Financial Rights
LEGAL CENTRE

Submission by the
Financial Rights Legal Centre

Australian Human Rights Commission

Human Rights and Technology Issues Paper, July 2018

October 2018

Financial Rights Legal Centre |PO BOX 538, Surry Hills 2010 | Tel (02) 9212 4216 |Fax (02) 9212 4711 |
info@financialrights.org.au | www.financialrights.org.au | @Fin_Rights_CLC | ABN: 40 506 635 273

About the Financial Rights Legal Centre

The Financial Rights Legal Centre is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters. Financial Rights took close to 25,000 calls for advice or assistance during the 2017/2018 financial year.

Financial Rights also conducts research and collects data from our extensive contact with consumers and the legal consumer protection framework to lobby for changes to law and industry practice for the benefit of consumers. We also provide extensive web-based resources, other education resources, workshops, presentations and media comment.

This submission is an example of how CLCs utilise the expertise gained from their client work and help give voice to their clients' experiences to contribute to improving laws and legal processes and prevent some problems from arising altogether.

For Financial Rights Legal Centre submissions and publications go to
www.financialrights.org.au/submission/ or www.financialrights.org.au/publication/

Or sign up to our E-flyer at www.financialrights.org.au

National Debt Helpline 1800 007 007
Insurance Law Service 1300 663 464
Mob Strong Debt Help 1800 808 488

Monday – Friday 9.30am-4.30pm

Introduction

Thank you for the opportunity to comment on the Australian Human Rights Commission's (**AHRC's**) Human Rights and Technology Issues Paper, July 2018. The Financial Rights Legal Centre (**Financial Rights**) believes this is a timely investigation.

The Financial Rights is a community legal centre that specialises in helping consumers understand and enforce their financial rights, especially low income and otherwise marginalised or vulnerable consumers. We provide free and independent financial counselling, legal advice and representation to individuals about a broad range of financial issues. Financial Rights operates the National Debt Helpline, which helps NSW consumers experiencing financial difficulties. We also operate the Insurance Law Service which provides advice nationally to consumers about insurance claims and debts to insurance companies, and the Mob Strong Debt Help services which assist Aboriginal and Torres Strait Islander Peoples with credit, debt and insurance matters.

Our interest in the issues being raised by the Australian Human Rights Commission in this paper is focussed on the implications of technology on financially vulnerable consumers and their human rights. This submission is based upon our casework experience with people experiencing financial hardship and what we have started to witness with respect to the increased use of new computing technologies in the financial services sector and their subsequent and expected impact..

Threats and opportunities arising from new technology

---

1. What types of technology raise particular human rights concerns? Which human rights are particularly implicated?

Financial Rights has identified a number of technologies that are currently being used (or are expected to be used) in the financial services sector whose impact and use needs to be considered by the AHRC. Many of these technologies are being used outside of the financial services sector but are being put to use in this sector in unique ways. Most are a combination of both:

- new hardware i.e. new computing devices (such as smart phones, tablets and other personal computing devices), and computing infrastructure such as cloud computing and GPS technologies; and
- new software utilising new data collection technologies and processing techniques.

This new computing power and technology has led to:

- an expansion of the data collection of their own customers as well as from external sources both conventional (e.g. government databases and transactional data), and unconventional (e.g. social media, emails etc.);

- advanced data processing techniques; and
- advanced analytical, artificial intelligence and algorithmic techniques including predictive analytics.

