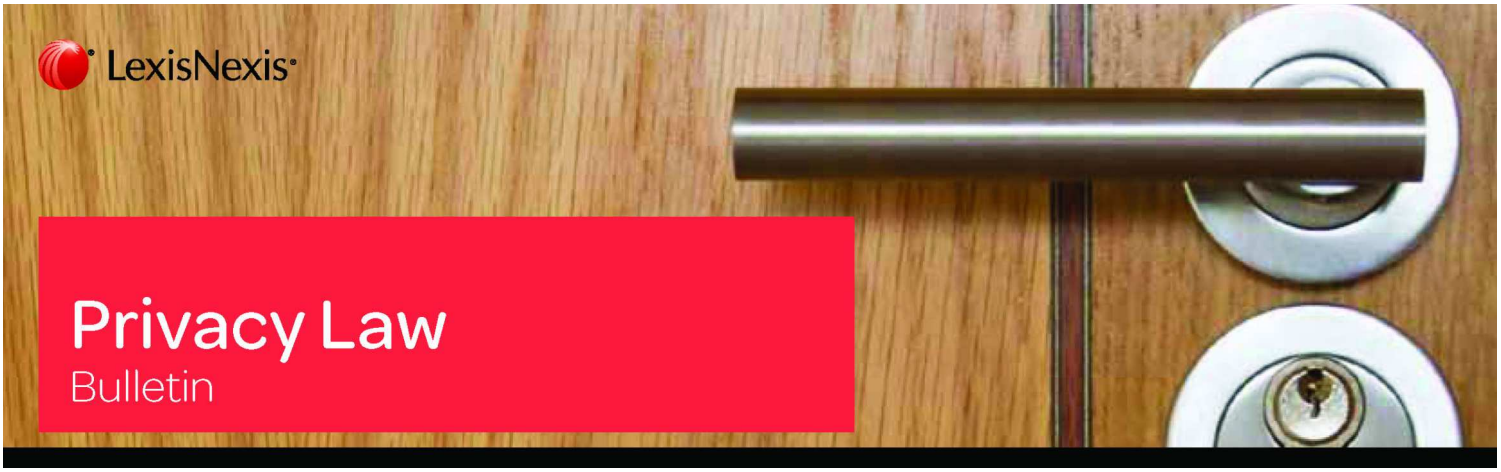

Privacy Law Bulletin

2020 . Vol 16 No 9

Contents

Information contained in this newsletter is current as at March 2020

LexisNexis Butterworths

Privacy Law
Bulletin

Paradise, privilege and the High Court of Australia: the ATO and accessing corporate confidential information

***Robert Wyld**, **Angus Hannam** and **Macsen Nunn** JOHNSON WINTER & SLATTERY*

Introduction

In *Glencore International AG v Commissioner of Taxation*[1] (*Glencore International*), the High Court of Australia unanimously affirmed the status of legal professional privilege (LPP) as merely an immunity from the exercise of compulsory statutory powers. The court held that LPP is not an actionable right founding an independent cause of action capable of restraining third parties from using privileged communications in their possession. LPP very much remains a shield against prying eyes, not a sword to wield independently against those who would use privileged communications against the privilege holder.

Key points/how does it affect you?

- The High Court of Australia has continued to restrict the use of LPP to an immunity from compulsory procedures.
- Equitable relief for breach of confidence remains undisturbed, assuming the communications remain confidential.
- This decision underscores the importance of cybersecurity and data protection in a digital age for clients and law firms to protect against the risks of unauthorised disclosures and loss of confidential (and privileged) communications.
- Companies should seek advice as to the best methods of communication with legal practitioners and the process for claiming LPP.

Background

In October 2014, the plaintiff, Glencore International AG (Glencore), engaged a law and services provider practice in Bermuda (Appleby) through its Sydney-based solicitors to provide legal advice on a group-wide restructure called "Project Everest".

In November 2017, over 1 terabyte of data, colloquially known as the "Paradise Papers", was hacked from Appleby by a third party, handed over to the International Consortium of Investigative Journalists, and published worldwide. The Australian Taxation Office (ATO) came into possession of the Project Everest papers without Glencore's consent and intended to use them in a tax audit of Glencore and the corporate group more generally. Glencore continued to assert LPP over the Project Everest communications, requesting that they not be relied upon by the ATO and that they be returned. The ATO repeatedly declined to agree to Glencore's demands. The ATO took the position that it was entitled to make an assessment of a taxpayer's taxable income from the taxpayer's returns "and from any other information in the Commissioner's possession".[2]

The issue before the High Court was whether LPP extended to a positive right, that is, an independent cause of action capable of being enforced, to restrain the ATO from using the documents. Traditionally, LPP could be relied upon only as a means of blocking the compulsory production of such documents, but in this case the court considered whether the privilege could be used as a "sword" rather than a "shield".

