# NEW TECHNOLOGY, PERSONAL DATA PROTECTION AND IMPLICATIONS

## *for financial services regulation*

CAMILLE BLACKBURN, Director and Advisor, Regulation and Financial Systems

*Information, Communication and Technology (ICT) developments present a challenge to public expectations about the collection, use, control and cross-border transmission of personal data, including financial data. This paper considers the data protection laws in Australia, and in Europe, which has the most comprehensive personal data protection laws globally. It also examines the impact of different regulatory approaches to data protection for three areas of technology-driven financial sector innovation.*

Though policy settings are not yet stable or consistent globally, substantial regulatory activity continues in the field of data protection.[1] Most data protection regimes globally, including Australia's, have two major policy drivers:

- *human rights:* to protect the fundamental rights and freedoms of natural persons and, in particular, the right to privacy with respect to the processing of personal data
- *economic:* not to restrict the free flow of personal data between states for reasons connected with human rights to personal data protection.

A global approach to these policy considerations is hampered by an absence of consensus on the benefits and potential harms arising from ICT innovation and, consequently, the useful role for regulation. Private sector responses or 'privacy-enhancing innovation' also contribute to uncertainty about the need for regulation.

### Personal data protection in Europe and Australia

Australia's personal data protection regime is contained in the *Privacy Act 1988* (Cth) ('Privacy Act') that mandates 13 Australian Privacy Principles (APPs). While the Office of the Information Commissioner provides administrative interpretation of the law, Australian privacy and data protection concepts do not have much depth of jurisprudence arising from the application of the statute or common law concepts.

The Australian position also contrasts with the deep human rights jurisprudence that supports the EU data protection architecture. Personal data protection is recognised as a fundamental right in EU member states under the *Charter of Fundamental Rights* ('European Charter'), although the exact content of the new additional protection afforded by a human right to personal data protection over the established right to privacy is still an open question.[2] Public policy debate in Europe is also fanned by the imminent replacement of the existing EU *Data Protection Directive* ('Directive') with the more expansive *General Data Protection Regulation* ('Regulation'). Data protection issues have media prominence and feature regularly in public policy forums.

## Digital innovation in financial services

Technology-driven innovation is transformative for the financial services sector, which revolves around recording, analysing and interpreting transactions, and managing associated information flows. With no physical products to manage, these processes readily lend themselves to improvement through the application of digital technologies.[3]

In this paper we discuss three categories of innovation: big data and profiling; cloud, and trans border data flows; and data portability, robo advice and credit provision.

## Big data and profiling

Many financial services firms have always had access to big data. Their business depends on access to personal identity and financial data about customers.

Much of that information arises from service provision itself. Other information is solicited to meet legislative requirements for risk assessment or to tailor product offerings. International standards require all customers to provide details about their identity prior to services being provided. Clients seeking credit need to provide information to inform credit assessments. Advisors require information about personal circumstances and needs in order to provide a reasonable basis for advice. Legislation increasingly requires information to inform tax authorities and international market trading obligations.

In addition to these data sets, an explosion of sensors, smart devices and social collaboration technologies is supplementing data from traditional sources. Additional data is also being collected by centralised bodies: international clearing houses for financial market trading, central credit reporting databases, and new payment platforms overseen by central banks are a few examples of this.[4] National governments are encouraging these trends with open data policies and academic institutions are increasingly publishing useable data.[5] Data generated by all sources is also increasingly connected.

For financial services firms, the benefits of big data make it a commercial imperative. Studies point to enhanced algorithmic and market research capabilities, better risk management and regulatory reporting benefits, increased customer loyalty from better anticipation of customer needs and other forms of data monetisation. The benefits to customers are also self-evident — less friction in product and service choice because of more targeted product offerings and, often, lower cost.

However, the proliferation and use of data cause a general sense of unease increasingly being described as a loss of 'informational self-determination' — a lack of control of how one presents oneself to others. The retention of information alone is sufficient to give rise to these concerns — the German Constitutional Court has referred to a 'diffusely threatening feeling of being watched'.

*Big data challenges privacy because it facilitates the processing of aggregated information, or depersonalised ('pseudonymous') information and matching with other information, enabling personal attributes to be derived. Most data protection laws use a concept of 'personal' data or information as the threshold for substantive protections. That concept is increasingly challenged by the fact that general data can be personalised without the data subject's knowledge or consent.*

At a more granular level, there are two more micro sets of policy concerns: privacy and discrimination.[6]

Big data challenges privacy because it facilitates the processing of aggregated information, or depersonalised ('pseudonymous') information and matching with other information, enabling personal attributes to be derived. Most data protection laws use a concept of 'personal' data or information as the threshold for substantive protections. That concept is increasingly challenged by the fact that general data can be personalised without the data subject's knowledge or consent.