These have, in turn, led to the development of financial technology or what has become known as FinTech. The burgeoning FinTech sector is creating products and services that allow consumers to interact with financial services via these new technologies. These services include:

- mobile and online banking (CBA, ANZ apps);
- Open Banking (as currently being implemented in Australia) using consumer transaction data to assist in a series of services including but not limited to account switching, mortgage search services;
- new personal financial management services (such as Money Dashboard);
- investment and wealth management services with automated or robo-advisers services such as Wealthfront;
- new lending and unsecured credit services based on data led credit-scoring and risk profiling (e.g. Afterpay, Defer It);
- new payment services (Apple Pay),
- encrypted digital wallets that stored bank, debit or credit card detailing for online payments (e.g. PayPal and AliPay);
- neo banks and FinTech savings banks such as AliPay's Yu'eBao;
- offline mobile payments such as Apple Pay, Android Pat or Ali Pay used at retail locations; and
- credit scoring and social scoring – utilising financial and social datasets from non-traditional sources such as Facebook and other social media to create measures of credit worthiness, outside of the "traditional" credit reporting and scoring.

There is also a sub-class of FinTech known as InsurTech. Connected devices and telematics technology (e.g. Fitbit), connected home technologies (e.g. Amazon Alexa) and what is known as the "Internet of Things" (e.g. connected smoke alarms, locks, fridges and light switches) are also being put to specific use by the insurance sector.

Telematics technologies involve the use of GPS technology and increased information processing power to collected and transmit information and data to insurers directly. Telematics devices being used by insurers include:

- Motor vehicle telematics – devices in vehicles that can record GPS location data as well as information from a vehicle's engine management system to monitor all aspects of driving style QBE, for example, offers "Insurance Box for young drivers.". Here, drivers install an electronic device or "black box" in their car that transmits back to the insurer a detailed breakdown of their driving habits in areas such as their braking, acceleration,

steering, cornering, speed and night driving.[1] QBE then calculate a "DriveScore" rating to evaluate the driver. The higher the DriveScore the less the policyholder will pay for insurance. The lower the score, the more the driver pays.

- Home telematics – devices can monitor the use and supply of a range of utilities as well as security of a home. Smart smoke alarms, water leak and freeze detectors are already being used overseas by insurers.
- Health monitors – fitness monitors such as Apple Watch and FitBit can record the location, movement, activities and other health information. AIA vitality[2] is an example of a product that enables a life insured to gain benefits such as discounts and rewards via the earning of "vitality points" for activities undertaken.[3] Others include Asteron Life Plus Health Rewards and Bupa Living Well.

Insurers (as well as banks, FinTech companies and other financial services) are also harvesting data from non-traditional sources to identify risk and increase their ability to analyse and underwrite risk.

Insurers are using genetic testing technology in their underwriting provided to them under disclosure laws, an ability borne of increased computing processing power, new hardware and data analytics.

Many of the FinTech and InsurTech services are using algorithms and artificial intelligence (**AI**) for automated decision making.

Blockchain - a distributed ledger with no central governing body - has been used to support, most famously, the development of Bitcoin and other cryptocurrency transactions – but also supports the development of FinTech technologies related to loans, payments, trading by enabling authenticity, efficiency and transparency. Blockchain can enhance the efficiency of loan origination and servicing, improve clearing house functions and can be applied to so-called smart contracts.

Many of these products and services have various effects upon consumers. Some of the more positive impacts include:

- enabling increased access to financial services;
- shifting the channel and form of how consumers interact with financial service providers from a physical to a non-physical presence;
- creating new non traditional services;
- changing the way consumers transact or receive or give payments; and
- potentially empowering consumers in increasing their own financial literacy, behavior or wellbeing.

[1] https://www.qbe.com.au/news/car/how-insurance-box-works

[2] https://www.aiavitality.com.au

[3] https://www.aiavitality.com.au/vmp-au/rewards

There are however a series of impacts upon consumers – particularly consumers experiencing financial vulnerability or hardship - that are of significant concern to Financial Rights. These impacts directly relate to the right to privacy, the right to equality and right to live free from discrimination and the right to safety and security.

FinTech, Data and Privacy

FinTech products and services' utility arises from a near total reliance on data – largely a consumer's personal financial data - their transactions history, credit history, etc. FinTechs are also integrating financial data with other data about individuals drawn from social media and other sources – information that people would consider have nothing to do with their financial status. InsurTech is also tracking people's every movement and drawing conclusions about a person's identity and their life derived from the use of their car.

