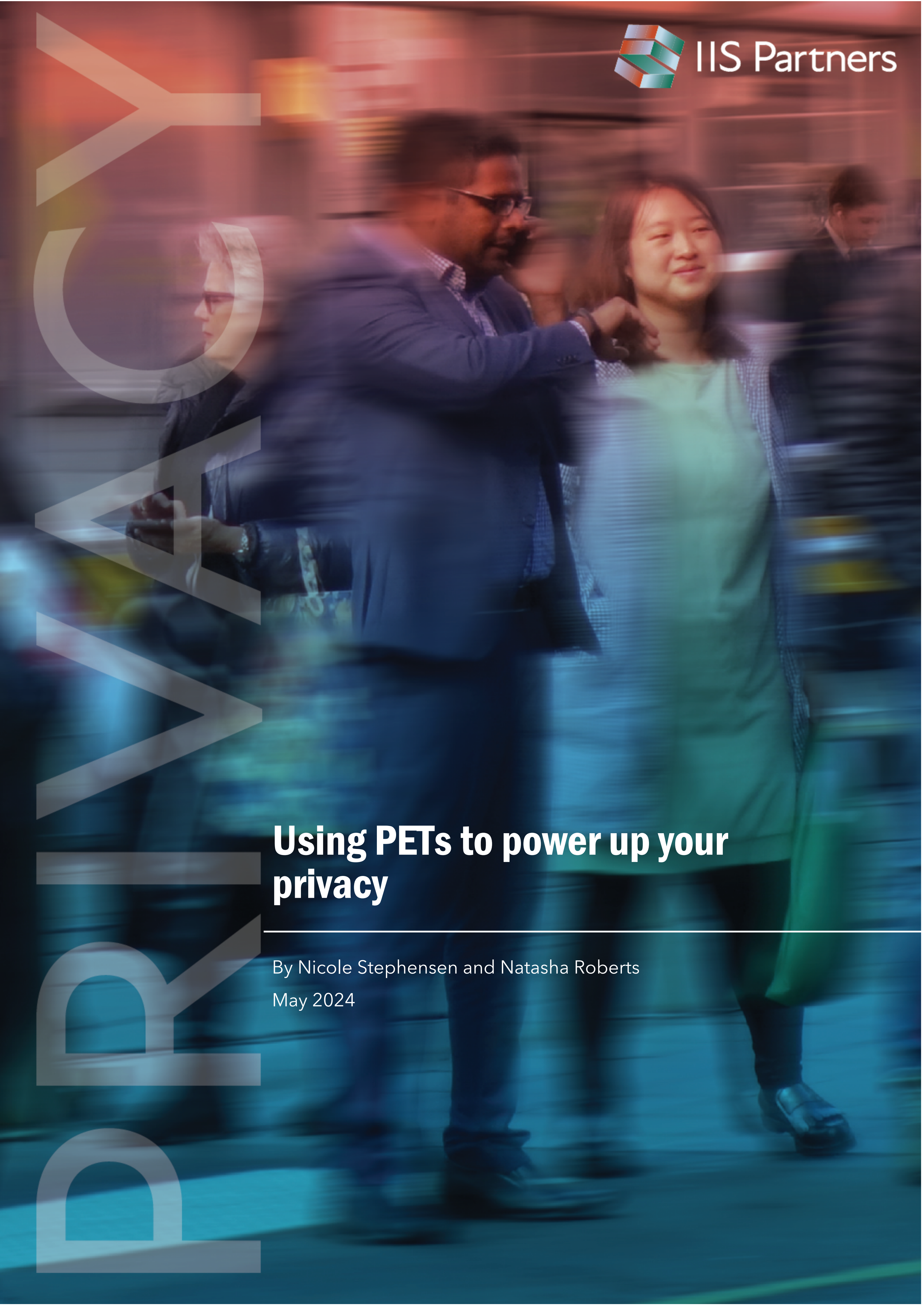
IIS Partners



Using PETs to power up your privacy

By Nicole Stephensen and Natasha Roberts

May 2024

Using PETs to power up your privacy

Introduction

In support of Privacy Awareness Week 2024, themed '*Power up your privacy*', IIS Partners and our technology subsidiary TrustWorks360 explore Privacy Enhancing Technologies (PETs) and how these can be used to enhance the privacy posture of organisations (including private, public and not-for-profit sectors) [1].