The Australian and European regimes have approached this issue differently. Both regimes use the concept of 'personal information' (Australia) and 'personal data' (EU) as a definitional threshold for the protections they provide. However, in addition the European regime defines their term more widely and specifies threshold grounds for use of personal data. The most common ground is:

> (a) the data subject has unambiguously given his consent …
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[7]

Where consent is not obtained, the interests of the data controller and data subject need to be weighed against each another. For example, creation of pre-built profiles on non-social network sites though the aggregation of data independently contributed by social network users lacks a legal basis and is not permitted.

*Profiling and matching also give rise to important policy issues regarding discrimination and adverse selection. For the financial sector that can be particularly harmful where those analytics are embedded in online or automated decision tools not transparent to the data subject.*

The Australian regime does not have a legal grounds concept limiting personal data use.

Profiling and matching also give rise to important policy issues regarding discrimination and adverse selection. For the financial sector that can be particularly harmful where those analytics are embedded in online or automated decision tools not transparent to the data subject.

Increasing accuracy in analytics reduces the market for financial products that pool risks across a group or society. Risk pooling operates so that in an uncertain future the more fortunate underwrite the misadventure of the less fortunate. Accurate predictive analytics decrease the size of the 'uncertain future'. Persons with attributes that suggest an unacceptably high probability of future risk are either priced out of the market or not offered financial products at all.

This policy concern of adverse selection was first recognised for genetic information. In Europe restrictions prohibit the use of genetic information in insurance assessments.[8] In Australia the Privacy Act applies to genetic information collected by insurers and a comprehensive report in 2003 into genetic practices recommended strengthening of industry practice in this regard.[9] While some steps have been taken, the issue is still the subject of industry guidance rather than tailored legislative protection for individuals.[10]

A recent report commissioned by the UK government into the commercial use of personal information has also considered adverse selection for motor vehicle insurance.[11] It notes the increasing use of big data in assessment of risk, including a rising incidence of 'black box' insurance policies requiring installation of telematics in a person's car to monitor driver behaviour. Other information such as a good credit rating might also be used as a proxy in risk assessments for evidence of responsible behaviour.[12]

It is well-recognised in Europe that big data and automated decision making present a new frontier for policy. Article 15 of the Directive provides a right not to be subject to a decision based on automated processing: such a decision is defined as 'a measure that produces legal effects concerning this natural person or significantly affects this natural person'. This right allows a data subject to require human intervention in any significant decision that affects them. Proposed Article 20 of the Regulation extends these protections.[13]

None of these issues is explicitly addressed in Australia's regulatory settings.

## Cloud and trans-border data flows (TBDFs)

Since the 1990s there has been broad acceptance that free flow of data was crucial to international integration of trade and commerce. What may not have been anticipated was the speed and level of disaggregation of financial service value chains. Offshore data processing is reliant upon data being provided to facilitate the activity — a trans-border data flow (TBDF).

The movement of data internationally provides complexity for policy formulation. It introduces the risks of:

> avoidance of tight data protection requirements (particularly in Europe)

> enforcement difficulties in foreign jurisdictions

> protecting home citizens against inadequate data protection or intrusive government surveillance practices.

Cloud computing highlights these issues although they arise for any internationally outsourced financial service function, and particularly where the financial product or service is dependent on distributed ledger innovations.

In financial services, there are significant efficiency benefits that result from reliance on cloud services. By using cloud, Australia's largest bank has reduced its storage, application testing, and development costs by 50 per cent. Previously, 75 per cent of the bank's IT expenditure was on infrastructure but cloud usage has reduced this to 26 per cent.[14] While the Australian Prudential Regulation Authority has issued some guidance on risks, there is no detailed guidance on the level of regulatory tolerance of the use of cloud services by the financial services sector.[15]

In Australia APP 8 allows disclosure of personal information to a recipient outside Australia if the entity 'reasonably believes the overseas recipient is subject to a law or binding scheme that, overall, is at least substantially similar to the way in which the APPs protect the information' and enforcement mechanisms in place. The provisions do not apply where the data stays within the same entity globally.

