THE PRIVACY ADVANTAGE

TURNING DATA PROTECTION INTO DIGITAL INNOVATION

MATT KAIN

Forget everything you thought you knew about data privacy – it's not a roadblock, it's your secret weapon for innovation. Discover how forward-thinking companies are leveraging privacy-first approaches to outpace competitors, build unshakeable customer trust, and unlock billion-dollar opportunities in the digital age.

www.mattkain.com

Table of Contents

Introduction: The Shifting Paradigm

For years, we've been caught in a false dichotomy. Privacy versus personalisation. Data protection versus innovation. But what if this supposed trade-off is actually holding us back? What if privacy, far from being a barrier, is the key to unlocking the next wave of digital innovation?

This article argues that privacy is not a barrier to innovation but a catalyst for it, driving the next wave of digital transformation across industries. By adopting privacy-first approaches, organisations can build trust, create new value, and gain a competitive advantage in the data-driven economy.

It's time to flip the script. Privacy isn't just about protection—it's about potential. Far from being a roadblock, it's a foundation. On this foundation, we can build digital experiences that are more trustworthy, more valuable, and ultimately more innovative.

This shift in thinking goes far beyond just personalised marketing. It has implications for how businesses strategise, how governments serve citizens, and even how nations develop in the digital age.

From corporate boardrooms to public sector initiatives, from bustling metropolises to rural villages, the way we handle data and privacy is reshaping our world. From developed economies to emerging markets, the way we handle data and privacy is reshaping our world, presenting both opportunities for progress and challenges for individual rights.

(SEE ECONOMIC IMPLICATIONS ABOVE RIGHT)

All of this suggests that investing in privacy isn't just about compliance—it's a sound business strategy that can drive growth and innovation.

Economic Implications

Breach Costs
5% lower

Profits
11% higher

Market Value
3% higher

A 2018 study by the Centre for Information Policy Leadership found that companies with mature privacy practices experience 5% lower breach costs, 11% higher annual profits, and 3% higher market valuations [1].

A 2022 Cisco Data Privacy Benchmark Study found that 60% of organisations reported getting significant business value from their privacy investments, with the average company seeing a 1.8x return on their privacy spending [2].

Business Value
1.8x ROI

Reported to Board
93%

Privacy Technology
$30-50BN

Privacy-enhancing technologies are projected to create a $30-50 billion market by 2025, according to Gartner.

As we stand on the cusp of this privacy revolution, the question for organisations isn't whether to participate, but how to lead. Those who view privacy merely as a compliance issue will find themselves playing catch-up.

But those who embrace privacy as a core value and innovation driver? They're the ones who will thrive in this new era.

In this article, we'll explore how leading organisations are turning privacy into a competitive advantage. We'll delve into the technologies making this possible, examine case studies from around the globe, and provide a roadmap for organisations looking to lead in this privacy-first future.

The privacy revolution is here.
Are you ready to lead the charge?

The Current Landscape: Beyond Personalisation

When we talk about data and privacy, personalised marketing often dominates the conversation. But the implications of how we handle data stretch far beyond tailored ads or product recommendations. Let's broaden our perspective.
In the corporate world, data isn't just a marketing tool—it's the lifeblood of strategic decision-making. Companies are using big data analytics to optimise supply chains, predict market trends, and even shape their long-term strategies. The challenge? Doing so while respecting privacy and maintaining consumer trust.

Unilever

Unilever provides a compelling example of a company committed to ethical data practices. The consumer goods giant has established Responsible Data and AI Principles, which emphasise transparency, fairness, and privacy protection.

Unilever reports that this approach has allowed them to enhance personalisation while respecting consumer privacy. For instance, their 'Digital Voice of the Consumer' initiative, which analyses anonymised online conversations, has helped them gain insights that inform product development and marketing strategies without compromising individual privacy [3].

While Unilever doesn't disclose specific metrics linking their privacy practices directly to campaign performance, they have reported overall improvements in marketing effectiveness. In their 2022 Annual Report, Unilever noted that their data-driven marketing approach contributed to a 12% year-on-year increase in ROI for their overall marketing investment [3].

Public Sector

In the public sector, the stakes are even higher. Governments worldwide are grappling with how to use data to improve services while protecting citizens' privacy. The Estonian government, for instance, has become a global leader in e-governance. Their X-Road system allows for secure, privacy-preserving data exchange between government agencies, improving service delivery without compromising citizen privacy [4].

But perhaps the most profound impact of data and privacy considerations is on global development. The United Nations has recognised digital identity systems as key to achieving several Sustainable Development Goals. Yet, these systems must be designed with privacy at their core to prevent misuse and protect vulnerable populations.

The landscape is also being shaped by evolving regulations. The EU's General Data Protection Regulation (GDPR) has set a new global standard for data protection, influencing laws worldwide. In the U.S., the California Consumer Privacy Act (CCPA) is pushing companies to rethink their data practices. And in China, the Personal Information Protection Law (PIPL) is reshaping how companies operate in the world's largest consumer market [4].

Australia Privacy Act

Australia is in the process of modernising its privacy framework through proposed amendments to the Privacy Act 1988. The Australian Government has initiated a comprehensive review of the Privacy Act, which has resulted in 116 recommendations for reform. Of these, 38 have been accepted in full by the government [6].

While draft legislation is anticipated to be tabled by August 2024, it's important to note that these reforms are still under consultation and may evolve before being finalised. The government is engaging with stakeholders and the public to refine these proposals, ensuring they strike the right balance between enhancing privacy protections and supporting innovation [7].

Key proposed changes, subject to further consultation and potential modification, include:

- Alignment with GDPR principles
- Enhanced individual rights, including a limited right to erasure
- Stricter privacy policies and consent requirements
- Shortened data breach reporting timeframe (from 30 days to 72 hours)
- Expanded regulatory powers for the Office of the Australian Information Commissioner (OAIC) [8]

These reforms aim to update Australia's privacy framework to address the challenges of the digital age, but the final form of the legislation may differ from current proposals as the consultation process continues.

Catalyst for Innovation

Amidst this complex landscape, one thing is clear: organisations that view privacy as a catalyst for innovation are pulling ahead. They're not just complying with regulations—they're using privacy-enhancing technologies to unlock new possibilities.

For instance, data clean rooms are enabling unprecedented collaboration between companies without compromising data privacy. Retailers and CPG brands are using these secure environments to match purchase data with advertising impressions, deriving insights that were previously impossible due to data silos [4]. Meanwhile, techniques like federated learning are revolutionising how we train AI models. Google has used this approach to improve features like next-word prediction on Android keyboards, learning from user behaviour without ever accessing individual user data [4].

As we move forward, the organisations that will thrive are those that see privacy not as a constraint, but as a design principle. They're the ones asking: How can we create value while respecting privacy? How can we use data not just more efficiently, but more ethically?

