Personal data should be an asset on the balance sheet

Improving current accounting standards could work as a regulatory tool and contribute to an organisation's privacy preparedness. By **Dr John Selby** of Privcore.

The information revolution that has fundamentally altered our society is fueled by data, particularly personal information, enabling significant efficiency gains and innovative solutions to problems. The benefits of handling data also pose risks of significant harms.[1]

Governments and industry regulators have responded to the risks of harms from cyber-attacks and privacy breaches through an array of strengthened regulations. In Australia, we have privacy legislation at the federal level and in most states/territories, as well as sectoral regulation, directors' duties under the Corporations Act, the Security of Critical Infrastructure Act, ASX Listing Rules requiring disclosure of market sensitive information, and proposals for a Cyber Security Act (amongst others). Similar, or stronger, regulatory regimes exist or are under development in many comparable jurisdictions.

Whilst most of these laws, codes and regulations seek to incentivise uplift in organisations' cyber security and privacy maturity through threats of post-breach sanctions, evidence suggests that many government agencies and the private sector are still under-investing in cyber security and privacy controls.[2] One contributing factor to this under-investment is the failure to account for externalities when making funding decisions on cyber security and privacy controls, such as in the original (still widely-used) Gordon-Loeb 2002 model for calculating cyber security investments.

Reactive regulation is not the only way to alter the decisions made by organisational leaders. Proactive regulation which incentivises organisations to uplift their cyber security and privacy maturity on a regular basis regardless of whether a breach has occurred is another option, which arguably has received less attention from scholars, government and industry experts.

Accounting standards hinder privacy maturity

Cyber-security and privacy are not the main focus of accounting standards and financial reporting which enable investors and creditors to more accurately understand how organisations are performing, and to make better decisions regarding those organisations. Whilst accountants do not deal with concepts like Internet protocols and zero-days, they do have their own technical language and formalized processes to create and alter rules for how organisations' accounts are prepared and disclosed. Unlike hackers, accountants operate on periodic time cycles, focusing on concepts like assets, liabilities, expenses, revenue and capital, so it is appropriate to explore how the problems identified in the previous section have been influenced by the way accountants think about some of those concepts.

Assets: Intangible assets (such as software licences) have become critically important to increasing the productivity and value of organisations.[3] For much of the Information Age, accounting standards made a distinction between whether different types of intangible assets could be recognised on the balance sheet of an organisation. Whilst intangible assets that were purchased from third parties could be recognised as an asset, internally-developed intangible assets could not. Only recently have internally generated intangible assets been recognised on the balance sheet.[4]

One of the interesting consequences of this accounting decision is its impact on data mining, cyber security and privacy. For example, when companies that took advantage of Big Data analytics listed on the stock exchange, they did not have to inform their investors or lenders about the size or value of the datasets of personal information which they were holding. A gap thus widened between the book value of their assets and their total market capitalization (accountants refer to this broader issue as the "asset-light" problem). Those organisations could build massive internal datasets containing billions of records and inferences about tens of millions of people, but not have to list those datasets as assets on their balance sheet.

Information that is hidden from disclosure in financial reports affects not just the decision-making of external parties like investors and lenders. It also influences the decision-making of internal parties within organisations, notably their boards and executives. Their decisions about the necessary maturity of data governance programs, and appropriate investments into cyber security and privacy controls are affected.

Without the pressure of adequate transparency required by financial reporting rules, organisations have a natural tendency to under-invest in their cyber security and privacy maturity, often preferring to deliver a mix of greater profits to their owners and greater bonuses to their leadership.[5] The expenses necessary to achieve that maturity uplift are certain to lower bottom-line profits (and potentially bonuses) in the short term, whilst the benefits of increased cyber security and privacy maturity are less certain and longer-term (if an organisation is not the victim of a successful cyber-attack or data breach, was that because of the adequacy of its existing controls? or because it was not targeted that year?).