Weighing in on the importance of accountable and secure personal information handling practice, opportunities PETs offer in this regard, and the challenges or barriers to PET adoption, is a panel of experts operating at the deep intersection of privacy, cybersecurity, technology policy, law and social licence:

- **Clarisse Girot** – Head of Data Governance and Privacy, Organisation for Economic Cooperation and Development (OECD)
- **Dr Katina Michael** – Professor, School for the Future of Innovation in Society, Arizona State University (ASU)
- **Branko Ninkovic** – Founder, Dragonfly Technologies and Board Member, Australian Information Security Association (AISA)
- **Sophie Bradshaw** – Partner (Privacy, Data and Technology Law), Hamilton Locke
- **Nicole Stephensen** – Partner and Privacy Lead, IIS Partners and Lead Privacy Advisor, TrustWorks360.*

* Expert views are their own, shaped by their industry experience and proficiencies.

Using PETs to power up your privacy

Good privacy practice

It is well established that adhering to principles of security and accountability is vital for personal information management. In both organisational and government contexts, these principles support material business interests as well as the public interest in knowing that information provided by individuals in exchange for goods, services or benefits is responsibly managed through its lifecycle.

Good privacy practice requires consistent attention to the personal information lifecycle – from the moment it is collected or ingested into the organisation until it is de-identified or securely destroyed. This can have several outcomes, such as:

Trust

When organisations take responsibility (i.e., are accountable) for how they collect, use, protect, share and dispose of personal information, this builds trust with customers, employees, and other stakeholders. There is power in community confidence that their information is being handled with care. Prioritising security and accountability, and being transparent about this, can lead to enhanced customer relationships and loyalty (and supports social licence of the organisation).

Compliance

Paying close attention to principles of security and accountability (and other 'privacy principles') supports the organisation in demonstrating compliance with privacy laws. Conversely, failure to comply with privacy laws can result in enforcement action (such as fines) and reputational damage – and importantly, harm to individuals.

Safe data

Implementing security measures across physical, technical and administrative domains is essential for data breach prevention; that is, it helps protect personal information from unauthorised access, use, disclosure or loss.

Reduced risk

In addition to data breach prevention, good privacy practice positively impacts the broader risk posture of the organisation, helping to safeguard against potential financial losses, legal liabilities, and damage to reputation.

Using PETs to power up your privacy

To underscore **the importance of accountability and security of information practice in organisations and governments,** our expert panel said:

Importance of accountability and security of information practice

Clarisse Girot (OECD)

The accountability principle is one of the eight principles of the OECD Privacy Guidelines, and reflects a global consensus that accountability comprises the taking of responsibility for personal data use and a means to demonstrate this to other stakeholders. The taking of responsibility suggests leadership from top management and the cascading of responsibility throughout the organisation. In addition, ethical considerations regarding data are increasingly becoming a necessary part of accountability, particularly given that personal data use has become more complex, entailing impacts on a broad range of stakeholders. The concept of accountability also encompasses the notion that the organisation is legally responsible for its data protection practices including before the judicial system.

Katina Michael (ASU)

In a world that has become reliant on data-driven solutions as the foundation upon which to make evidence-based decisions, the demand for dynamic consent that requires on-going communication between stakeholders and data custodians is unquestionable. Privacy is no longer a "nice to have" add-on functional requirement fulfilled only if there is budget left over, rather it is at the very heart of the design and development of any service offering, essential and integral to its long-term success.

Branko Ninkovic (Dragonfly)

Data is being transferred and stored at an exponential rate. Organisations and governments collect data to enhance, personalise or optimise experiences. Our reliance as consumers of these services and the casual or ill-informed acceptance of data protection statements is why we need accountability. Accountability is a driver for the safe keeping of our data within organisations and governments while privacy laws and regulations are the levers towards accountability. Organisations and governments that demonstrate transparency and accountability are better prepared than those who do not and in time consumers will choose what information they share and with whom. Information is at the heart of our society and strength our economies.

Sophie Bradshaw (Hamilton Locke)

International privacy principles of accountability and security are enshrined in Australia's privacy laws. As these laws are principles-based and generally employ a "reasonableness" test, it requires organisations and governments to take into account their particular circumstances, as well as current standards and community expectations. This often means decisions around information handling practices are not static and should not only consider legal obligations ("can we do it"), but also broader ethical, reputational and social licence considerations ("should we do it").