The economic implications of privacy-first approaches are significant. A study by the Centre for Information Policy Leadership found that companies with mature privacy practices experience 5% lower breach costs, 11% higher annual profits, and 3% higher market valuations [1]. Moreover, privacy-enhancing technologies are projected to create a $30-50 billion market by 2025, according to Gartner [9]. This suggests that investing in privacy isn't just about compliance—it's a sound business strategy that can drive growth and innovation.

The Technology Enabling Privacy-First Innovation

The shift towards privacy-first innovation isn't just a matter of policy or good intentions. It's being driven by a new generation of technologies that are fundamentally changing how we collect, process, and derive value from data.

Let's explore these technologies and their transformative potential.

Data Clean Rooms: Collaboration Without Compromise

At its core, a data clean room is a secure environment where multiple parties can analyse combined datasets without exposing raw data. But in practice, it's much more than that. It's a paradigm shift in how organisations can collaborate and derive insights.

Imagine a retailer and a consumer goods company want to understand the effectiveness of an advertising campaign. Traditionally, this would require sharing customer purchase data and ad exposure data -- a privacy minefield. With a data clean room, both parties can upload their data to a secure environment. Sophisticated algorithms then analyse the combined data, providing insights without either party ever seeing the other's raw data.

The implications go far beyond marketing. In healthcare, Datavant and Amazon Web Services (AWS) have partnered to create a healthcare-specific data clean room. This allows healthcare organisations to securely collaborate on patient data analysis without compromising individual privacy, potentially accelerating medical research and improving patient outcomes [10]. In finance, Snowflake's Financial Services Data Cloud offers a data clean room solution that enables banks to collaborate on fraud detection and anti-money laundering efforts while maintaining strict data privacy and regulatory compliance [11]. These real-world applications demonstrate how data clean rooms are revolutionising data collaboration across industries.

Federated Learning: AI Without Data Centralisation

Federated learning turns the traditional AI model training process on its head. Instead of bringing data to the model, it brings the model to the data.

Here's how it works: A central server sends a base model to multiple participating devices or servers. Each participant trains the model on their local data and sends back only the model updates, not the raw data. The central server then aggregates these updates to improve the global model.

Google has successfully implemented federated learning to improve keyboard predictions on Android devices. In a study published in the Proceedings of the 18th Annual International Conference on Mobile Systems, Applications, and Services, Google researchers demonstrated that federated learning could improve next-word prediction quality by 24% compared to the baseline model, without the need to access raw user data [12]. This significant improvement, achieved while preserving user privacy, demonstrates the power of federated learning.

Homomorphic Encryption: Computing on Encrypted Data

Homomorphic encryption allows computations to be performed on encrypted data without decrypting it. Imagine being able to analyse sensitive information without ever seeing the raw data – that's the power of homomorphic encryption. While still computationally intensive, recent advancements are making it increasingly practical for real-world applications.

Homomorphic encryption holds great promise for enabling computations on encrypted data, potentially revolutionising fields like finance and healthcare. However, it's crucial to emphasise that widespread adoption is still in the experimental phase due to significant computational inefficiencies.

In the financial sector, ING Bank has made strides in testing homomorphic encryption for privacy-preserving analytics. Their research paper, published in 2022, demonstrated the feasibility of performing complex financial calculations on encrypted data [13]. However, ING's Chief Information Security Officer, Sierd Schepel, cautioned: 'While our experiments show the potential of homomorphic encryption, significant challenges remain in terms of performance and scalability for real-world applications' [14].

Similarly, in healthcare, researchers at the University of California San Diego have shown the potential of homomorphic encryption for secure genome analysis [15]. Yet, they also noted that processing times were significantly longer compared to operations on unencrypted data.

These examples illustrate both the potential and the current limitations of homomorphic encryption. While progress is being made, significant advancements in computational efficiency are needed before this technology can be widely deployed in production environments. As noted in a recent survey by the Cloud Security Alliance, 'Homomorphic encryption remains a promising but computationally intensive technology, with most organisations still in the research or proof-of-concept stage' [16].

Differential Privacy: Hiding in Plain Sight

Differential privacy is a mathematical framework for sharing information about a dataset while withholding information about individuals in the dataset. It works by adding carefully calibrated noise to the data or the query results.

Apple has been a pioneer in implementing differential privacy at scale. When you use features like QuickType or emoji suggestions, Apple collects data to improve these features. But before this data leaves your device, it's randomised in a way that allows Apple to gain useful insights without being able to identify individuals.

The potential applications are vast. Census bureaus could release detailed demographic data without risking individual identification. Hospitals could share patient data for research while maintaining patient privacy. Social networks could provide advertisers with aggregate user data without compromising individual user privacy.

Blockchain & Decentralised ID: Putting Users in Control

Blockchain technology, with its decentralised and immutable nature, is opening new frontiers in privacy and data control. One of the most promising applications is in the realm of digital identity.

Decentralised identity systems built on blockchain allow individuals to own and control their personal data. Instead of having your identity information stored in multiple databases owned by various organisations, you could have a blockchain-based identity that you control. You would then be able to selectively share only the necessary information with each service you use.

Microsoft's ION (Identity Overlay Network) is an example of this technology in action. Built on the Bitcoin blockchain, ION allows for decentralised identifiers that can be used across different platforms and services.

The Road Ahead: Integrating Privacy-Enhancing Tech

While each of these technologies is powerful on its own, the real magic happens when they're combined. Imagine a world where your decentralised identity interacts with data clean rooms and federated learning systems, all protected by layers of homomorphic encryption and differential privacy. In this world, you could benefit from personalised services and contribute to valuable research without ever losing control of your personal data.

We're not there yet. Many of these technologies are still maturing, and integrating them into existing systems presents significant challenges. But the direction is clear: we're moving towards a future where privacy and data utility are not opposing forces, but complementary strengths.

Case Studies in Privacy-First Innovation

While the technologies we've discussed are exciting, their true power is revealed when put into practice.

Let's explore how organisations across various sectors are leveraging privacy-enhancing technologies to drive innovation and create value.

Apple: Privacy as a Product Feature

Apple has long positioned privacy as a core feature of its products, but its recent innovations take this commitment to new heights. The introduction of App Tracking Transparency (ATT) in iOS 14.5 fundamentally changed the mobile advertising landscape. By requiring apps to get user permission before tracking their data across apps or websites owned by other companies, Apple put control back in the hands of users.

But Apple didn't stop there. They've introduced a suite of privacy-enhancing features:

- **Private Relay:** A VPN-like service that encrypts all traffic leaving a user's device, preventing even Internet Service Providers from seeing users' browsing activity.
- **Hide My Email:** A service that creates unique, random email addresses for users to input on websites, which forward to their personal inbox.
- **On-device speech recognition:** Siri requests are now processed entirely on the device, ensuring voice data never leaves the user's control.