Glencore did not seek relief in equity for breach of confidence. The court did not rule upon whether the documents remained confidential, notwithstanding their public dissemination, and notwithstanding that Glencore was an innocent victim and did not consent to, or participate in, their disclosure. Another avenue for relief, as the court noted, might have been to seek to expand the tort of unjustified invasion of privacy. However, Glencore relied only on LPP as a basis for relief.

Glencore's submissions

Glencore's primary submissions were as follows:

- LPP is a fundamental common law right.
- The High Court in *Daniels Corp International Pty Ltd v Australian Competition and Consumer Commission (ACCC)* (*Daniels Corp*) did not intend to

confine the scope of LPP when it stated that "[i]t is an important common law right or, perhaps, more accurately, an important common law *immunity*" (emphasis added).[3]

- The English decision of *Lord Ashburton v Pape*,[4] which has been followed in Australia, would leave a significant gap in the law if it was understood to have held that an injunction will be granted on the basis that documents are confidential rather than privileged.
- As a result of the above, the court should find that LPP is an independent actionable right that may restrain the use of, and aid in the recovery of, privileged documents. This would bring the scope of LPP more into line with the policy on which it is based.

High Court's reasoning

The court strongly and unanimously determined that the argument that LPP constitutes an independent legal right which is capable of being enforced was fundamentally wrong. Although LPP has been described as a right which is founded upon a matter of public interest (as opposed to, for instance, a mere rule of procedure or evidence), the court found that this "right" was a right to "decline to disclose or to allow to be disclosed the confidential communication or document in question", "a right to resist the compulsory disclosure of information", or "a freedom from the exercise of legal power or control".[5] It found that *Daniels Corp* should correctly be interpreted as confining the scope of LPP to that of an immunity. There was nothing tentative in the court's characterisation of the privilege as an immunity provided by the common law.

With respect to *Lord Ashburton v Pape*, the High Court was clear that on the present state of the law, once privileged communications have been disclosed, resort must be had to equity for protection respecting the use of that material. The juridical basis for relief in equity is confidentiality.

The High Court rejected Glencore's arguments that the public interest would be advanced by making LPP an actionable right and the common law should therefore reflect that underlying public interest. Rather, the High Court was trenchant in stating that the common law develops by applying settled principles to new circumstances or reasoning from settled principles to new conclusions. The court noted that "[p]olicy considerations cannot justify an abrupt change which abrogates principle in favour of a result seen to be desirable in a particular case".[6]

The High Court considered authorities from the United Kingdom and Singapore where appellate courts had, so Glencore argued, restrained the use of documents obtained without consent other than based upon a breach of confidence. The High Court rejected those arguments, making it clear that:

> … it is necessary for an equity to arise that the person to be restrained must have an obligation of conscience, but the basis for an injunction is the need to protect the confidentiality of the privileged document.[7]

Conclusion and practical implications

The significance of this case lies in the continued restriction of LPP to use as an immunity from compulsory procedures. Equity may assist a plaintiff in restraining breaches of confidentiality by third parties, but often affords no protection in circumstances where documents have lost their confidential nature. LPP cannot be relied upon as a basis to restrain the use of leaked communications.

The case provides a timely reminder of the importance of cybersecurity and data protection for both corporate clients and law firms in a digital age, as well as the risks that can arise when confidential communications are hacked or accessed by third parties and publicised. In Australia, as the ATO has a statutory right to make assessments based upon documents or information in its "possession", accessing such material from the Paradise Papers is a potential rich windfall to the ATO and a probable source of a headache for affected taxpayers who will likely face increased scrutiny or even a formal audit and tax assessment in light of such disclosures. Clients and lawyers should consider their own computer software and hardware vulnerabilities to minimise the unauthorised disclosure of confidential and privileged data.