Whilst the challenges in valuing intangible assets like data lakes of personal information and inferences generated from data analytics has been used as a justification by some organisations to not report those assets on their balance sheets[6], there is a situation in which such datasets have come to be routinely valued. When organisations

enter bankruptcy in the US, customer datasets are valued and sold as valuable assets to third parties (typically operating in a similar line of business) to help pay off outstanding creditors of that organisation. The American Bankruptcy Code and bankruptcy courts have even utilised the role of a "consumer privacy ombudsman" who expertly assesses whether the proposed sale might create excessive privacy harms.[7]

Liabilities: Beyond the asset side of the balance sheet, another issue that exacerbates the lack of disclosure in financial reports about high-risk datasets containing large volumes of personal information is the way in which accountants interpret some liabilities as either provisions (which are reported and affect bottom line profits) or contingent liabilities (which are disclosed, but which do not affect bottom line profits).[8]

For example, organisations currently only report as provisions in their balance sheets direct costs expected to be incurred because of data breaches that have already occurred (financial reports are backwards-looking in time).[9] The costs of compensating potential litigation by victims of data breaches might be disclosed as a contingent liability, but do not affect profitability during the time period in which the data breach occurred. The much larger indirect costs typically incurred by organisations after a data breach (such as reputation loss, distracted executives, reduced future sales, etc.) are not typically reported or disclosed at the time of a data breach, except perhaps as expenses affecting their future profits which may or may not be linked by the organisation to the data breach.[10]

Reporting time cycles: The annual cycle and historical focus of financial reporting under accounting standards may also contribute to under-investment in cyber security and privacy controls.[11] Hackers tend to be unpredictable, and the time taken to detect and respond to a data breach is often lengthy. This means that many data breaches straddle across financial reporting periods (i.e. the hackers penetrated the organisation's systems during one accounting period, detection occurred in the next financial period and the consequences of the breach (particularly indirect costs) will continue to affect the organisation over the next several accounting periods). Therefore, any one financial report will only contain a partial view of the overall data breach and its consequences – profits may be over-stated in one financial report because costs will be incurred in subsequent years. Inherent uncertainties in data breach consequences intersect with limitations on how organisations can report provisions and disclose contingent liabilities, making it harder for investors and lenders to get an accurate understanding of how well the organisation is adequately investing to control its cyber security and privacy risks.[12]

Materiality: Underlying analysis of both assets and liabilities (and revenue/expenses) is the accounting concept of materiality.[13] It acts as a high-pass filter, enabling an organisation to ignore (for financial reporting purposes) amounts considered to be too small relative to the size of the organisation. Until recently in Australia, many more organisations than you might expect could regard a data breach as being more likely to be immaterial than material. This was due to the Privacy Act 1988 excluding from compliance most businesses with less than $3 million in annual turnover (the small business exemption), the low level of penalties and enforcement under that Act, and the limited means for victims of data breaches to seek a remedy. However, organisations will need to reassess the extent to which they regard an interference with privacy as material from an accounting perspective due to:

- the recent amendments to the Privacy Act which significantly increase penalties for interferences with privacy; and
- the Attorney-General's Department's recommendations to remove the small business exemption and introduce both a direct right of action and statutory tort.

This includes interferences with privacy beyond data breaches.

Opportunities to influence new accounting standards

Both Australian and international accounting standards bodies are in the early stages of a lengthy process to consider how cyber security and privacy risks affect the information communicated to investors and lenders through financial reports (falling within the accounting concept of sustainability).[14] This provides an opportunity for Australia's cyber security and privacy expert communities to help influence and shape the extent to which another regulatory regime motivates organisations to uplift their cyber security and privacy postures.

Unlike the reactive nature of the notifiable data breaches scheme and increased penalty provisions under the Privacy Act, one advantage of financial reporting obligations and accounting standards is that they can proactively influence organisational behaviour (i.e. organisations have to prepare and publish annual financial reports, regardless of whether or not they have experienced a data breach that year). This means that increased cyber security and privacy reporting obligations imposed by accounting standards have the potential to apply consistent prospective pressure on organisations to uplift their cyber security and privacy maturities systematically, rather than the sporadic pressures imposed when organisations are recovering from a data breach.