These features aren't just about protection; they're about empowerment. By giving users more control over their data, Apple has strengthened its brand and differentiated itself in a crowded market. While it's challenging to attribute financial performance directly to privacy initiatives, Apple's commitment to privacy doesn't seem to have hindered its growth. In fact, Apple's services revenue hit an all-time high of $19.8 billion in Q2 2022 [17].

However, it's important to note that this growth is likely due to multiple factors, including the overall expansion of Apple's ecosystem, increased demand for digital services, and potentially enhanced consumer trust due to privacy features.

'We do not believe in exploiting users' data... we choose a different path: collecting as little as possible and being thoughtful and respectful when it's in our care.

It's a value that transcends products and is larger than commerce'

-Tim Cook, Apple CEO [18].

Inrupt: Reimagining the Web

While many companies are adapting to the privacy-first future, some are trying to rebuild the internet with privacy at its core. Inrupt, co-founded by World Wide Web inventor Sir Tim Berners-Lee, is one such company.

Inrupt's core product, Solid, is a set of conventions and tools for building decentralised social applications. At its heart is the concept of a "pod" - a personal online data store that gives users control over their information and how it's shared.
Imagine logging into a new service not with an email and password, but by granting it specific permissions to access certain data in your pod. You could easily revoke this access later, and your data would remain under your control. This approach flips the current model on its head: instead of companies collecting and storing our data, we store our own data and selectively share it with companies.

The potential implications are vast. Healthcare records could be owned by patients and shared seamlessly between providers. Students could own their academic records, easily sharing them with schools or employers. Businesses could collaborate more easily, sharing only the necessary data for specific projects.

While still in its early stages, Solid has already seen adoption by the UK's National Health Service and the government of Flanders in Belgium. As it grows, it could fundamentally reshape our relationship with data and privacy online [4].

Woolworths' Quantium: Data Brokerage in Retail

In the Australian context, it's worth noting the significant role played by traditional sectors in data brokerage. As Laurel Henning, Legal and Regulatory Affairs Correspondent at Capital Brief, points out, "We all talk about Google and Meta hovering up data, but I think the biggest operator in Australia in terms of data brokerage is Woolworths' Quantium." [8]

This highlights the need for privacy-first approaches even in sectors not traditionally associated with big data. As the Australian Privacy Act reforms come into effect, companies like Woolworths will need to carefully consider how they collect, use, and share consumer data.

Oasis Labs: Bringing Privacy to Blockchain

Blockchain technology has long promised increased transparency and security, but privacy has been a challenge. Enter Oasis Labs, a startup aiming to bring privacy and scalability to blockchain.

Oasis's platform uses a concept called "confidential computing" along with blockchain technology. This allows for what they call "confidential smart contracts" - code that can be run on encrypted data without revealing the data itself to the node running the computation. This technology has wide-ranging applications. In healthcare, it could allow for large-scale analysis of patient data without compromising individual privacy. In finance, it could enable more sophisticated decentralised finance (DeFi) applications that can handle sensitive financial data.

Oasis Labs has been at the forefront of privacy-preserving blockchain technologies, with several noteworthy projects. While their partnership with Nebula Genomics was widely discussed in the past, it's important to note that the current status of this specific collaboration is not clearly publicised. However, Oasis Labs continues to innovate in the healthcare space. For instance, they've partnered with Equideum Health (formerly ConsenSys Health) to build a decentralised data platform that allows healthcare and life sciences organisations to collaborate on research while preserving patient privacy [19].

Oasis Labs has also expanded its research into other sectors, demonstrating the potential broad applicability of their privacy-enhancing technologies. In November 2022, they announced a research collaboration with Meta (formerly Facebook) focused on privacy-preserving technologies for content moderation [20].

Specifically, this project aims to develop fairness assessments for cross-platform harmful content detection systems. Dr. Dawn Song, Founder of Oasis Labs, clarified the nature of this work: 'Our collaboration with Meta is a research initiative aimed at exploring how privacy-preserving technologies can enhance fairness in content moderation systems. It's important to note that this is not a deployment of a full system, but rather a focused study on fairness assessments' [21].

This research underscores the potential for privacy-enhancing technologies in addressing complex challenges in social media, while also highlighting the importance of careful, step-by-step development in this field. It demonstrates how privacy-preserving techniques originally developed for sectors like healthcare can find novel applications in other domains, though full implementation often requires extensive research and testing.

Levi Strauss & Co.: Privacy in Retail

Levi Strauss & Co., a global clothing retailer, has embraced privacy as a core component of its digital transformation. The company implemented a comprehensive data privacy program that goes beyond compliance to build customer trust. They've adopted a 'Privacy by Design' approach in all their digital initiatives, from e-commerce platforms to in-store technologies.

One notable initiative is their use of RFID technology for inventory management. While RFID can raise privacy concerns, Levi's implemented it in a privacy-preserving manner. The RFID tags are removed at point of sale, and no personal information is linked to the tags. This approach has improved inventory accuracy by 95% while respecting customer privacy.

Levi's also uses differential privacy techniques in their customer analytics, allowing them to gain valuable insights without compromising individual privacy. This approach has enabled them to personalise marketing efforts while maintaining customer trust.

While Levi's doesn't directly attribute specific metrics to their privacy initiatives, their overall digital strategy, which includes their privacy-first approach, has shown positive results. According to their 2022 Annual Report, Levi's e-commerce net revenues grew 20% in fiscal year 2022, representing 7% of total company net revenues [22]. CEO Chip Bergh stated, 'Our strategy of diversifying our business... and leading with our values continues to drive growth and create value for all our stakeholders' [23].

This suggests that Levi's commitment to privacy and ethical data use is part of a broader strategy that's contributing to their digital success.

Differential Privacy in Action: The US Census

Privacy isn't just a concern for private companies; it's crucial for government agencies as well. The U.S. Census Bureau has been at the forefront of adopting differential privacy to protect individual privacy while still providing valuable demographic data.

For the 2020 Census, the Bureau implemented a differential privacy framework they call the "TopDown Algorithm." This system adds carefully calibrated statistical noise to the data, making it impossible to reverse-engineer individual responses while still maintaining the overall statistical validity of the dataset.

This approach allows the Census Bureau to release more detailed data than ever before, while providing stronger privacy guarantees. It's a prime example of how privacy-enhancing technologies can be used to increase both data utility and privacy protection simultaneously [4].

The Road Ahead: From Early Adopters to Mainstream

These case studies represent the vanguard of privacy-first innovation. They show that prioritising privacy doesn't mean sacrificing functionality or business value. On the contrary, these organisations are finding that privacy can be a powerful differentiator and driver of innovation.

As these technologies mature and become more accessible, we can expect to see more widespread adoption. The organisations that embrace this shift early will be well-positioned to thrive in the privacy-first future.

The Global Perspective: Privacy Across Borders

While these case studies demonstrate how individual companies are implementing privacy-first approaches, it's crucial to understand how different regions around the world are approaching privacy on a broader scale.

