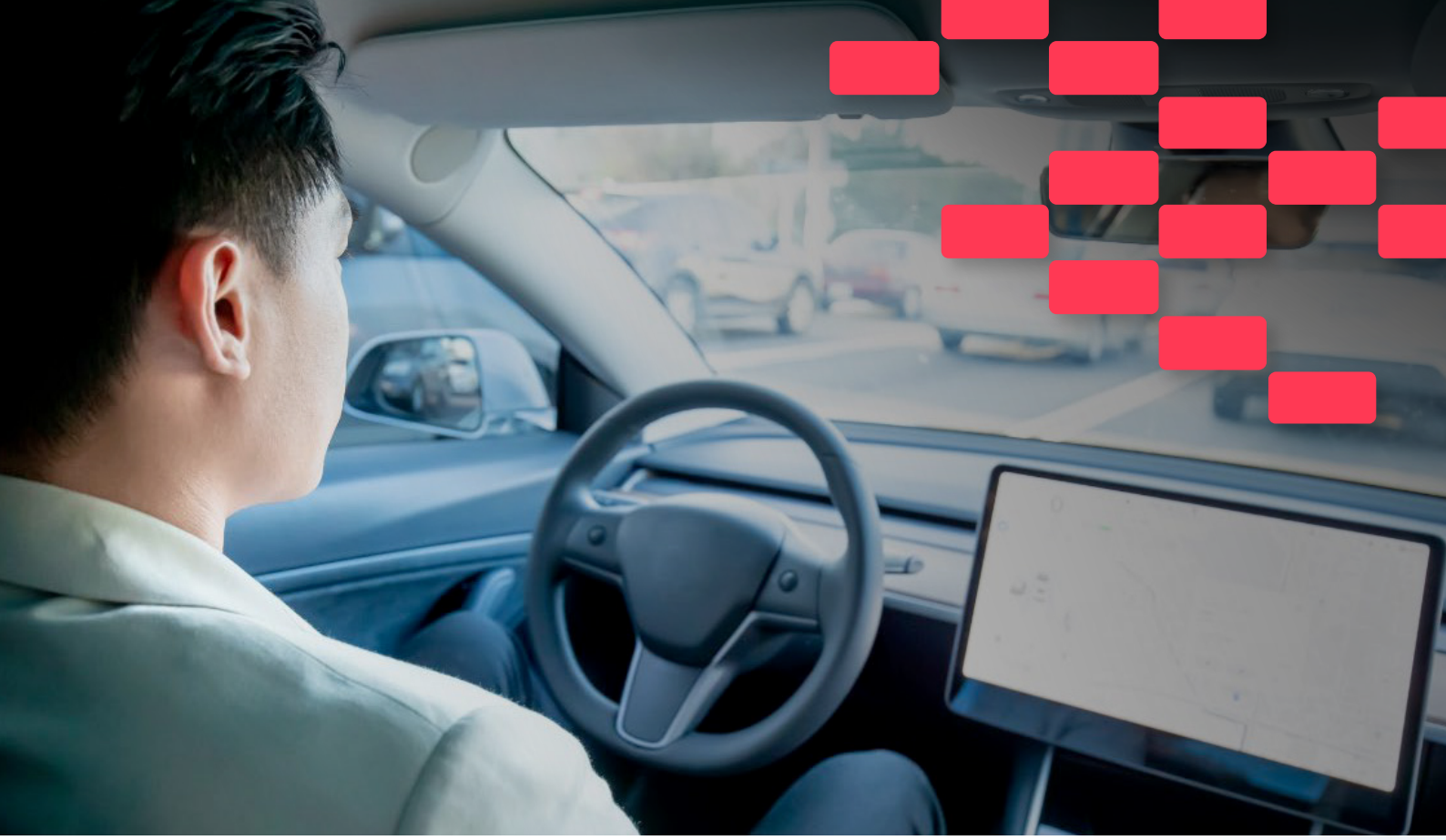
Genetic research, when applied to humans, has both enormous potential benefit and risk, simultaneously.

On the potential benefit side, genetic studies are looking for, and finding, solutions to such serious problems as cancer, alcoholism, heart disease, Alzheimer's, and many other health problems that have a genetic component.

On the other hand, the same genetic information that can drive critical cures also has the potential to harm research subjects. For example, in the wrong hands, such as insurance companies and employers, it can lead to genetic discrimination.

However, the stronger the privacy protections for these sensitive data points, the more restrictive may be the data flows, which in turn interrupts scientific progress and public good.

As a result, as bioengineering continues to flourish and data sharing needs continue to increase, privacy concerns in bioengineering will also continue to evolve. PETs may help solve some of the privacy concerns while enabling the required data sharing, but privacy professionals will need to participate in this long-term, high impact activity for years to come.



ACES Vehicles

Standing for Autonomous, Connected, Electric, and Shared, ACES is the vehicle wave of the future. Self-driving cars are already on our highways and are expected to save lives through reduction in accidents.

Most newer vehicles already are 'connected' – meaning that they can send and receive data, which allows them to provide services like crash-triggered 911 calls, wireless hotspot, online mapping, radio station location, predicting/preventing safety issues, and many others.

Many auto manufacturers have an aggressive – and some even sole – electrification strategy. Shared vehicles may allow people to stay mobile while reducing the number of vehicles needed overall, given that most vehicles sit unused most of the time.

Together, these futuristic-sounding developments in the automotive industry are all driven by data, and in many cases, by personal data. Autonomous driving is possible, in part, through cameras – which can present privacy challenges. Connected vehicles send and receive thousands of data points to make services possible, including geolocation and driving information.

To work seamlessly, the electrification network of vehicles and charging stations also demand personal data, including location and payment information. Vehicle sharing also requires communication between and about other individuals.