This increased collection of data is feeding the creation of a "financial identity" – a concept increasingly used by financial institutions to get to know their customer more.

Financial institutions have for years stored and verified customer identities and attributes through "Know Your Customer" systems i.e. the process by which banks or other financial institutions identify their customers in order to evaluate the possible legal and other risks. They therefore have a commercial incentive to collect more and more accurate information about their individual customers. The World Economic Forum in 2016 has in fact argued that financial institutions "should champion efforts to build digital identity systems, driving the building and implementation of identity platforms."[4] However the development of an increasingly accurate financial identity built by data has serious consequences and harms for consumers. A person's financial circumstance is highly sensitive since its use by financial institutions, or in other cases a breach causing a leak of this private information, opens them up to a range of significant problems. We detail the following identified harms.

Exploitation by unscrupulous operators and profiling for profit

We are concerned that with the rise of FinTech and more accurate financial identities, we will see increased occurrences of consumers being 'profiled for profit', which will see more people experiencing financial difficulties or hardship being offered unsuitable (but highly profitable) products.

Target marketing of products to particular groups of consumers is not new. In consumer lending, technology can be used to identify consumers who are likely to be profitable, tailor and price products that the most profitable customers are likely to accept, and develop strategies to reduce the likelihood that the most profitable customers will close their accounts.

Consumers struggling with debt are however often the most profitable customers for banks and lenders. It is often argued that it is not in the interests of lenders to extend credit to people who are unable to repay. However, our experience suggests that many consumers struggle for

[4] World Economic Forum & Deloitte (2016) "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity": page 28
http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

years at a time to make repayments to their credit accounts without ever reaching the point of default, but paying significant amounts of interest. These customers are very profitable for lenders, despite the fact that repayments are causing further financial hardship.

Another example of profiling for profit is the practice (used by many pay day lenders) whereby customers are asked to provide access to their bank statements via third party account aggregation software for responsible lending assessment purposes. Providing access to this 'screen scraping' technology can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the ePayments Code. We are concerned that some lenders may be keeping these links open after the initial lending assessment has been completed, so that they can direct their marketing of further loans to consumers specifically when their account is empty and their need for cash is likely to be at a high point.

These concerns have been echoed by consumer advocates in the United Kingdom, who have raised concerns that 'Open Banking enables lenders to continually monitor accounts and take repayment as soon as income is detected.' These are real risks that are poorly understood by consumers and unlikely to be dealt with by disclosure and consent because of the take it or leave nature of the service.

Seemingly 'free' or 'freemium' business models could also see an increase in the onward sale of transactional data or the commission-based selling of unsuitable financial products, because it is a way for firms to monetise what they do without requesting a fee upfront.

Price discrimination on low-income households

Much of the promise of FinTech is that more tailored products and services will be made available with lower fees or lower loan interest rates for many banking customers. However, the flip side to lower fees and interest rates for some is that costs will increase for others. These 'others' will undoubtedly be Australia's most vulnerable, disadvantaged and financially stressed households.

Those in more precarious financial situations – again identified as such by their data driven financial identities - will likely be unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders. In other words, the consumers who can afford it the least will pay the most be it via higher interest rates or higher fee products. There are serious fairness considerations at play here. As banks and credit providers are increasingly able to use consumer data and technology to better target particular financial services offers to 'profitable' consumers, we will likely see an increased use of 'risk-based pricing'. This may result in some lenders targeting 'riskier' borrowers with higher interest rates. While risk based pricing has effectively existed in Australia in the non-bank sector for some years, we have recently seen the first example of risk based pricing by a major bank.