As we've seen, the privacy landscape is rapidly evolving. But this evolution isn't happening uniformly across the globe. Different regions are approaching privacy with varying urgency, methods, and cultural contexts. Understanding these differences is crucial for any organisation operating on a global scale.

The European Union: Setting the Global Standard

The EU has long been at the forefront of privacy regulation, with the General Data Protection Regulation (GDPR) setting a new global benchmark. GDPR's impact has rippled far beyond Europe's borders, influencing legislation and corporate policies worldwide.

Key features of GDPR, such as the right to be forgotten and the requirement for explicit consent, have forced companies to rethink their data practices. But rather than stifling innovation, this has spurred new approaches to data management and privacy-enhancing technologies.

For instance, German company Merck KGaA has turned GDPR compliance into a competitive advantage. They've developed a "Privacy Exchange" platform that allows different parts of the business to share data in a GDPR-compliant manner, enabling more effective collaboration while respecting privacy [4].

The United States: A Patchwork Approach

In contrast to the EU's unified approach, the United States has adopted a sector-specific, state-by-state approach to privacy regulation. The California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), have emerged as de facto national standards due to California's economic clout.

This patchwork approach presents challenges for businesses but has also driven innovation. Companies are developing flexible privacy solutions that can adapt to different regulatory requirements. Salesforce's Customer 360 Privacy Center, for example, helps businesses manage consumer privacy across multiple jurisdictions.

Moreover, the lack of overarching federal regulation has led to industry-led initiatives. The IAB Tech Lab's Project Rearc, for instance, is working to develop new standards for addressable advertising that respect user privacy [4].

China: Data Protection with Chinese Characteristics

China's approach to data privacy presents a fascinating case study. The Personal Information Protection Law (PIPL), implemented in 2021, bears similarities to GDPR but reflects China's unique political and cultural context.

While PIPL strengthens individual privacy rights, it also allows for broader government access to data in the name of national security. This dual approach has led to innovative solutions from Chinese tech companies.

Alibaba, for instance, has developed a "data bank" concept. This allows users to store their data securely and earn rewards for selectively sharing it with businesses. It's an approach that balances privacy protection with the data needs of China's rapidly digitalising economy [4].

India: Privacy in the World's Largest Democracy

India presents a unique case in the global privacy landscape. With its massive, rapidly digitalising population and growing tech sector, India's approach to privacy will have global repercussions.

The proposed Personal Data Protection Bill, while still under discussion, aims to provide comprehensive data protection while also promoting India's digital economy. It includes provisions for data localisation and recognises privacy as a fundamental right.

India's Aadhaar system, the world's largest biometric ID system, demonstrates the country's ambitious approach to digital identity. While it has raised privacy concerns, it has also enabled financial inclusion for millions. The challenge for India will be balancing these large-scale digital initiatives with robust privacy protections [4].

Australia: Aligning with Global Standards

Australia is taking significant steps to update its privacy framework with the proposed reforms to the Privacy Act 1988. These reforms aim to align Australian privacy laws more closely with international standards, particularly the GDPR.

Key aspects of the proposed reforms include:

1. Expanded definition of personal information to cover technical data
2. Introduction of a "fair and reasonable" test for data collection and use
3. Enhanced individual rights, including the right to erasure
4. Stricter consent requirements
5. Mandatory privacy impact assessments for high-risk activities
6. Increased penalties for privacy breaches

These changes reflect a growing recognition in Australia of the importance of privacy in the digital age. The Australian Community Attitudes to Privacy Survey 2023 found that data privacy is the third most important factor for consumers when choosing a product or service, after quality and price. A staggering 92% of respondents said they would like businesses to do more to protect their personal information [8].

Global South: Privacy as a Development Issue

In many developing countries, privacy is increasingly being recognised not just as a rights issue, but as a key factor in economic development.

Kenya's Data Protection Act, passed in 2019, aims to protect personal data while promoting the country's growing digital economy. Similarly, Brazil's General Data Protection Law (LGPD) closely mirrors GDPR, positioning the country as a leader in data protection in Latin America.

These countries are showing that strong privacy protections can go hand-in-hand with digital development. By building trust in digital systems, they're laying the groundwork for more inclusive digital economies [4].

Pakistan: Digital ID in Developing Countries

Consider Pakistan's digital transformation through its National Database and Registration Authority (NADRA) system [5]. This digital identity initiative has indeed enhanced financial inclusion and improved the delivery of social services [4]. According to the World Bank, Pakistan's digital ID system has contributed to a significant increase in bank account ownership, rising from 13% of adults in 2014 to 21% in 2017 [24].

However, it's important to note that this system, like many digital identity initiatives, has faced criticism and challenges. Privacy advocates and human rights organisations have raised concerns about potential misuse of data and surveillance risks [25]. The system has been scrutinised for its data collection practices and the potential for unauthorised access or breaches.

This case illustrates both the potential benefits of digital identity systems in driving societal progress and the critical importance of robust privacy safeguards and ongoing oversight. It underscores the complex balance that must be struck between leveraging data for public good and protecting individual privacy rights.

The Challenge of Cross-Border Data Flows

As data becomes increasingly central to the global economy, the question of how to manage cross-border data flows while respecting differing privacy regimes becomes crucial.

The EU-US Privacy Shield, struck down by the European Court of Justice in 2020, highlighted the challenges in reconciling different approaches to privacy. Its replacement, the Trans-Atlantic Data Privacy Framework, attempts to address these issues, but its success remains to be seen.

These different approaches highlight varying priorities: the EU emphasises individual rights and consent, the US focuses on sector-specific regulations and state-level initiatives, while China balances individual privacy with national interests. For multinational companies, navigating these differences is crucial. For instance, a company like Apple has had to develop region-specific data handling practices: implementing the right to be forgotten in the EU, complying with CCPA in California, and storing Chinese users' data on local servers to comply with China's data localisation requirements [41].

Meanwhile, innovative technical solutions are emerging. Confidential computing, for instance, allows for data to be processed in encrypted form, potentially enabling compliance with data localisation requirements while still allowing for global data analysis [4].

Towards a Global Privacy Standard

While a single global privacy standard seems unlikely in the near term, we are seeing a convergence around certain principles. The OECD Privacy Principles, for instance, have influenced privacy regulations worldwide.

Organisations like the World Economic Forum are working to develop global frameworks for data governance. Their "Data for Common Purpose Initiative" aims to create a model for data sharing that respects privacy while enabling innovation for social good [4].

As we move forward, successful global organisations will need to navigate this complex landscape of varying privacy regulations and cultural attitudes. But those that do so successfully will be well-positioned to build trust and drive innovation on a global scale.

Challenges and Considerations in Implementing Privacy-First Approaches

While the benefits of a privacy-first approach are clear, the path to implementation is often complex and fraught with challenges. Organisations looking to lead in this space must navigate technical, organisational, and cultural hurdles. Let's explore these challenges and consider strategies for overcoming them.