Robert Wyld
Consultant
Johnson Winter & Slattery
Robert.Wyld@jws.com.au
https://jws.com.au/en

Angus Hannam
Associate
Johnson Winter & Slattery
Angus.Hannam@jws.com.au
https://jws.com.au/en

Macsen Nunn
Graduate
Johnson Winter & Slattery
Macsen.Nunn@jws.com.au
https://jws.com.au/en

Footnotes

1. *Glencore International AG v Commissioner of Taxation* (2019) 372 ALR 126; [2019] HCA 26; BC201907072.
2. Income Tax Assessment Act 1936 (Cth), s 166.
3. *Daniels Corp International Pty Ltd v Australian Competition and Consumer Commission (ACCC)* (2002) 213 CLR 543; 192 ALR 561; [2002] HCA 49; BC200206568 at [11].
4. *Lord Ashburton v Pape* [1913] 2 Ch 469.
5. Above n 1, at [22].
6. Above n 1, at [41].
7. Above n 1, at [37]–[39].

New privacy permissions in response to the 2019/20 bushfire emergency

Dr Ashley Tsacalos *and* ***Monique Azzopardi*** *CLAYTON UTZ*

In response to the recent Australian bushfires, on 20 January 2020, the Attorney-General made the Privacy (Australian Bushfires Disaster) Emergency Declaration (No 1) 2020 (Declaration). The Declaration was made under s 80J of the Privacy Act 1988 (Cth).

What does the Declaration achieve?

The Declaration declares "Bushfires in Australia resulting in death, injury and/or property damage occurring from August 2019 into 2020" to be a "disaster" for the purposes of s 80J of the Privacy Act.

Subject to meeting the conditions set out below, the Declaration allows Commonwealth agencies and certain private sector entities subject to the Privacy Act to collect, use or disclose personal information in circumstances otherwise not permitted by the Privacy Act.

The following conditions must be satisfied before any collection, use or disclosure of personal information is made:

- the entity must have a reasonable belief that the individual concerned is involved in the bushfire emergency and
- the proposed collection, use or disclosure must be for a "permitted purpose"

Section 80H of the Privacy Act defines a "permitted purpose" as "a purpose that directly relates to the Commonwealth's response to an emergency or disaster in respect of which an emergency declaration is in force". Some examples of "permitted purposes" include:

- identifying individuals who are, or may be, missing, injured or dead, or who are otherwise involved in the bushfire
- assisting individuals involved in the bushfire to obtain medical treatment, health services, or financial or other humanitarian assistance
- assisting law enforcement in relation to the bushfire and
- coordinating or managing the bushfire

Important points to note

- The Declaration only applies to entities covered by the Privacy Act. It does not override state and territory privacy laws which regulate the collection, use and disclosure of personal information.
- Under s 80P of the Privacy Act, there are limits on whom personal information can be disclosed to. The specific limits depend on whether the disclosure is by an agency, an organisation or other person. For example, Commonwealth agencies can only disclose personal information to Australian government agencies, state and territory authorities, the person(s) responsible for the concerned individual, an "organisation" (as defined under the Privacy Act) and any other entity involved in managing the bushfire emergency.
- The Declaration does not permit disclosure to media organisations.
- Entities will still need to comply with other obligations under the Privacy Act, including collection notices.

How long does the Declaration last?

The Declaration is effective for 12 months (that is, until 20 January 2021). After this time, entities governed by the Privacy Act will no longer be permitted to collect, use or disclose personal information for the reasons listed above, unless the relevant use or disclosure is permitted by other provisions of the Privacy Act or another relevant law.

How should entities respond?

Entities subject to the Privacy Act should familiarise themselves with the implications of this Declaration. In particular, they should ensure that they understand the Declaration's parameters.

The Office of the Australian Information Commissioner has published some guidance material on this topic for Commonwealth agencies and private sector organisations.[1]

If you require further information about the Declaration and its effects, please get in touch.

Dr Ashley Tsacalos
Partner
Clayton Utz
atsacalos@claytonutz.com
www.claytonutz.com

Monique Azzopardi
Senior Associate
Clayton Utz
mazzopardi@claytonutz.com
www.claytonutz.com

Footnotes

1. Office of the Australian Information Commissioner, Australian Bushfires Disaster Emergency Declaration — Understanding your privacy obligations, 21 January 2020, www.oaic.gov.au/privacy/guidance-and-advice/australian-bushfires-disaster-emergency-declaration-understanding-your-privacy-obligations.

DNA testing kits and privacy: a teaspoon of spit helps the medicine go down

Sharon Givoni *and* ***Rahul Shah*** *SHARON GIVONI CONSULTING*

Take away tips:

- Genetics testing companies, like Veritas Genetics, Ancestry and 23andMe, are providing consumers with an unprecedented level of access to their personal genome.
- Law enforcement agencies and the Australian Federal Police can heavily influence genetic testing companies to share people's genetic data.
- Large genetic testing companies have signed a list of best practices when it comes to privacy, but these practices are voluntary.
- Consumers should study the terms and conditions and privacy policy of DNA testing companies to understand how their genetic data will be used and shared.