These are just a few of the privacy challenges facing the auto industry today and, in the years, to come, keeping privacy interesting as the public need for advances in safety, environmental protection, and convenience have the potential to create friction with consumer privacy expectations.

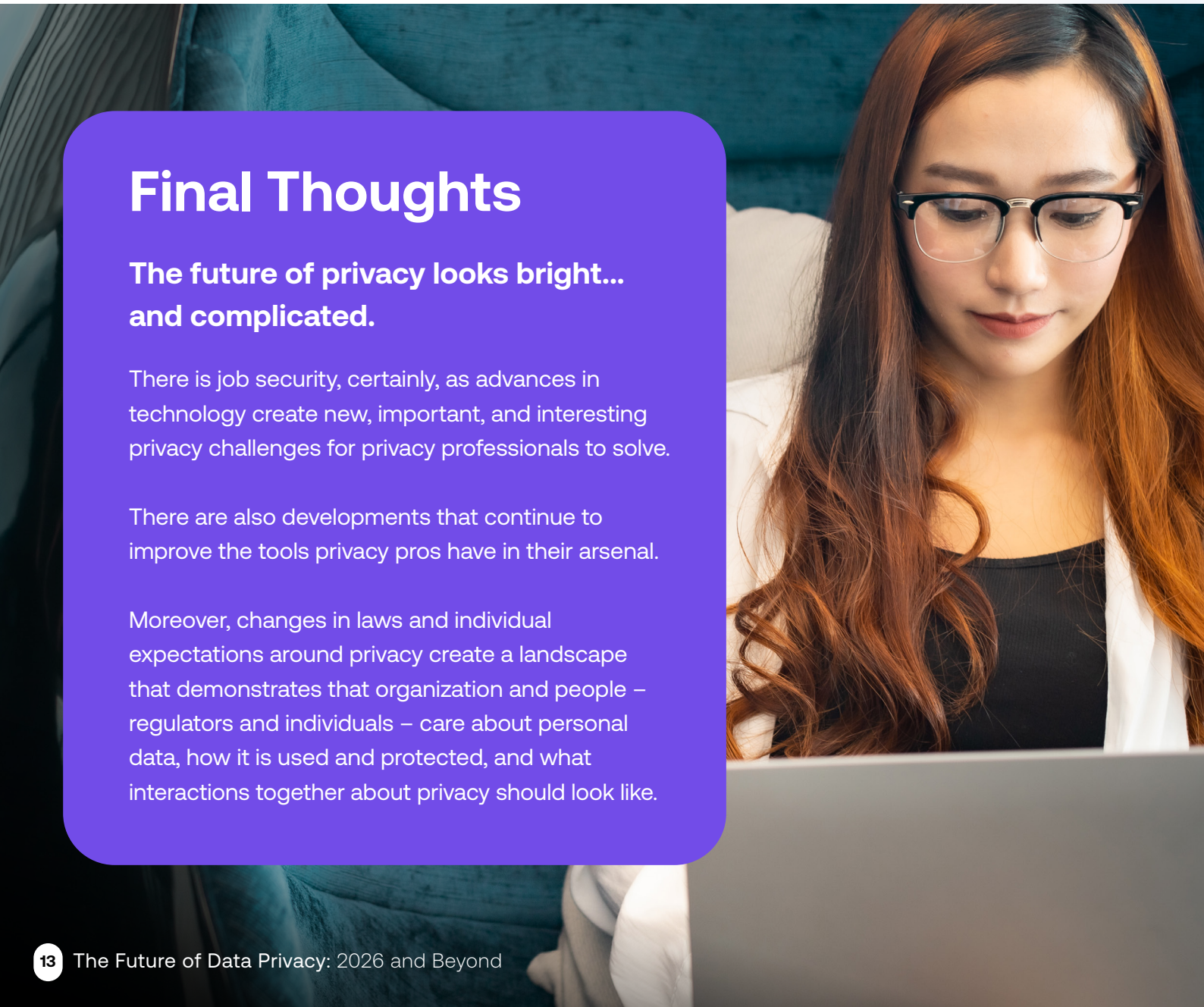
Quantum Computing

Though there are several different definitions of quantum computing, all underscore a few key points – a new approach to computing, based on physics principles, that allows for fast analysis of complex problems.

Quantum computing can process vast amounts of data at unprecedented speeds, enabling more efficient data management and analysis. This can improve the accuracy and effectiveness of PETs and consent management systems.

One of the most significant challenges is that quantum computers could potentially break current encryption methods, such as RSA and ECC, which are widely used to protect data. This poses a serious threat to data privacy. Regulations – which tend to move slowly – will need to play catch up to ensure there is substantial safeguarding in place.

Regardless of the exact definition, any time a large amount of data is involved, privacy and security are critical controls to consider. Also, ironically, quantum computing in the wrong hands can mean that quantum algorithms can break down security protections, leading to breaches.



Final Thoughts

The future of privacy looks bright... and complicated.

There is job security, certainly, as advances in technology create new, important, and interesting privacy challenges for privacy professionals to solve.

There are also developments that continue to improve the tools privacy pros have in their arsenal.

Moreover, changes in laws and individual expectations around privacy create a landscape that demonstrates that organization and people – regulators and individuals – care about personal data, how it is used and protected, and what interactions together about privacy should look like.

syrenis

Contact us
hello@syrenis.com

US Office
Suite 700 3379 Peachtree Road NE
Atlanta, Georgia 30326, United States
+1 844 585 6264

UK Office
V2, Sci-Tech Daresbury, Warrington,
WA4 4AB United Kingdom.
+44 (0) 20 4551 9501