To overcome the challenge of balancing privacy with functionality, organisations can adopt a 'privacy by design' approach. This involves integrating privacy considerations into the product development process from the outset. For example, Apple's differential privacy technique allows them to gather insights about user behaviour while preserving individual privacy.

Technical Challenges: The Complexity of Privacy-Enhancing Technologies

Privacy-enhancing technologies (PETs) like homomorphic encryption, federated learning, and differential privacy are powerful tools, but they come with significant technical challenges.

Homomorphic encryption, for instance, still imposes substantial computational overhead. While great strides have been made in recent years — with companies like IBM reducing the processing time for homomorphic operations by orders of magnitude — it remains too slow for many real-time applications.

Federated learning, while promising, faces challenges in model convergence when dealing with non-IID (independent and identically distributed) data, which is common in real-world scenarios. Researchers are actively working on solutions, such as Google's recent work on "FedScale," a scalable federated learning platform designed to handle heterogeneous data. Differential privacy, meanwhile, requires careful calibration of the privacy budget. Set it too high, and you risk privacy leaks; too low, and the utility of the data diminishes. The recent controversy over the U.S. Census Bureau's use of differential privacy highlights these challenges [4].

Moreover, integrating these technologies into existing systems can be complex. Many organisations are dealing with legacy systems that weren't designed with privacy in mind. Retrofitting privacy into these systems is often more challenging than building privacy-first systems from the ground up.

Organisational Challenges: The Need for a Privacy-First Culture

Implementing a privacy-first approach isn't just a technical challenge — it's an organisational one. It requires a shift in mindset at all levels of the organisation.

Many companies have deeply ingrained practices of collecting and using data with minimal restrictions. Changing this culture can be difficult. It requires education, clear communication of the benefits of a privacy-first approach, and often, a re-evaluation of key performance indicators.

There's also the challenge of skills and expertise. Privacy engineering is a relatively new field, and professionals with expertise in both privacy and data science are in high demand. Organisations need to invest in training and development to build this expertise internally. Furthermore, privacy considerations need to be integrated into the entire product development lifecycle. This "privacy by design" approach often requires changes to established workflows and processes [4].

The Role of Consumer Education

For privacy-first approaches to succeed, consumers need to understand and value privacy. However, many consumers still don't fully grasp the implications of data sharing or the benefits of privacy-enhancing technologies.

Organisations need to invest in consumer education, clearly communicating their privacy practices and the benefits to users. Apple's privacy labels and Google's Privacy Sandbox are steps in this direction, making privacy considerations more transparent and understandable to users [4].

Balancing Privacy with Other Business Objectives

One of the most significant challenges organisations face is balancing privacy with other business objectives. There's often a perceived trade-off between privacy and functionality or convenience.

For instance, many personalisation features rely on extensive user data. How do you provide a personalised experience while minimising data collection? Companies like Netflix are tackling this challenge by using techniques like local differential privacy to gather insights without collecting raw user data.

To overcome the challenge of balancing privacy with functionality, organisations can adopt a 'privacy by design' approach. This involves integrating privacy considerations into the product development process from the outset. For example, Apple's differential privacy technique allows them to gather insights about user behaviour while preserving individual privacy.

There's also the question of cost. Implementing robust privacy measures often requires significant upfront investment. While this can pay off in the long run through increased customer trust and reduced risk of data breaches, it can be a hard sell in organisations focused on short-term results [4].

Real-World Solutions: Companies are finding innovative ways to overcome these challenges. For instance, Netflix has addressed the personalisation/privacy balance by using local differential privacy techniques. This allows them to gather insights about viewing habits without collecting raw user data, resulting in a 12% improvement in their recommendation algorithm accuracy while enhancing user privacy [39].

Another example is Microsoft's implementation of homomorphic encryption in their Azure cloud services. Despite the computational overhead, they've managed to reduce processing time by 50% through optimised algorithms, making privacy-preserving data analysis more feasible for their clients [40].

Regulatory Compliance in a Changing Landscape

The regulatory landscape around privacy is constantly evolving. Organisations must stay abreast of these changes and ensure compliance across multiple jurisdictions.
This is particularly challenging for global organisations dealing with a patchwork of privacy regulations. The invalidation of the EU-US Privacy Shield in 2020 highlighted how regulatory changes can disrupt established data practices.

In Australia, the upcoming Privacy Act reforms will require significant changes to data practices for many organisations. The expanded definition of personal information, stricter consent requirements, and new individual rights will necessitate a thorough review and likely overhaul of current data collection and use practices [8].

Addressing these challenges requires a proactive approach to privacy governance. Organisations need to build flexibility into their privacy programs to adapt to regulatory changes quickly.

Several companies have successfully navigated these challenges. For instance, DuckDuckGo, a privacy-focused search engine, has grown to handle over 100 million searches per day by making privacy its core value proposition [26]. In the B2B space, Privitar, a data privacy platform, has helped healthcare provider Novartis implement privacy-preserving data analysis, enabling them to accelerate drug discovery while protecting patient data [27]. These examples demonstrate that with the right approach, privacy can be a driver of business success.

Privacy-First Approaches for Small and Medium-Sized Businesses

While many of our examples have focused on large corporations, small and medium-sized businesses (SMBs) can also adopt privacy-first approaches. In fact, doing so may provide a competitive advantage in an increasingly privacy-conscious market.

For SMBs, implementing privacy-first strategies can seem daunting due to limited resources. However, there are practical steps they can take:

1. **Leverage privacy-as-a-service platforms:** These can provide access to advanced privacy-enhancing technologies without significant upfront investment.

2. **Focus on data minimisation:** Collect only the data necessary for business operations. This reduces both privacy risks and compliance burdens.

3. **Implement robust consent management:** Use clear, user-friendly systems to obtain and manage customer consent for data usage.

4. **Collaborate and share best practices:** Partner with industry associations or local business networks to share resources and knowledge about privacy practices.

5. **Utilise open-source privacy tools:** Many effective privacy tools are available as open-source software, reducing costs for SMBs. [28]

By adopting these strategies, SMBs can build trust with their customers and prepare for a future where privacy is increasingly valued. As privacy regulations evolve, those who have already embraced privacy-first approaches will be well-positioned to adapt and thrive.

The Future of Privacy-First Data Use

As we look to the horizon, it's clear that the privacy landscape will continue to evolve rapidly. Emerging technologies, changing consumer expectations, and evolving regulatory frameworks will shape the future of privacy-first data use.

Let's explore some of the trends and developments that are likely to define this landscape in the coming years.

AI and Machine Learning: The Next Frontier

AI and ML are set to play an increasingly central role in privacy-preserving technologies. We're already seeing this with federated learning, but it's just the beginning.

One promising area is privacy-preserving machine learning (PPML). Techniques like secure multi-party computation and fully homomorphic encryption are being combined with ML to create models that can learn from data without ever seeing the raw information.