A teaspoon worth of spit can not only unlock mysteries surrounding one's ancestry, genes and geographical origins but can recommend what skincare or diet regime is best for someone.

Genetic testing is turning the corner on pre-screening technology in many ways. If done right, it means that you can know in advance your health risks based on genetic precursors that could be passed on to your offspring. It even helps you work out a diet and fitness regimen to stave off certain cancers or keep your health at such a level to slow or stop inherited gene mutations that lead to illness.[1]

Commercial DNA testing companies are on the rise, and DNA testing prices have significantly reduced in the last few years.[2] By the start of 2019, a staggering more than 26 million people had taken an in-home ancestry test from four leading commercial DNA testing companies. If this trend continues, then these companies could house DNA data of more than 100 million people in the near future.[3]

Genetic testing can reveal everything from traits toward balding, macular degeneration and hearing loss, to whether an athlete's muscles are genetically tuned toward fast twitch or slow twitch. Gene testing can also find markers for far more invasive issues such as cystic fibrosis, Parkinson's disease, breast/ovarian cancers and amyotrophic lateral sclerosis.[4]

DNA tests are big business. While once considered as the future of medicine, now they are part of a social network, and the result is a data privacy mess.[5] In this article, we will discuss the risks of sharing DNA with genetic testing companies, what steps are being taken to protect the consumer's DNA and what can consumers do to protect their genetic data.

Risks of sharing DNA with genetic testing companies

Not everyone reads the privacy policy, only a minority do. According to a new Pew Research Study, under 10% of the people always review a privacy policy.[6]

Consumers are often not aware that their genetic data can be shared with third-party companies. In 2018, 23andMe signed a USD300 million deal with GlaxoSmithKline that gives the pharmaceutical company access to aggregate consumer data.[7]

There are other weaknesses. Privacy policies of genetic testing companies are, at times, ambiguous and do not divulge information on how they deal with a customer's DNA. Dr James Hazel, in his research on genetic test privacy policies, found that 39% of the 90 genetics testing companies had "no readily accessible policy applicable to genetic data on their website".[8]

As such, there have been complaints that the terms and conditions of the DNA testing companies are not always transparent about data sharing.[9] The US Federal Trade Commission (FTC), therefore, in 2018 began investigating the data security practices of DNA testing companies like 23andMe and AncestryDNA and how they share data with third parties.[10]

Law enforcement agencies and the federal government can use DNA data from genetic testing companies. Police were able to arrest the notorious Golden State killer by using data from GEDMatch, a genealogy research site where genealogical and genetic information are uploaded.[11] In February 2019, FamilyTreeDNA granted the Federal Bureau of Investigation access to its almost 2 million genetic profiles.[12] In November 2019, a US judge approved a warrant for the police to search the full GEDMatch database during an investigation.[13]

Discrimination on the basis of genetics by employers and insurance companies may also be possible. In the past, life insurance companies were able to ask applicants to disclose all genetic test results, including results from direct-to-consumers tests.[14] Life insurers then used these results in underwriting and policy decisions, and there had been cases where consumers were discriminated on the basis of their genetics.[15]

However, in 2014, the Financial Services Council has imposed a ban on the life insurance companies from requesting the results of genetic testing.

The ban will last until 30 June 2024 and a review will be conducted in 2022.[16] Surveys have also found a handful cases of discrimination in employment on the basis of genetic status in Australia.[17] In Australia, discrimination on the basis of genetic information is dealt by the Commonwealth, state and anti-territory laws. In the US, the Genetic Information Nondiscrimination Act 2008 was enacted, and it prohibits employers and health insurers from discriminating on the basis of genetics.[18] However, according to the legal experts this Act is narrow and few Americans who receive insurance from the government are not covered by this Act.[19]

Companies that seek permission from consumers to use DNA data in research studies use either de-identified aggregate data, de-identified individual level data or both. According to Dr Hazel, de-identified aggregate data is safe but de-identified individual level data is not always safe. There is always a risk that a person can be re-identified from a de-identified individual level data.[20]

Analysts have warned that there is very little information on how long the genetic testing companies will store the physical sample. Some companies say that the samples are stored for 1 to 10 years. Further, laws governing DNA databases vary from country to country. An individual's DNA may also become a part of the global database.[21]