Just as cyber security and privacy experts benefit from the help of accountants when preparing their tax returns, accountants are likely to benefit from the insights of cyber security and privacy experts when developing and revising accounting standards relevant to cyber security and privacy.

1. The first challenge in achieving the benefits possible from such a collaboration is for both groups of experts to better understand each other's concepts and jargon.
2. The second is to gain the capability to successfully navigate each other's institutional processes.
3. Patience is the third challenge – new accounting standards are not developed overnight. Indeed, they may take five to ten years – which is several generations of risk evolution in cyber security terms.

Sustained effective engagement with the development of accounting standards relevant to cyber security and privacy will likely require the involvement of and support from both industry bodies and government agencies. Failure to engage

effectively may result in the development of accounting standards and financial reporting requirements in Australia and internationally which undermines incentives for organisations to invest in uplifting their cyber security and privacy maturities.

Conclusion

Experiences with cyber-attacks and privacy breaches over the last decade have highlighted the dual-nature of data, capable of simultaneously fueling the Information Age and causing significant harm when mis-used or leaked. As under-investment by organisations in uplifting their cyber security and privacy maturity persists despite implementation of many reactive regulatory regimes, changes to accounting standards might reduce the extent to which data continues to leak from organisations as a form of toxic waste.

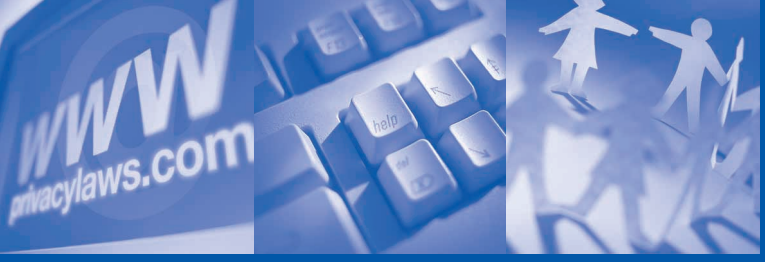
There is also an opportunity for Australia's cyber security and privacy expert communities to begin a conversation with accounting standards bodies to assist them to craft new accounting standards which may drive organisations to make more adequate investments into uplifting their cyber security and privacy maturity.

AUTHOR

Dr John Selby is a Principal Consultant and Head of Research at Privcore, Australia www.privcore.com.
Email: selby@privcore.com

REFERENCES

1 Cory Doctorow, 'Personal Data is as Hot as Nuclear Waste' *the Guardian* (16 January 2008).
2 The audit offices of Commonwealth and state governments have repeatedly lamented the inability of agencies to fully implement even the ASD's "Essential Eight" controls. For analysis of the private sector's incentives to under-invest in adequate controls, see: Lawrence Gordon, et al, 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms' (2018) 9 *Journal of Information Security* 133-153.
3 Australian Accounting Standards Board, Australian Accounting Standard AASB138 Intangible Assets.
4 Not all accountants agree with this change: see, for example, Stephen Penman, Accounting for Intangible Assets: Thinking It Through (2023) *Australian Accounting Review*, vol. 33, issue 1, 5-13.
5 Lawrence Gordon, et al 'Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms' (2018) 9 J*ournal of Information Security* 133.
6 Laura Veldkamp, 'Valuing Data as an Asset' (2023) Review of Finance 1-18; Jurgen Sidgman and Malcolm Crompton, 'Valuing Personal Information to Foster Privacy: A Thought Experiment and Opportunities for Research' (2016) 30(2) *Journal of Information Systems* 169-181.
7 Michael Brandess and Kathryn Nadro, 'Getting Personal: Acquiring PII out of Bankruptcy' (2022) 41 *American Bankruptcy Institute Journal* 14.
8 Australian Accounting Standards Board, AASB Standard 137: Provisions, Contingent Liabilities and Contingent Assets; Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021).
9 See, for example, how Medibank Private disclosed provisions for direct costs arising out of its 2022 data breach in its financial reports.
10 Marty Puranik, 'What is the Cost of a Data Breach?' *Forbes* (2 December 2019).
11 Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021).
12 Australian Auditing and Assurance Standards Board, Staff Paper: The Consideration of Cyber Security Risks in an Audit of a Financial Report (May 2021).
13 Australian Accounting Standards Board, Practice Statement: Making Materiality Judgements (December 2021).
14 Australian Accounting Standards Board, Staff Paper: Project: Sustainability Reporting GSSB Draft Work Program 2023-2025 (23 January 2023), paragraphs 13-15; IFRS, Staff Paper: Management Commentary Risks (May 2020).