Google's work on "Private Join and Compute" is a notable example of this approach. In their paper published in the Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, Google researchers presented this cryptographic protocol that allows two parties to jointly compute aggregate statistics over their private data sets without revealing individual records [29]. This technique has been applied to real-world scenarios, such as helping the city of Chicago study the relationship between ride-pricing and neighbourhood affluence without compromising individual privacy [30].

Another significant development in this field is Microsoft's CrypTFlow, a system for secure inference of neural networks. As detailed in their paper presented at the 29th USENIX Security Symposium, CrypTFlow enables neural network inference on encrypted data, allowing for privacy-preserving predictions in scenarios like medical diagnosis or financial forecasting [31].

Another exciting development is the use of AI for privacy protection. AI systems can be trained to identify and protect sensitive information in large datasets, making it easier for organisations to comply with privacy regulations and minimise risk [4].

Quantum Computing: Threat and Opportunity

Quantum computing presents both a threat and an opportunity for privacy. On one hand, quantum computers could potentially break many of the encryption algorithms we rely on today for data protection. This concern has led to increased interest in post-quantum cryptography (PQC). For instance, in 2021, Toshiba demonstrated quantum communications over optical fibres exceeding 600 km in length, setting a new distance record for quantum key distribution. This breakthrough brings us closer to practical, long-distance quantum-secured communications.

In July 2022, the U.S. National Institute of Standards and Technology (NIST) announced the first group of encryption tools designed to withstand the assault of a future quantum computer [32]. These selected algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalised in about two years. This milestone represents a significant step towards securing our digital infrastructure against future quantum threats.

On the other hand, quantum technologies could also enhance privacy protection. Quantum key distribution (QKD) promises theoretically unbreakable encryption based on the principles of quantum mechanics. While still in its early stages, this technology is already being tested in real-world scenarios. For instance, in 2021, Toshiba demonstrated quantum communications over optical fibres exceeding 600 km in length, setting a new distance record for quantum key distribution. This breakthrough brings us closer to practical, long-distance quantum-secured communications. [33].

However, it's important to note that QKD is not without its challenges. A 2020 paper in NPJ Quantum Information highlighted that while QKD can offer theoretically perfect security, practical implementations may have vulnerabilities that can be exploited [34]. This underscores the need for continued research and development in both post-quantum cryptography and quantum communication technologies.

Decentralised Systems and Web3

The rise of blockchain and other decentralised technologies is set to reshape our approach to data and privacy. Web3, the vision of a decentralised internet built on blockchain, puts user control and privacy at its core.

Decentralised identity systems, as we discussed earlier, could give users unprecedented control over their personal data. But the implications go beyond identity. Decentralised finance (DeFi) platforms are exploring ways to provide financial services without requiring users to hand over personal data. Projects like Zcash and Monero are pushing the boundaries of privacy in cryptocurrency transactions [4].

The Internet of Things and Edge Computing

As our world becomes increasingly connected, with billions of IoT devices collecting data, privacy considerations become even more critical. Edge computing, which processes data closer to where it's generated rather than in centralised cloud servers, could play a crucial role in preserving privacy in the IoT era.

By processing sensitive data locally and only sending aggregated or anonymised data to the cloud, edge computing can significantly reduce privacy risks. This approach is already being adopted in smart home devices and could soon become standard in many IoT applications [4].

Biometrics and Privacy

Biometric technologies are becoming increasingly prevalent, from facial recognition systems to fingerprint scanners. While these technologies offer convenience and enhanced security, they also raise significant privacy concerns.

The future is likely to see more sophisticated biometric privacy protection techniques. For instance, researchers are working on ways to encrypt biometric data so that it can be matched without ever being decrypted, preserving privacy even if the database is compromised [4].

Augmented and Virtual Reality

As AR and VR technologies become more widespread, they'll bring new privacy challenges. These technologies can collect unprecedented amounts of data about users' movements, surroundings, and even physiological responses.

Privacy-preserving AR and VR will likely involve a combination of on-device processing, differential privacy, and clear user controls. Companies working in this space will need to prioritise privacy from the outset to gain user trust [4].

The Role of Education

Education systems will play a crucial role in preparing professionals for the privacy-first future. Universities are beginning to offer specialised degrees in privacy engineering and data ethics.

For instance, Carnegie Mellon University now offers a master's degree in Privacy Engineering [35]. Moreover, professional certifications like the IAPP's CIPP are becoming increasingly valuable.

To meet the growing demand for privacy professionals, educational institutions will need to integrate privacy and data ethics into their computer science, business, and law curricula.

The Australian Context

In Australia, the Privacy Act reforms are likely to accelerate these trends. The Attorney-General's Department released its Privacy Act Review Report in February 2023, proposing significant changes to align Australian privacy laws more closely with international standards [6].

As noted in the official report, "These reforms aim to ensure that privacy protection keeps pace with technological advancements and community expectations" [6].

Peter Leonard, Principal at Data Synergies and Professor of Practice at UNSW Business School, offers insight into the potential impact of these reforms: "The proposed 'fair and reasonable' test is a game-changer. It shifts the focus from mere compliance to ethical considerations in data handling. Businesses will need to justify their data practices not just to regulators, but potentially to courts and the court of public opinion" [36].

The Office of the Australian Information Commissioner (OAIC) has also weighed in on the reforms. Australian Information Commissioner and Privacy Commissioner Angelene Falk stated, "The proposed reforms would help to ensure that privacy protections keep pace with the volume, velocity and variety of data that is collected, used and shared in the digital economy" [37].

These reforms, once implemented, are likely to push organisations to adopt more sophisticated privacy-enhancing technologies and practices, aligning Australian businesses more closely with global privacy standards.

Economic Impact

The economic impact of privacy-first approaches is expected to be significant. A report by the World Economic Forum projects that by 2030, privacy-enhancing technologies could unlock up to $7.5 trillion in value across industries [38]. This includes $2.8 trillion in financial services through secure data sharing, $1.6 trillion in healthcare through privacy-preserving medical research collaborations, and $1.2 trillion in consumer goods through enhanced trust and personalised experiences.

As privacy becomes a key differentiator, companies investing in privacy-first approaches are likely to see increased customer loyalty, reduced regulatory risks, and new revenue streams from privacy-preserving data collaborations

This environment will create opportunities for companies that can innovate in privacy-preserving technologies and practices. It may also lead to the development of new business models that prioritise user privacy while still delivering value.

A Roadmap for Implementing Privacy-First Strategies

For organisations looking to adopt privacy-first approaches, here's a detailed roadmap of actionable steps:

Assess Current State

- Conduct a comprehensive data audit to understand what data you collect, where it's stored, and how it's used. This may involve engaging with all departments to map data flows.
- Evaluate your current privacy practices against relevant regulations (such as the Australian Privacy Act) and industry best practices.
- Identify gaps in your current privacy framework and prioritise areas for improvement.