Hacking is a real threat to the genetic testing companies. In 2018, an Israeli DNA testing company MyHeritage declared that a security researcher had found tens of millions of account details for approximately 92 million customers, including email addresses and hashed passwords. However, the company assured its users that there was no evidence of unauthorised access to accounts and data, like DNA. Further, the company said that the DNA data is stored on separate servers and is protected by additional layers of security. In the subsequent days, the company expired all of its users' passwords and employed a two-factor authentication system.[22] Further, scientists believe that genes can also be hacked, and that malware could be placed in DNA to compromise the security of the computers holding databases.[23]

Protecting a consumer's DNA

Genetic testing companies are taking steps to protect the DNA of their consumers. According to Dr James Hazel, large companies such as 23andMe and Ancestry have signed a list of best practices (a policy framework created by the Future of Privacy Forum). These practices require DNA testing agreements to be transparent on data collection, adoption of active security measures and usage of valid legal processes when working with law enforcement officials.

The genetic testing companies have agreed to get separate express consent before providing genetic information to third parties. The Privacy Best Practices for Consumer Genetic Testing Services can be found on the Future of Privacy Forum website.[24] However, it should be noted that these practices are voluntary and not mandatory. Big companies, due to public opinion and feedback, may choose to follow these practices, small companies may overlook them.[25]

On a legal level, the European Union's General Data Protection Regulation treats DNA as a special category of personal data. In other words, genetic data has heightened protections over regular personal data. In the US, data privacy Bills on genetic data regulation are being circulated and considered at the federal level.

In Australia, the Privacy Act 1988 (Cth) defines "health information" as including "genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual" and "sensitive information" as including "genetic information about an individual that is not otherwise health information". The term "genetic information" is not expressly defined in the Privacy Act but can include information gained from various sources such as clinical examination, DNA testing, chromosome studies, family history and the like. Therefore, Australian privacy laws protect a consumer's rights for DNA testing services provided in Australia. However, these protections do not apply to overseas DNA testing services.

Despite the international laws and regulations, studies have shown that the direct-to-consumer genetic testing companies are not consistently meeting the guidelines relating to confidentiality, privacy and secondary use of data.[26]

What can consumers do to protect their data?

The US FTC advises consumers to be proactive about their privacy. They recommend examining each DNA testing companies' website for details about data usage and sharing. Consumers are also encouraged to select more protective options when opening an account with a

DNA testing company. Further, if a genetic testing company isn't living up to its promises, then consumers can lodge a complaint with the FTC.[27]

Conclusion

So next time, before you spit into a tube, remind yourself that you are not only sharing your genetic data, you are also sharing the genetic make-up of your ancestors. Further, the science behind DNA testing may not be accurate.

Some tests can be informative and even life-saving — others can be the beginning of someone's worst nightmare; and who knows the effect of a false-positive on how a life will be lived.

Consumers should not underestimate the privacy risks that home DNA testing kits pose. Genetic data can be shared with third parties, local enforcement agencies and the police and hacking may result in DNA data being leaked. Privacy risks are not well understood by consumers. They should be encouraged to read the privacy policy and terms and conditions of the genetic testing companies and they should bear in mind that these agreements can change over time. There is nothing more private than one's personal information. The question is — do consumers really know the true risks. The answer is — in most cases probably not.

Sharon Givoni
Principal Solicitor
Sharon Givoni Consulting
sharon@iplegal.com.au
www.sharongivoni.com.au

Rahul Shah
Paralegal
Sharon Givoni Consulting
rahul@iplegal.com.au
www.sharongivoni.com.au