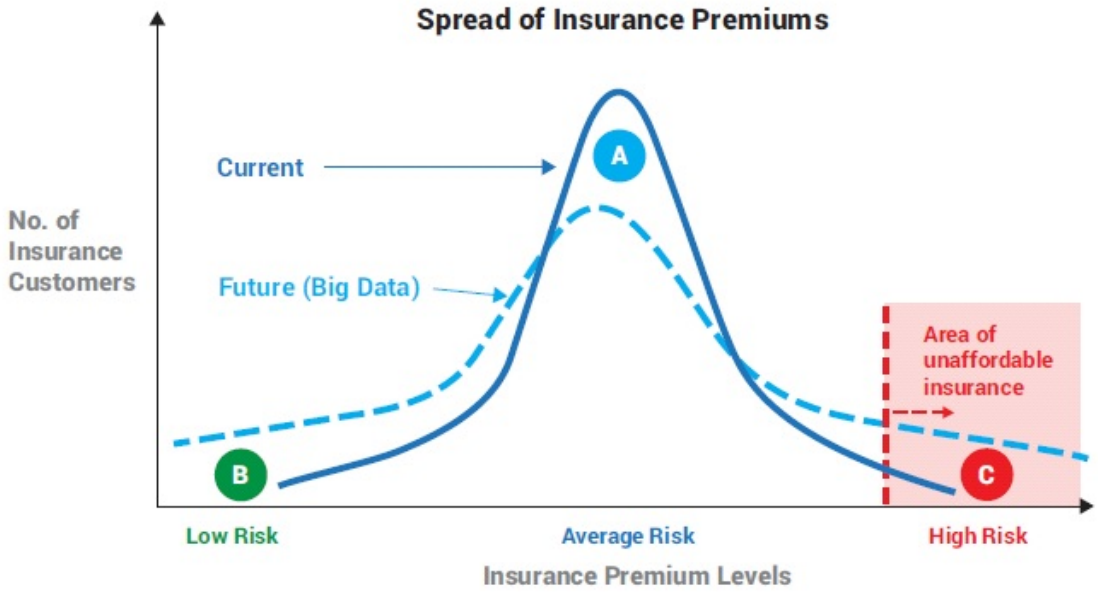
A 2015 report by United States organisation Data Justice has previously raised concerns about big data enabling advertisers to offer goods at different prices to different people to extract the maximum price from each individual consumer. The report found that such price discrimination not only raised prices overall for consumers, but particularly hurts low-income and less technologically savvy households. In fact, the ability to segment the market further

will likely mean that firms can 'cherry pick' the most commercially viable consumers and exclude others (or charge them more).

It is clear that the result of the price discrimination enabled by these technologies in the financial services sector is a downward spiral of debt. A self-fulfilling prophecy ensues. A consumer's low credit rating decreases from a default, which in turn feeds an algorithm of credit-worthiness leading to higher interest rates and further financial difficulty and further defaults.

In the insurance sector, the increased use of big data analysis and processing allowed by increased computing power will enable insurers to increasingly distinguish between risks on an increasingly granular level. This will lead to the higher risks only being able to be insured for higher prices or on worse terms. According to the Actuaries Institute

> *"At the extreme, some policyholders will have their risks assessed as so high that the price will be prohibitive or insurers will decline to provide cover. The following diagram illustrates the effect that increasing data will have on insurance premiums"*



> *Overall, there will be fewer insureds treated as "average" risk (area A) and paying average premiums. They will increasingly be classed as either lower or higher than average. Greater numbers of insureds will thus be recognised as being lower risk and given lower insurance premiums (area B). Conversely there will be more consumers falling into the higher risk category, ultimately reaching the "unaffordable" levels of insurance premiums (area C).*
>
> …
>
> *In response, some people may mitigate or avoid the risk. Others who find the insurance premiums for their risk to be unaffordable may have to take the risk themselves. If the risk event does happen, they will suffer financially. The more people change from insured to*

uninsured status because of price increases arising from more targeted use of data, the greater the burden will be on the public purse or on others outside the insurance system.[5]

Price discrimination in insurance and the broader financial services sector should be a cause for serious concern where it contributes to lower-income people paying higher prices than others, or where pricing discrimination negatively affects particularly marginalised groups. In the insurance sector, people who need insurance the most may increasingly find they have been excluded completely as a result of issues which may be completely beyond their control. These are key issues of fairness and equity.