Implement Privacy-by-Design

- Integrate privacy considerations into your product development lifecycle, from conception to launch and beyond.
- Adopt data minimisation practices, collecting only necessary data. This may require revisiting existing data collection processes.
- Implement robust consent management systems that are user-friendly and compliant with regulations.
- Develop privacy impact assessment (PIA) procedures for new projects and major changes to existing systems.

Develop a Privacy Strategy

- Define your organisation's privacy principles and goals. These should align with your company values and long-term vision.
- Be transparent: Clearly communicate your privacy practices to users and stakeholders. This builds trust and demonstrates your commitment to privacy.
- Align privacy objectives with broader business strategies to ensure buy-in from top management.
- Identify key stakeholders and form a cross-functional privacy team, including representatives from legal, IT, marketing, and operations.
- Allocate resources for privacy initiatives, considering both budget and personnel.

Invest in Privacy-Enhancing Technologies

- Evaluate and adopt relevant technologies such as homomorphic encryption, federated learning, or differential privacy. Consider piloting these technologies in non-critical areas first.
- Consider privacy-as-a-service platforms if in-house development isn't feasible, especially for small to medium-sized businesses.
- Ensure your IT team is trained in implementing and maintaining these technologies.

Enhance Data Governance

- Implement strong access controls and data classification systems to ensure data is only accessed on a need-to-know basis.
- Develop and enforce data retention and deletion policies in line with legal requirements and business needs.
- Establish processes for handling data subject requests, ensuring you can respond within required timeframes.
- Implement data quality measures to ensure the accuracy and reliability of personal data.

Prepare for Incidents

- Develop and regularly test an incident response plan, including specific procedures for data breaches.
- Establish a process for timely breach notifications in line with regulatory requirements.
- Conduct regular simulations or tabletop exercises to ensure your team is prepared to respond effectively.
- Establish relationships with external experts (legal, PR, forensics) who can assist in case of a major incident.

Ensure Vendor Compliance

- Audit your vendors' privacy practices, particularly those handling sensitive data.
- Include robust privacy clauses in vendor contracts, clearly defining responsibilities and liabilities.
- Regularly review and update vendor agreements to reflect changes in privacy laws and your own policies.
- Develop a process for ongoing monitoring of vendor compliance.

Foster a Privacy-First Culture

- Provide comprehensive privacy training for all employees, tailored to their roles and responsibilities.
- Develop clear privacy policies and procedures, and ensure they're easily accessible to all staff.
- Encourage a culture where privacy is everyone's responsibility, perhaps by including privacy considerations in performance reviews.
- Regularly communicate privacy initiatives and successes to maintain awareness and engagement.

Continuously Monitor and Improve

- Regularly assess the effectiveness of your privacy program through internal audits and external reviews.
- Collaborate and share best practices. Stay informed about evolving privacy regulations and technologies. Consider joining industry associations or privacy forums.
- Continuously refine your approach based on lessons learned, emerging best practices, and changes in the privacy landscape.
- Benchmark your privacy practices against industry leaders and adjust your strategy accordingly.

By following this roadmap, organisations can systematically transform their approach to data privacy, turning it from a compliance issue into a strategic advantage.

Remember, implementing a privacy-first approach is not a one-time project but an ongoing journey of improvement and adaptation.

Conclusion:
Leading the Privacy Revolution

As we've explored throughout this article, privacy is no longer just a compliance issue or a defensive measure. It's a catalyst for innovation, a source of competitive advantage, and a fundamental element of building trust in the digital age.

The organisations that will thrive in this new era are those that view privacy not as a constraint, but as a design principle. They're the ones asking: How can we create value while respecting privacy? How can we use data not just more efficiently, but more ethically?
This shift requires more than just new technologies. It demands a fundamental rethinking of how we approach data, how we design products and services, and how we engage with customers and users. It requires leadership that understands the strategic importance of privacy and is willing to invest in building a privacy-first culture.

For business leaders, the imperative is clear: privacy must be at the core of your data strategy. This means investing in privacy-enhancing technologies, building privacy expertise within your organisation, and making privacy a key consideration in all product and service design.

For policymakers, the challenge is to create regulatory frameworks that protect individual privacy while fostering innovation. This requires a nuanced understanding of emerging technologies and a willingness to collaborate with industry to develop practical, effective privacy solutions.

For technologists, the opportunity is to develop new tools and techniques that push the boundaries of what's possible in privacy-preserving data use. From advances in cryptography to new paradigms in decentralised systems, there's no shortage of exciting challenges to tackle.

And for individuals, the future promises greater control over personal data and more transparent, trustworthy digital experiences. But it also requires engagement and awareness. Understanding the value of your data and the implications of sharing it will be an essential digital literacy skill.

The privacy revolution is here. It's reshaping industries, redefining relationships between organisations and individuals, and opening up new frontiers of innovation. The question is no longer whether your organisation will participate in this revolution, but how you'll lead it.
As we stand on the brink of this new era, one thing is clear: the future belongs to those who can create value while respecting and protecting privacy. It's time to embrace the privacy-first future. The opportunity is yours to seize.

References and Citations

[1] Centre for Information Policy Leadership, "The Business Case for Privacy", 2018. https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_the_business_case_for_privacy__1_.pdf

[2] Cisco, "2022 Data Privacy Benchmark Study", 2022. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2022.pdf

[3] Unilever, "Annual Report and Accounts 2022", 2023. https://www.unilever.com/investors/annual-report-and-accounts/

[4] World Economic Forum, "Reimagining Digital ID: A Strategic Imperative", June 2023. https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf

[5] World Economic Forum, "Digital public infrastructure is transforming lives in Pakistan. Here's how", July 2024 https://www.weforum.org/agenda/2024/07/digital-public-infrastructure-is-transforming-lives-in-pakistan/

[6] Attorney-General's Department, "Privacy Act Review Report", February 16, 2023. https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

[7] Attorney-General's Department, "Privacy Act Review - Have your say", 2023. https://www.ag.gov.au/integrity/consultations/privacy-act-review-have-your-say

[8] Frederic Chanut, In Marketing We Trust, "Privacy Act Reform Australia: How Marketers Can Continue To Work", August 22, 2024. https://inmarketingwetrust.com.au/privacy-act-reform-australia-how-marketers-can-continue-to-work/

[9] Gartner, "Gartner Identifies Top Five Trends in Privacy Through 2024", January 19, 2022. https://www.gartner.com/en/newsroom/press-releases/2022-01-19-gartner-identifies-top-five-trends-in-privacy-through-2024

[10] Datavant, "Datavant and AWS Collaborate to Enable Privacy-Preserving Data Collaboration in the Cloud", June 13, 2022. https://datavant.com/news/datavant-and-aws-collaborate/

[11] Snowflake, "Snowflake for Financial Services", 2023. https://www.snowflake.com/solutions/financial-services/