Footnotes

1. J Jones, Is a genetic testing a good idea?, 10 January 2018, www.thegardenisland.com/2018/01/10/lifestyles/is-a-genetic-testing-a-good-idea/.
2. L Coackley, Which DNA testing company should I use?, 23 March 2015, www.genie1.com.au/which-dna-testing-company-to-use/.
3. A Regalado "More than 26 million people have taken an at-home ancestry test" *MIT Technology Review* 11 February 2019 www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.
4. Above n 1.
5. P Aldhous, 10 Years Ago, DNA Tests Were The Future of Medicine. Now They're A Social Network — And A Data Privacy Mess, 11 December 2019, www.buzzfeednews.com/article/peteraldhous/10-years-ago-dna-tests-were-the-future-of-medicine-now.
6. R Molla, Genetic testing is an inexact science with real consequences, 13 December 2019, www.vox.com/recode/2019/12/13/20978024/genetic-testing-dna-consequences-23andme-ancestry.
7. S Zhang "Big Pharma Would Like Your DNA" *The Atlantic* 27 July 2018 www.theatlantic.com/science/archive/2018/07/big-pharma-dna/566240/.
8. Above n 6.
9. M Baram "The FTC is investigating DNA firms like 23andMe and Ancestry over privacy" *Fast Company* 6 May 2018 www.fastcompany.com/40580364/the-ftc-is-investigating-dna-firms-like-23andme-and-ancestry-over-privacy.
10. C Brook, FTC Investigating How DNA Testing Firms Protect User Data, 11 June 2018, www.digitalguardian.com/blog/ftc-investigating-how-dna-testing-firms-protect-user-data.
11. Above n 9.
12. K V Brown, Major DNA Testing Company Sharing Genetic Data with the FBI, 2 February 2019, www.bloomberg.com/news/articles/2019-02-01/major-dna-testing-company-is-sharing-genetic-data-with-the-fbi.
13. C Osborne, Privacy worries cited as possible reason for DNA test firm 23andMe's sales downturn, 24 January 2020, www.zdnet.com/article/privacy-worries-cited-as-reason-for-dna-test-firm-23andme-layoffs/.
14. J Tiller, M Otlowski and P Lacaze "Should Australia Ban the Use of Genetic Test Results in Life Insurance?" (2017) 5 *Frontiers in Public Health*.
15. J Tiller and others "Genetic discrimination by Australian insurance companies: a survey of consumer experiences" (2020) 28 *European Journal of Human Genetics* 108.
16. J Collett "Discrimination on genetic testing by life insurers ends" *The Sydney Morning Herald* 2 July 2019 www.smh.com.au/money/insurance/discrimination-on-genetic-testing-by-life-insurers-ends-20190701-p522wj.html.
17. Australian Law Reform Commission *Essentially Yours: The Protection of Human Genetic Information in Australia* ALRC Report 96 (2003), Vol 2 Chapter 30 "Evidence of genetic discrimination in Australia" (28 July 2010) www.alrc.gov.au/publication/essentially-yours-the-protection-of-human-genetic-information-in-australia-alrc-report-96/30-genetic-discrimination-in-employment/evidence-of-genetic-discrimination-in-australia/.
18. National Human Genome Research Institute, Genetic Discrimination, 5 February 2020, www.genome.gov/about-genomics/policy-issues/Genetic-Discrimination.
19. E Rosenbaum "5 biggest risks of sharing your DNA with consumers genetic-testing companies" *CNBC* 16 June 2018 www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html.

20. E Ravenscraft "How to Protect Your DNA Data Before and After Taking an at-Home Test *The New York Times* 12 June 2019 www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html.
21. Mozilla Foundation, 23 reasons not to reveal your DNA, April 2019, https://internethealthreport.org/2019/23-reasons-not-to-reveal-your-dna/.
22. Above n 10.
23. M Molteni, Scientists Upload a Galloping Horse GIF Into Bacteria With Crispr, 7 December 2017, www.wired.com/story/scientists-upload-a-galloping-horse-gif-into-bacteria-with-crispr/.
24. Future of Privacy Forum *Privacy Best Practices for Consumer Genetic Testing Services* (2018) www.fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
25. Above n 6.
26. L I Laestadius, J R Rich and P L Auer "All your data (effectively) belong to us: data practices among direct-to-consumer genetic testing firms" (2017) 19 *Genetics in Medicine* 513. www.nature.com/articles/gim2016136.
27. L Fair, DNA test kits: Consider the privacy implications, 12 December 2017, www.consumer.ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications.

Privacy Law
Bulletin

Credit reporting and the consumer data right

Andrea Beatty *and* ***Gabor Papdi*** *PIPER ALDERMAN*

The purpose of the consumer data right (CDR) in the context of the banking sector is to increase competition by:

- enabling consumers to more easily compare products offered by different providers, and
- reducing the information advantage that incumbent participants have over new entrants to the market for banking services[1]

This article is to briefly explore the operation and purpose of the current credit reporting regime and speculate on how and why it may be affected by the incoming CDR.