To facilitate the forming of a reasonable belief with regard to data flows within Asia, Australia agreed to the APEC Cross-Border Privacy Rules (CBPRs). If adopted in an entity's privacy policy, the CPBRs facilitate the free flow of information inside a corporate group within Asia as well as to other entities that meet those standards.

EU authorities have some doubts over the adequacy of the CBPR framework itself and that prevents free flow of personal data from EU member states into Australia. New Zealand has made the necessary adjustments and was recognised as adequate in December 2013.[16]

Legitimate questions have been raised about effective enforcement of rules relating to TBDF where cloud technologies provide a dynamic jurisdictional environment not transparent to the user (or regulator). That concern is one reason for the rise of regional clouds, as in Europe, such that information within the cloud could be passed from service provider to service provider without concern for the legality of that TBDF within the EU.

## Data portability, robo advice and credit provision

In the EU, the draft Data Protection Regulation introduces a right to data portability ('RDP') giving a data subject the right to obtain (in a suitable format) and transfer data from one electronic processing system to another.

The proposed new right has its policy foundation in competition law. Lack of data portability has long been recognised as a potential switching cost, and a friction in the free operation of competitive forces.[17] The proposed right has large implications for emerging business models in financial services.

Robo advice is the provision of advice about financial products generated by algorithms that match potential investors with products that suit the investor's financial attributes and needs.[18] Online tools matching the investor to appropriate financial products may ultimately result in disintermediation of the human financial advisor.[19] Initial steps toward this future state already exist in most countries.

In the UK, lack of mobility in switching between deposit accounts has been identified an impediment to competition in retail banking.[20] A Current Account Switching Service (CASS) was introduced that required banks to provide details of the customer's services in a standard format to facilitate the switching of services to new providers in less than seven days. A recent review of the scheme has noted its limited success.[21] Another option mooted to facilitate bank account switching — Bank Account Number Portability (allowing the customer to 'own' their bank account number when switching akin to mobile number portability) — is considered too expensive and the Midata initiative (discussed below) may supersede CASS.

Lenders that refuse to extend credit to a small or medium-sized business are now subject to obligations that promote data mobility. The *Small and Medium Sized Business (Finance Platforms) Regulation 2015* requires lenders to share standardised data attributes of SMEs and their financing needs which can then be assessed by alternative lenders.

More broadly the UK 'Midata' initiative is a public/private program in the UK working toward standardising how personal information held by service providers can be provided to data subjects in machine readable form to allow greater consumer mobility, including for financial services. The US equivalent program is 'Smart Disclosure'.

These international developments have been noted and the Australian Government is considering the recommendation of the 2014 Financial System Inquiry to consider 'how financial product information is reported so third parties could use automated processes to create market wide datasets of available products … supporting consumers in making more informed online choices and enhancing competition'.[22]

## Implications for Australian financial services

Australian financial services flows are predominantly to and from Europe and the US.[23] While the Asian region is Australia's most significant trading partner for physical goods, financial flows do not mirror that. A discrepancy between data protection standards of Australia and Europe will cause increasing friction for the provision and receipt of financial services with Europe.

The significance of that discrepancy is yet to result in serious regulatory impositions or disciplinary action for Australian financial service providers. There are indications, however, that personal data protection is rapidly increasing as a regulatory focus. In the EU, the proposed Data Protection Regulation includes stronger sanctions, with data protection agencies able to impose fines of up to 1 million euro or 2 per cent of an enterprise's annual global turnover for personal data breaches — including for transferring data to prohibited jurisdictions where protections are not equivalent. There are also strengthened requirements to notify Data Protection Agencies and data subjects of personal data breaches.

*Australian financial services flows are predominantly to and from Europe and the US. While the Asian region is Australia's most significant trading partner for physical goods, financial flows do not mirror that. A discrepancy between data protection standards of Australia and Europe will cause increasing friction for the provision and receipt of financial services with Europe.*

Higher standards may also be 'imported' to Australia through international trade negotiations. Traditionally issues relating to personal data have been outside the scope of trade negotiations under the GATT and GATS frameworks, because of a carve-out from the scope of those treaties of measures 'to protect personal data, personal privacy and the confidentiality of individual records and accounts'.[24] However, a number of the largest bilateral treaties currently being negotiated include '21st century issues' ensuring the appropriate balance between the free flow of information and the right of governments to regulate data flows, and between protecting personal data and permitting access to that data for enforcement purposes.[25]

Other developments that may affect the regulatory landscape are private sector responses to policy concerns. Some of those innovations (briefly) include:

- *UK G-Cloud initiative:* an initiative to streamline procurement of cloud services by the public service by pre-approving procurement and making details public. This is intended to reduce due diligence costs across the economy for the private sector by providing confidence that the service provider meets UK government's criteria, including for personal data protection.
- *Personal privacy vaults and personal data services:* services available in Europe and the US that store an individual's personal data, and encrypt search history and so-called rich personal data (such as location, age or other info mined by website cookies) in a personal cloud inaccessible to data brokers. Services are emerging where one can allow particular companies access to particular data about oneself in exchange for monetary compensation — a 'sharing the wealth' strategy.
- *Information markets:* markets where personal information such as mobile phone information giving location information can be offered for a price.

*In Australia we can learn from the depth of public policy thinking that has occurred and continues in Europe. The solutions that have been reached in Europe will not necessarily suit our circumstances but will provide a useful reference point to better articulate the benefits and costs in data protection. Our approaches are lagging or intentionally diverging from Europe and cross-border economic consequences may well follow.*

Commercial incentives to increase data collection, mining, aggregation, profiling and analytics mean that policy settings for personal data protection will need to be considered by independent policy thinkers including academics, the courts and the public service.

In Australia we can learn from the depth of public policy thinking that has occurred and continues in Europe. The solutions that have been reached in Europe will not necessarily suit our circumstances but will provide a useful reference point to better articulate the benefits and costs in data protection. Our approaches are lagging or intentionally diverging from Europe and cross-border economic consequences may well follow.

## Notes

1. For an overview see Graham Greenleaf 2014, 'Scheherezade and the 101 data privacy laws: Origins, significance and global trajectories', *Journal of Law, Information and Science* 23, no. 1.
2. Orla Lynskey 2014, 'Deconstructing data protection: The added-value of a right to data protection in the EU legal order', *International and Comparative Law Quarterly 63*, no. 03, July, pp. 569–97.
3. Commonwealth of Australia 2014, *Financial System Inquiry 2014, Final Report*, November, p. 143.
4. Reserve Bank of Australia 2014, speech by Tony Richards, Head of Payments Policy, 'The path to innovation in payments infrastructure in Australia', Chicago Payments Symposium, September.
5. Timothy Glyn Davies 2014, 'Open data policies and practice: An international comparison'.
6. IS Rubinstein 2013, 'Big data: The end of privacy or a new beginning?', *International Data Privacy Law* 3, no. 2, May, pp. 74–87.
7. Article 7 Directive 95/46/EC.
8. The Council of Europe's Convention on Human Rights and Biomedicine Article 11 states that discrimination against a person on grounds of his or her genetic heritage is prohibited.
9. Australia and National Health and Medical Research Council (Australia) 2003, 'Essentially yours: The protection of human genetic information in Australia', *Australian Law Reform Commission Report*, no. 96.
10. Human Genetics Society of Australasia 2013, *Position statement: Genetic testing and life insurance in Australia*.
11. Competition and Markets Authority 2015, *The Commercial Use of Data, A Research Report for the CMA*.
12. Ibid., p. 51.
13. Rubinstein, op. cit., p. 79.
14. Commonwealth of Australia 2014, *Financial System Inquiry 2014, Interim Report*, November, p. 4–57.

15. Australian Prudential Regulatory Authority 2010, *Letter to Industry — Outsourcing and Offshoring: Specific considerations when using cloud computing services*.

16. 2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557).

17. P Klemperer 1995, 'Competition when consumers have switching costs: An overview with applications to industrial organization, macroeconomics and international trade', *The Review of Economic Studies 62*, no. 4, October, pp. 515–39.

18. US Securities and Exchange Commission 2015, *Investor Alert: Automated Investment Tools*.

19. Peter Arnold 2015, *A new form of financial advice*, Morningstar.

20. Competition and Markets Authority 2014, *Personal Current Accounts — Market Study Update*.

21. Financial Conduct Authority 2015, *Making Current Account Switching Easier: The Effectiveness of the Current Account Switch Service*.

22. Commonwealth of Australia, note 14, p. 188–89.

23. Commonwealth of Australia, note 14, see Figure 1.3 showing financial and physical outward flows and Chapter 10 'International Integration'.

24. Article XIV(c) GATS and Understanding on Commitment in Financial Services, para. 8.

25. FAS Project on Government Secrecy 2014, *Transatlantic trade and investment partnership (TTIP) negotiations*.