Discrimination

Closed proprietary algorithms used by FinTechs and InsurTechs to automatically calculate say an individual's credit worthiness or the interest rate they are offered could also potentially lead to situations where consumers are denied access to crucial products and services based on accurate or inaccurate data without the ability to determine why or to correct underlying assumptions.

Algorithmic bias or discrimination is already well documented[6] and arises when an algorithm used in a piece of technology – say a FinTech product or service – that reflects the implicit or explicit values of those who are involved in coding, collecting, selecting, or using data to establish and develop an algorithm.

Credit scoring, social scoring or e-scoring algorithms for example can produce feedback loops where somebody from a particular suburb where a lot of people default can be given lower credit ratings due to that association. Statistical correlations used by actuaries between a person's postcode (here geographical information standing in for a particular race, ethnicity or culture); their language patterns on social media; their potential to pay back a loan; or, keep a job; can lead to significant discrimination being built into opaque black box algorithm technology.

Cybercrime, identity theft and material theft.

As our financial services sector becomes more and more reliant on FinTech with more and more accurate information about financial identities, individuals become increasingly vulnerable to cybercrime.

Firstly consumers are vulnerable to identity theft. With increasingly sensitive and accurate data being held by FinTechs, breaches of these datasets make it easier for criminals to use this identifying information to undertake subsequent crimes, financial or otherwise.

The vulnerability of the data protection systems in place also facilitates actual theft of property – that is the hacking of FinTech systems to access payment systems and steal money. According to Juniper Research, fraudulent online transactions will reach a value of $25.6

[5] Page 19-20, Actuaries Institute, The Impact of Big Data on the Future of Insurance https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf

[6] See Cathy O'Neil, Weapons of Math Destruction, 2017

billion by 2020[7] In Australia online credit card fraud, with transactions made using stolen card details hitting $417.6 million in 2016, more than doubling since 2011.[8]

The recent news[9] that UK company Cambridge Analytica legitimately gathered some personal data from Facebook accounts and concurrently illegitimately gathered other people's data, and then, when found out and were requested to delete the data, did not, has raised public consciousness over the potential for data to be misused in various ways. Combined with the never ending list of significant and high profile data breaches at Equifax, Ashley Madison, Yahoo and more, consumer awareness of how vulnerable consumers are is increasing every day.

2. **Noting that particular groups within the Australian community can experience new technology differently, what are the key issues regarding new technologies for these groups of people (such as children and young people; older people; women and girls; LGBTI people; people of culturally and linguistically diverse backgrounds; Aboriginal and Torres Strait Islander peoples)?**

As noted, our interest in human rights and technology is focussed on the implications of technology on financially vulnerable consumers and their human rights.

Financial vulnerability and financial hardship can cut across many demographics in the Australian community, many of whom have been identified by the paper – young, people, older people, women, LGBTI people, people of culturally and linguistically diverse backgrounds and Aboriginal and Torres Strait Islander people. While clearly not one to one, the Venn diagram of these groups and the financially vulnerable overlap significantly and to varying degrees, all the while exacerbating a digital divide.

We wish to put forward the financially vulnerable as an identifiable group within the Australian population who will be significantly impacted upon by new technology in the ways outlined in the previous answer.

Financial vulnerability is a state where people experience financial instability or a situation that exposes them to significant financial risk and shock. Vulnerability can arise during a one off short time period (of say, financial hardship borne of unemployment or illness), can arise intermittently or can be endemic over a lifetime.

---

[7] "Online Transaction Fraud to More than Double to $25BN by 2020' Juniper Research UK, May 2016.