Nicole Stephensen (IIS/ TW360)

That privacy is an important consideration for organisations and governments is not new; however, the questions of how to 'be accountable' and how to 'be secure' are not always easy to answer, immediately obvious or cost neutral. Good privacy practice, therefore, requires a continued and frank dialogue about what privacy means for the organisation and the community it serves.

Using PETs to power up your privacy

What are PETs?

Privacy Enhancing Technologies (PETs) are tools, techniques, or mechanisms designed to protect individuals' privacy and personal information in various digital environments. These technologies aim to enhance privacy by minimising the collection, use, and disclosure of personal information, as well as by increasing a person's ability to control what happens to the information about them. PETs may work in conjunction with one another or be used standalone.

The OECD groups PETs into four categories [2]:

1. *Data obfuscation tools* – these embrace anonymisation/pseudonymisation, synthetic data and zero-knowledge proofs, among others.
2. *Encrypted data processing tools* – which comprise homomorphic encryption, multi-party computation, private set intersection and trusted execution environments.
3. *Federated and distributed analytics* – which include federated and distributed learning, allowing executing of analytical tasks upon data that are not accessible to those executing the tasks.
4. *Data accountability tools* – which encompass key technologies such as accountable systems and personal data stores.

PETs have been on the scene for a while now but the way we think about them has evolved. Academics were among the first to begin discussing and researching PETs, with the concept emerging in the 1990s as an area of study within the field of computer science and privacy research. Academics, researchers, and experts in privacy, cryptography, data anonymity, and other related fields have been instrumental in developing, studying, and promoting the use of PETs to enhance privacy and data protection in various contexts.

Now our understanding of PETs appears to have expanded and shifted, including an awareness of these tools as real for-purchase 'solutions' that organisations and governments can plug into or deploy to support their privacy and data governance programs. Additionally, where initially a key focus of PETs was protecting information at the perimeter of the organisation, this has modulated to a focus on enabling continuity of privacy protection even as data moves inside and outside an organisation.

Using PETs to power up your privacy

PETs to enhance security and accountability

A security use case

In Australia, organisations have some latitude with how they use and deploy PETs. This is due to the tech-neutral principles-based approach to privacy regulation here which requires organisations to follow overarching rules in relation to their personal information handling practices, but which leaves the fine-grained specifics of compliance up to the organisation. This is reflected in information security principles in Commonwealth and state/territory-based privacy legislation which require organisations to 'take steps as are reasonable in the circumstances' to secure personal information – it is up to the organisation to decide what those reasonable steps are in light of its own situation, operations and the amount, type, sensitivity and privacy risk associated with personal information it handles.

Due to this framing, Australian privacy laws offer flexibility *and* allow organisations to make use of cutting-edge PETs. Indeed – considering a social media or marketing organisation that processes large amounts of personal information and draws revenue from its uses – using such technologies in the processing of personal information may support the organisation in meeting 'reasonable steps' requirements.

Within this regulatory context, to treat investments in PETs as *optional* rather than *necessary* is risky. Consider the relatively common but seldom discussed problem of data leakage from websites or platforms, for example: If such data (which may include elements too voluminous for personnel to monitor or count) is identifiable, and its leakage places the individual (or several individuals) it is about at risk of a privacy harm, how would the organisation even know or prevent this if not actively scanning for the problem? And more, assuming the leakage amounts to a data breach under relevant privacy legislation, the organisation may be called upon by the regulator to justify decisions it has made in relation to protecting data. A PET – i.e., a tool for monitoring and preventing data leaks – could play a critical role in both demonstrating and offering assurance that an organisation is doing all it can to protect the personal information it holds.

An accountability use case

Currently, the Australian Government is in the process of reforming the *Privacy Act 1988*. Reform proposals will not change the tech-neutral, principles-based approach of the Act. However, the Government has signalled its acceptance, in principle, of proposals for the introduction of a fair and reasonable test. IIS has previously explained why it supports the introduction of such a test [3]. The test would require that collection, use and disclosure of personal information be 'fair and reasonable in the circumstances'.

The introduction of the fair and reasonable test will put greater onus on organisations to treat personal information fairly. For data intensive industries, this may necessarily involve greater engagement with, and use of, PETs to ensure data handling occurs in a manner of seamless integration with (as opposed to being frustrated by) privacy rules.