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU AI Act: Will there be Brussels effects?

The EU aims to establish a world-class AI hub. Will companies and legislators globally follow its regulatory lead? Independent scholar **Graham Greenleaf** assesses the situation.

The expression "the Brussels effect" is often used rather loosely to refer to any or all of the ways by which EU legislative standards come to be adopted in the practices of companies (or governments) in countries outside the EU ("third party countries"). These include both those required by law (*de jure*) and those adopted for other reasons (*de facto*), distinctions sometimes recognised.[1]

Continued on p.3

Germany debates changes to its federal data protection law

Julia Garbaciok and **Katharina Weimer** of Fieldfisher assess the upcoming changes to the German Federal Data Protection Act and their current status.

As data protection enforcement is spread across 18 different authorities in Germany, there have been calls for many years for simplification and harmonization regarding the application of the General Data Protection Regulation's (GDPR) requirements, especially to ensure a more innovation-friendly regime. According to a survey conducted by the digital industry association Bitkom[1], 65% of companies see the

Continued on p.7

Issue 190 **AUGUST 2024**

INTERNATIONAL report

ISSUE NO 190 AUGUST 2024

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Julia Garbaciok and Katharina Weimer
Fieldfisher, Germany

Paul Maynard and Madelaine Harrington
Covington, UK

Dr John Selby
Privcore, Australia

Asher Dresner
PL&B Correspondent

Poojan Bulani
University College London, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Enforcement phase begins for EU digital laws

For some years, we have seen much GDPR enforcement both at the national and EU level, although some countries are more active than others. The EU's new digital package means that there are now a multitude of digital laws to enforce, and ensure that they operate in the intended way with the GDPR which is the underlying regulation.

Recently, there have been interesting developments in this field. The ever-so-active noyb made complaints about Meta's AI training practices to 11 DPAs whose intervention put a stop to Meta's plans for now (p.12), and the EU Commission is looking into applying the Digital Markets Act in the area of pay or consent (p.22).

Civil society is playing an increasingly important role – consumer organisations have also challenged Meta over Pay or Consent (p.29). EDRi's action on LinkedIn's targeting of adverts based on sensitive personal data has already been successful (p.29).

In May, the European Commission decided to open infringement procedures by sending a letter of formal notice to 18 Member States that did not designate the responsible authorities to implement the Data Governance Act which facilitates data sharing across sectors and EU countries. Authorities also need to be appointed in Member States, in quite a short timescale, to become responsible for AI as per the EU AI Act. In some countries, the existing data protection supervisors may become AI authorities but this is not necessarily the case everywhere (p.18).

The EU AI Act was published in the EU Official Journal on 12 July 2024 and will be in force from 1 August. Most of its provisions will become applicable from 2 August 2026. This world-first Act may influence AI governance globally in many different ways – read analysis by Graham Greenleaf on p.1.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 180+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 180+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access *PL&B* events documentation, except for the Annual International Conferences in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

9. Free place at a *PL&B* event
A free place at a *PL&B* organised event when booked at least 10 days in advance. Excludes the Annual Conference. More than one free place with Multiple and Enterprise subscriptions.

privacylaws.com/reports

> *PL&B* reports are an invaluable resource to anyone working in the data privacy, e-commerce or digital marketing fields. Unlike many news feeds or updater services, each report provides rare depth of commentary and insight into the latest developments.
>
> **Rafi Azim-Khan, Partner – Head of Digital Law, Crowell & Moring**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the UK GDPR and related regulatory changes, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.