The introduction of the CDR, beginning with the banking industry, is imminent and inevitable. The required legislation[2] has been passed and all that appears to remain is for the rules and data standards to be finalised once technical issues discovered in testing of the CDR ecosystem have been remedied. Notwithstanding the delays in implementing the CDR, the Commonwealth Government is already flagging an intention to expand its functionality and has announced an inquiry to examine ways in which the CDR can be expanded beyond its current contemplated functionality and leveraged with other frameworks (eg, the New Payments Platform), among other things.[3]

The CDR in banking will encompass two broad kinds of data:

- product data, which is standardised general information about a particular product, and
- consumer data, which is data about a particular consumer and their use of a particular product (including certain items of personal information, account identification information, account balances and transaction data)

Product data facilitates product comparison by or for consumers, whereas consumer data facilitates price competition by overcoming the information advantage that an incumbent provider might have over a new entrant (or the consumer's existing provider over another market participant).

An obvious use case for the CDR is in relation to consumer credit products. Consumers may choose to share their data with credit providers and intermediaries who are accredited data recipients for the purpose of:

- enabling credit providers and credit assistance providers to perform responsible lending checks, and
- enabling credit providers to better ascertain the consumer's default risk and quote a price for credit more closely aligned with the consumer's risk profile

It is the latter purpose that the credit reporting regime in Pt IIIA of the Privacy Act 1988 (Cth) also seeks to fulfil. However, the incoming CDR appears to overlap with the objectives of the credit reporting regime and undercut some of its restrictions on dealing with information.

The current environment: credit reporting under the Privacy Act

Broadly speaking, the credit reporting regime in the Privacy Act is based on the concept of "credit information", and derivative items of information such as "CRB derived information" (which, together with credit information, makes up "credit reporting information" about an individual) and "CP derived information" (which, together with credit reporting information received from a CRB, makes up "credit eligibility information" about an individual). Credit providers provide credit information to credit reporting bodies (CRBs), who aggregate it with other credit information that they collect about an individual (from other credit providers and from publicly available sources) and provide credit reporting information to credit providers for the purpose of assessing applications for credit. Credit providers then use credit eligibility information to determine a consumer's credit application. Credit information and its derivative information items relate only to consumer credit; business/commercial credit is excluded, and equivalent information about business/commercial credit is not subject to Pt IIIA of the Privacy Act.

The stated purpose of the credit reporting regime is:

> … to balance an individual's interests in protecting their personal information with the need to ensure sufficient personal information is available to assist a credit provider to determine an individual's eligibility for credit following an application for credit by an individual …[4]

The balancing provided for by this purpose necessarily limits the effectiveness of the credit reporting regime in improving credit providers' ability to ascertain a consumer's risk profile for pricing and eligibility purposes. This reduces the effectiveness of credit reporting information to ascertain the default risk of a consumer. It also limits the goal of increasing competition in the consumer credit market:

- The kinds of information that may be collected, disclosed and used are very narrowly defined — credit information is defined in the Privacy Act[5] as being information within certain discrete categories of information about an individual — including default information, repayment history information, consumer credit liability information, payment information and new arrangement information — which in turn narrowly defined in the Privacy Act.
- Participation is limited to credit providers, credit reporting bodies, mortgage insurers and trade insurers, limiting the ability for credit intermediaries to use the information (other than by an access request on behalf of a consumer) to provide credit-related services to consumers.
- Aside from some limited exceptions, credit reporting information may only be disclosed and used in circumstances where an individual has already made an application for credit (or, for purchasers under securitisation arrangements, where credit has already been provided), limiting the extent to which it can promote price competition between credit providers.
- Credit eligibility information may only be used by a credit provider in similarly narrow circumstances.
- The Privacy Act and CR Code impose notification and grace period requirements that must be satisfied before the fact of a payment default can be reported as default information to a CRB.
- The Privacy Act limits the amount of time for which credit information can be retained for use by a CRB or credit provider.

Although the current iteration of the credit reporting regime is described as "more comprehensive"[6] than its predecessor system, it still restricts dealings in credit-related personal information. This is reflected in the narrowness of the permitted dealings in credit information and credit reporting information and, unlike for "ordinary" personal information under the Australian Privacy Principles, the absence of a general ability for individuals to consent to dealings in credit-related information about themselves outside those specifically permitted dealings. This is understandable in light of the purpose of protecting personal information about an individual, though it does undermine the utility of the information in assessing default risk and in promoting competition in the market for consumer credit.