Consider, for example, a healthcare organisation conducting research on patient data to identify trends and improve healthcare outcomes. By applying a PET – such as differential privacy (a form of data obfuscation) – to the data analysis process, the organisation can analyse the data in a way that prevents the identification of specific individuals, reducing the risk of re-identification and unauthorised disclosure of an individual's health information.

Differential privacy in this context allows the organisation to balance the need for data analysis and research with the protection of individuals' privacy rights, enabling fair and responsible information practice by anonymising data and preventing unauthorised access or some other misuse of sensitive information.

In the digital age, if organisations are to retain the trust and participation of individuals, demonstrating rigour and accountability in information practice – which includes evidencing controls in place to collect and manage personal information in accordance with privacy requirements – using technological solutions may be the 'secret sauce'.

.

Using PETs to power up your privacy

When weighing in on the question of ***whether PETs present an opportunity to power up privacy*** (noting the complementary and often intersecting objectives of privacy, information security, data governance and risk management), our expert panel said:

Benefits of adopting Privacy Enhancing Technologies

Clarisse Girot (OECD)

PETs enable a relatively high level of utility from data, while minimising the need for data collection and processing. PETs are not new but latest advances in connectivity and computation capacity have led to a fundamental shift in how data can be processed and shared. While still in their infancy, these developments hold immense potential to move society closer to the continuing process and practice of privacy by design, and thereby to foster trust in data sharing and re-use. A growing number of policy makers and privacy enforcement authorities are thus considering how they can promote the use of PETs in their domestic privacy and data protection frameworks and stimulate research in this area. The OECD has just launched an ambitious international cooperation program to support these reflections.

Katina Michael (ASU)

I really believe that all technologies must be privacy-enhancing. Why? Because PETs have the ability to accelerate stakeholder data strategy. It's a bit like asking whether good digital design practice is needed for certain age groups or is good for all users. Well, of course, PETs should be the default, allowing even greater feature innovation because end-users know their data has never actually left their device.

Branko Ninkovic (Dragonfly)

In my mind, there is no doubt that PETs present a great opportunity to power up privacy. However, for PETs to power up privacy there needs to be wider adoption of PETs inside organisations and governments. The drivers for PET adoption will largely be driven by how PET can help meet and how PET can reduce cost to meet an internal privacy goal or maintain regulatory compliance. With adoption, privacy will power up.

Sophie Bradshaw (Hamilton Locke)

We are seeing a different political and regulatory approach to holding organisations accountable for their privacy practices, particularly when it comes to data breaches. This is largely driven by increased community concern and the evolving cyber threat landscape. The clear message from regulators is that organisations (and their Boards) are on notice that they must know what data they hold, are prepared for a data breach and are not holding unnecessary data. PETs can be a useful tool to help regulated entities meet this challenge and support broader privacy management and data governance frameworks.

Nicole Stephensen (IIS/ TW360)

In the context of addressing organisational privacy risk, particularly where there is a business requirement to ingest and manage large volumes of personal information, PETs have the potential to make possible (at scale) data rigour in relation to personal information 'discovery', information flow mapping, retention and disposal scheduling and data leakage prevention/ remediation that could not be accomplished in a reasonable timeframe by one person or team.

Barriers to PET adoption

Determining whether and how to deploy PETs should be a critical agenda item for those working to support organisational privacy outcomes. So, why isn't it?

The sophistication of the technology that underpins many PETs has had two wider effects. First, greater PET sophistication has expanded the circumstances under which personal information can be safely re-used, leveraged and shared. Second, greater PET sophistication (and tech sophistication generally) has, according to the OECD, created a 'language barrier' between software engineers developing and deploying those technologies and everyone else [4]. Such a language barrier has the potential to adversely affect a range of decision-makers including C-suite executives responsible for internal resourcing allocation, privacy teams and officers responsible for overseeing enterprise compliance with privacy laws, and even governments and lawmakers trying to reform legislation to keep pace with emergent privacy risks and opportunities.

Without a solid grasp of new currents in data processing and associated PETs, organisations risk poor decision-making, weak data governance and legal non-compliance. It may, for example, be difficult for a Board to see the benefit in investing in tools that, on their face, appear costly and unnecessary if those on the Board have low insight into the nature of those tools, the operational return-on-investment those tools represent, or how wider organisational goals can be advanced by such an investment. The language barrier may therefore create a real obstacle to organisations stepping up the maturity of their data-centric (and therefore privacy-related) operations.