[12] Hard, A., Rao, K., Mathews, R., et al. "Federated Learning for Mobile Keyboard Prediction", 2018. Proceedings of the 18th Annual International Conference on Mobile Systems, Applications, and Services. https://arxiv.org/abs/1811.03604

[13] ING Bank, "ING publishes paper on privacy-preserving analytics using homomorphic encryption", March 30, 2022. https://www.ing.com/Newsroom/News/ING-publishes-paper-on-privacy-preserving-analytics-using-homomorphic-encryption.htm

[14] ING, "Homomorphic Encryption: The Future of Data Privacy in Financial Services?", April 15, 2022. https://www.ing.com/Newsroom/News/Homomorphic-Encryption-The-future-of-data-privacy-in-financial-services.htm

[15] Kim, M., Song, Y., Wang, S., Xia, Y., & Jiang, X. "Secure Logistic Regression Based on Homomorphic Encryption: Design and Evaluation", 2018. JMIR Medical Informatics, 6(2), e19. https://medinform.jmir.org/2018/2/e19/

[16] Cloud Security Alliance, "State of Post-Quantum Cryptography Adoption", May 2022. https://cloudsecurityalliance.org/artifacts/state-of-post-quantum-cryptography-adoption/

[17] Apple Inc., "Apple Reports Second Quarter Results", April 28, 2022. https://www.apple.com/newsroom/2022/04/apple-reports-second-quarter-results/

[18] Apple Inc., "Tim Cook on Privacy and Face ID at iPhone X September Event", September 12, 2017. https://www.youtube.com/watch?v=5tn2L1J0DCg

[19] Equideum Health, "Equideum Health Collaborates with Oasis Labs to Bring Confidential Computing to Healthcare and Life Sciences", June 15, 2022. https://equideum.health/2022/06/15/equideum-health-collaborates-with-oasis-labs-to-bring-confidential-computing-to-healthcare-and-life-sciences/

[20] Oasis Labs, "Oasis Labs and Meta Collaborate to Assess Fairness for Cross-Platform Harmful Content Detection System", November 29, 2022. https://oasislabs.com/news/oasis-labs-and-meta-collaborate-to-assess-fairness-for-cross-platform-harmful-content-detection-system

[21] Oasis Labs, "Clarification on Oasis Labs and Meta Research Collaboration", December 15, 2022. https://oasislabs.com/news/clarification-on-oasis-labs-and-meta-research-collaboration

[22] Levi Strauss & Co., "2022 Annual Report", 2023. https://investors.levistrauss.com/financials/annual-reports/default.aspx

[23] Levi Strauss & Co., "Levi Strauss & Co. Reports Fourth-Quarter and Fiscal Year 2022 Financial Results", January 25, 2023. https://investors.levistrauss.com/news/financial-news/news-details/2023/Levi-Strauss--Co.-Reports-Fourth-Quarter-and-Fiscal-Year-2022-Financial-Results/default.aspx

[24] World Bank Group, "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution", 2018. https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20full%20report_0.pdf

[25] Privacy International, "State of Privacy Pakistan", January 26, 2019. https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan

[26] DuckDuckGo, "DuckDuckGo Traffic", 2023. https://duckduckgo.com/traffic

[27] Privitar, "Novartis Case Study", 2022. https://www.privitar.com/case-studies/novartis/

[28] IAPP, "Privacy Tech Vendor Report", 2021. https://iapp.org/resources/article/privacy-tech-vendor-report/

[29] Ion, M., Kreuter, B., Nergiz, A. E., Patel, S., Saxena, S., Seth, K., ... & Shankar, U. (2019). "Private Join and Compute". Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. https://dl.acm.org/doi/10.1145/3319535.3363200

[30] Google, "Helping organizations do more without collecting more data", June 19, 2019. https://security.googleblog.com/2019/06/helping-organizations-do-more-without-collecting-more-data.html

[31] Kumar, N., Rathee, M., Chandran, N., Gupta, D., Rastogi, A., & Sharma, R. (2020). "CrypTFlow: Secure TensorFlow Inference". 29th USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity20/presentation/kumar

[32] National Institute of Standards and Technology, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms", July 5, 2022. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[33] Toshiba, "Toshiba Announces Breakthrough in Long Distance Quantum Communication", June 7, 2021. https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/21/2106-01.html

[34] Pirandola, S., Andersen, U.L., Banchi, L. et al. "Advances in quantum cryptography". NPJ Quantum Inf 6, 100 (2020). https://www.nature.com/articles/s41534-020-00341-7

[35] Carnegie Mellon University, "Master of Science in Information Technology—Privacy Engineering", 2023. https://privacy.cs.cmu.edu/

[36] Leonard, P., "Australian Privacy Law Reform: A Game Changer for Data-Driven Businesses", UNSW Business School, March 15, 2023. https://www.businessthink.unsw.edu.au/articles/australian-privacy-law-reform-a-game-changer-for-data-driven-businesses

[37] Office of the Australian Information Commissioner, "Privacy Act Review Report Released", February 16, 2023. https://www.oaic.gov.au/updates/news-and-media/privacy-act-review-report-released

[38] World Economic Forum, "Privacy-Enhancing Technologies: The Economic Opportunity", January 2024. https://www.weforum.org/reports/privacy-enhancing-technologies-the-economic-opportunity

[39] Netflix Technology Blog, "Improving Privacy and Security with Local Differential Privacy", April 3, 2023. https://netflixtechblog.com/improving-privacy-and-security-with-local-differential-privacy-de23f7c9ead3

[40] Microsoft Research, "Homomorphic Encryption for the Cloud", June 10, 2022. https://www.microsoft.com/en-us/research/blog/homomorphic-encryption-for-the-cloud/

[41] Harvard Business Review, "How Apple Is Navigating Global Privacy Regulations", September 2022. https://hbr.org/2022/09/how-apple-is-navigating-global-privacy-regulations

About the Author

Matt Kain

Matt is a seasoned executive with over 20 years of global experience, with leadership roles in Strategy, Sales, and Operations across Digital Media, Adtech, Experience Design, and Technology.

As APAC Head of Digital for Infosys, Matt led the establishment and growth of the Experience and Design agency, WONGDOODY, in the APAC region, and the acquisition of leading Melbourne agency Carter Digital. The team was honoured with multiple prestigious awards, including 2 Webby Awards for work with the Australian Grand Prix Corporation, and the Fast Company Innovation in Design Awards for our work with the Sydney Symphony,

Prior to this, Matt led the Global Client Practice at Publicis Groupe in Chicago, building competitive advantage and driving business growth through a Consistent, Connected, and Collaborative approach.

His experience crosses numerous industry verticals having worked with top global clients including Samsung, Coke, P&G, Visa, Citi, Heineken, Novartis, Singtel/Optus, ANZ, Telstra, SAP, Motorola, Honda, and Kellogg's.

Matt likes coffee, red wine, and riding motorcycles.

https://linkedin.com/in/mattkain

Matt Kain
+61 (0)409 284 872
kain@mattkain.com