Further, the focus on having sufficient information to assess an individual's eligibility for credit assumes that the price of credit is a constant. Whilst some credit providers' individual risk controls may result in them refusing to provide credit to consumers of a certain risk grade, regardless of the price of credit, other credit providers may be willing to provide credit to anyone at a price that appropriately reflects the default risk borne by the credit provider. Also, price and eligibility come into consideration at different points in the credit sales process. The price of credit is generally announced at the outset and, if a consumer considers the price to be agreeable, they may apply for credit, after which the credit provider assesses their eligibility by reference to, among other things, credit reporting information obtained from CRBs. The current credit reporting regime prevents credit reporting information from being used earlier in the process to determine the price at which a credit provider may be willing to provide credit to a particular individual.

The incoming CDR

The essence of the CDR is a right for consumers to obtain a copy of specified information about themselves from a designated data holder, or to direct the data holder to give a copy of it to another person (an accredited data recipient) in a standardised machine readable format. When fully operational, the CDR for the banking sector will require:

- product data to be made available to the public in standardised machine readable format, and
- consumer data to be made available to the consumer to whom it relates in machine readable format and to accredited data recipients in standardised machine readable format

As noted earlier in this article, product data will facilitate comparisons between product features. It is likely to lead to an increase in product comparison services. The sharing of consumer data, however, is the more revolutionary aspect of the CDR. It will enable personal information about the consumer related to their account, account information including account balances and periodic payment authorisations, and transaction data for the account for the past 7 years.[7] Accounts covered will include transaction and deposit accounts, credit and debit card accounts and mortgage and personal loan accounts.

The sharing of data will be consumer-driven. It will be for the consumer to consent to an accredited data

recipient collecting and using data, and to authorise the data holder to disclose data to the accredited data recipient for that purpose. Consents will be express, voluntary, limited to specific collection and uses — it will not be possible to give or obtain a blanket consent — and time-limited.

Potential interaction between credit reporting and the CDR

Consumer data, particularly a customer's transaction history, will provide information that is relevant and probative to the issue of a consumer's default risk. To this extent, its function will overlap with that of the credit reporting regime. Further, transaction data may in some cases provide an opportunity to reconstruct various items of credit information — for example, the existence of a particular consumer credit liabilities could be inferred from transactions relating to regular payments, and default information could be inferred from transactions for default fees or the absence of a regular payment. In this sense, CDR data could be at least a partial substitute for credit reporting information from credit reporting bodies.

This is because CDR data generally may offer a richer source of data that is more probative of a person's default risk than credit information. This richer data will need to be traded off against the fact that for credit reporting information, much analysis of raw data has been performed by the CRB and resulted in an output that provides a relative measure of default risk (eg, a credit score). For CDR data or consumer data, the burden of analysing the raw data to draw conclusions about an individual's default risk will be with the data recipient credit provider. However, for third party data processors with no doubt after consumer data analysis services, themselves becoming accredited data recipients for this purpose.

Where to next for credit reporting?

It appears likely that, in the near future at least, credit reporting will have a role to play in credit risk assessment and will not be entirely replaced by the CDR. CRB derived information that is the result of analysis by the CRB, using proprietary default risk models developed over long periods of time, will continue to be valuable to credit providers.

The enthusiasm with which consumers receive and use the CDR in relation to banking may also influence the future of credit reporting. It seems likely that CRBs and other third parties will leverage their data analysis services to provide information that is more probative of default risk than available from current credit reporting information only.

Also, as much of the value added by CRBs is through the data analysis that they perform, the CDR may give rise to new opportunities for CRBs to leverage their experience in modelling default risk to provide data analysis services in respect of CDR consumer data.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
https://piperalderman.com.au/

Gabor Papdi
Lawyer
Piper Alderman
gpapdi@piperalderman.com.au
https://piperalderman.com.au/

Footnotes

1. In this article, "banking services" refers to services typically provided by banks in Australia and so goes beyond the concept of "banking business" to include financial advice, wealth management, insurance and moneylending.
2. Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth), amending the Competition and Consumer Act 2010 (Cth), Privacy Act 1988 (Cth) and Australian Information Commissioner Act 2010 (Cth).
3. The Hon Josh Frydenberg MP "Building on the Consumer Data Right" media release (23 January 2020) https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/building-consumer-data-right.
4. Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, 90.
5. Privacy Act 1988, s 6N.
6. Above n 4.
7. Proposed Competition and Consumer (Consumer Data Right) Rules 2019 sch 3 cl 1.3, www.accc.gov.au/system/files/Proposed%20CDR%20rules%20-%20August%202019.pdf.

For editorial enquiries and unsolicited article proposals please contact Genevieve Corish at genevieve.corish@lexisnexis.com.au or (02) 9422 2047
Cite this issue as (2020) 16(9) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067