A notion that PETs have the potential to close down data use or curtail innovation is a case of mistaken impression. Of the four categories of PETs described above, the first three (data obfuscation, encrypted data processing, and federated and distributed analytics) all *facilitate* safe data use. In some cases, data use might otherwise be prohibited or strictly limited under legislation but for the use of a PET. And, as an organisation's data processing becomes more complex, the final PET category – data accountability – becomes all the more critical to ensuring meaningful and demonstrable data governance is baked into system BAU operations through automation and privacy integration.

.

Using PETs to power up your privacy

When weighing in on the question of ***barriers to PET adoption***, our expert panel said:

Barriers to adopting Privacy Enhancing Technologies

Clarisse Girot (OECD)

The highly technical and fast evolving nature of the technologies underlying PETs, and the associated costs, often present a barrier to implementation by organisations and to their consideration in policy and legal frameworks applicable to data. As well, regulators are cautious about adopting definitive positions on the merits of certain PETs to meet specific legal requirements, for example on cross-border data transfers, which underscores the difficulty in definitively validating specific PET solutions in a rapidly evolving landscape. The OECD is currently analysing these obstacles within the framework of a dedicated multi-stakeholder working group, to determine if these obstacles can be removed to facilitate the implementation of these technologies in specific use cases.

Katina Michael (ASU)

I am going to say the #1 barrier is the perceived cost. The value proposition for privacy is still not well-understood in terms of potential return on investment, brand power, and user experience. It means we have to change our business thinking and declare a focus on privacy as being a competitive advantage ensuring the long-term sustainability of products and processes.

Branko Ninkovic (Dragonfly)

I agree with the statements from the panel. Privacy barriers have the same challenges as Information Security. Proactive versus reactive organisations. The largest barrier to PET adoption will be reactive organisation who either are under resourced or do not have the financial appetite to implement PETs. Again, like in Information Security there still needs to be a demonstrated return on investment – and, failing that, laws to drive good privacy practices – then the adoption of PETs will take hold.

Sophie Bradshaw (Hamilton Locke)

Operationalising legal obligations under the Privacy Act (and related laws with respect to cyber security risk management, such as security of critical infrastructure and corporations legislation) and contractual obligations with respect to the secure handling of data is not always easy. Where the right PET tool is chosen and properly implemented and maintained, the cost of procurement can help mitigate the potential cost to a regulated entity of not properly operationalising their privacy compliance obligations.

Nicole Stephensen (IIS/ TW360)

The mainstream existence of PETs and their practical application in organisational and government contexts remains somewhat opaque. In my experience, much of the information about PETs exists in academic or vendor domains, and privacy teams are not necessarily tapped into this. Where privacy teams are aware, they may not be empowered within their organisational or government contexts to raise the opportunities presented by PETs to those with decision-making authority (but I see this as a broader barrier to good privacy practice, not just a barrier to PET adoption).

Using PETs to power up your privacy

Key takeaways

The expert panel has provided the following key takeaways for your organisation to consider when adopting PETs to ‘power up your privacy’:

- Good privacy practice requires attention to matters of accountability and security
- PETs are many and varied, and can be grouped into four broad categories:
    a. Data obfuscation
    b. Encrypted data processing
    c. Federated and distributed analytics
    d. Data accountability
- There are practical use cases for PETs
- There are also barriers to the adoption of PETs
- As our understanding of PETs and their practical application grows, barriers to their adoption may soften or dissolve altogether, allowing for these tools, technologies and mechanisms to meaningfully support (or ‘power up’) organisational privacy programs.

Bibliography

1. IIS Partners, <https://www.iispartners.com/>; TrustWorks360, <https://www.trustworks360.com>.
2. OECD, ‘Emerging privacy-enhancing technologies: Current regulatory and policy approaches’, (2023) *OECD Digital Economy Papers No 351*, <https://doi.org/10.1787/bf121be4-en>.
3. IIS Partners, ‘Privacy Act review: A closer look at the fair and reasonable test’, (2023) *Insights Post*, <https://www.iispartners.com/insights/2023/11/23/privacy-act-review-a-closer-look-at-the-fair-and-reasonable-test>.
4. OECD, ‘Emerging privacy-enhancing technologies: Current regulatory and policy approaches’, (2023) *OECD Digital Economy Papers No 351*, <https://doi.org/10.1787/bf121be4-en>.

IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898