[8] Lucy Cormack, Carol Saffer, Online credit card fraud on the rise, accounting for 78 per cent of total card fraud in Australia, SMH, 3 August 2017 https://www.smh.com.au/business/consumer-affairs/online-credit-card-fraud-on-the-rise-accounting-for-78-per-cent-of-total-card-fraud-in-australia-20170802-gxnwd7.html

[9] 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower, *The Guardian*,18 March 2018 https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

The financially vulnerable consumer is therefore someone who, due to their personal circumstances, is especially susceptible to detriment, when a corporation – be it a financial service entity or technology company - is not acting with an appropriate level of care.

Financially vulnerable consumers can find accessing financial and other products, difficult as they don't fit the mould of most consumers facing "mainstream" or "streamlined" services.

Many financially vulnerable consumers are overwhelmed by complex information and can find it hard to distinguish between promotional material and important messages about products. Otherwise intelligent and literate people experience reduced cognitive capacity as a result of financial stress.

Financially vulnerable consumers are particularly susceptible to new financial technologies in a number of ways.

Those experiencing financial hardship, as outlined above,can be very profitable to companies and therefore be vulnerable to risk profiling, price discrimination and exploitation by unscrupulous entities. Those in more precarious financial situations are more likely to be unfairly charged higher amounts or pushed to second tier and high cost fringe lenders.

Financial vulnerability can impact upon different groups of people in such a way that exacerbates the issues faced by those who are already experiencing some for form of social disadvantage.

For example, Aboriginal and Torres Strait Islander people are particularly at risk. Studies have shown lower financial literacy rates in Aboriginal and Torres Strait Islander peoples than non-indigenous communities.[10] Combined with geographic location, lack of identification documents, unemployment, we believe (and have seen in much of our case work) that many Aboriginal and Torres Strait Islander people will be particularly susceptible to negative impacts arising from financial technologies.

Young children too may be particularly vulnerable to new technologies. They may not fully understand the consequences of consents required in gaining access to FinTech as they will increasingly be expected to do.

Women are also vulnerable to the impact of new financial technologies. In the first place women subject to domestic violence are placed in a particularly acute form of financial vulnerability. The Economic Abuse Reference Group (EARG) states:

> *Family violence can have a significant detrimental impact on a woman's financial wellbeing, both during the violent relationship, and if (and when) a woman leaves the perpetrator. Financial insecurity is one reason a woman may stay in a violent relationship. Leaving a violent relationship must sometimes be done quickly and suddenly. A woman may not be able to take much with her, or may have to move far away from her home due to safety concerns.*

[10] Suzanne Wagland, Sharon Taylor, The conflict between financial decision making and indigenous Australian culture https://www.griffith.edu.au/__data/assets/pdf_file/0023/205682/FPRJ-V1-ISS1-pp33-54-indigenous-australian-culture.pdf

This can leave a family violence survivor (and often her children) with few financial resources and make it difficult to find secure housing and establish a new life.[11]

Economic abuse as a form of family violence can exacerbate the situation faced by many women. Economic abuse can include, among other things, coercing a woman to:

- incur debt for which she does not receive a benefit, or take on the whole debt of a relationship;
- relinquish control of her assets or income, or reduce or stop paid employment;
- claim social security payments;
- sign a contract, loan application or guarantee;
- sign documents to establish or operate a business;
- be prevented from access to joint financial assets, such as a joint bank account, for the purposes of meeting normal household expenses;
- disclose her credit card details and/or passwords against her will or better judgment;
- provide cash she cannot spare;
- be prevented from access to online banking or purchasing;
- be prevented from seeking or keeping employment.

This is all made much easier for the perpetrator via the use of almost frictionless technology – that is technology that is quick, simple and easy to use with little delay and lag time.

Specific problems that arise out of increased use of FinTech and InsurTech for women subject to violence include:

- inadvertently alerting an abusive partners to financial related activity that places the abused partner in an unsafe position;
- preventing abused partners from accessing products and services that would assist their situation; and/or
- consents may not be freely given when consenting to use a product or service.

These are all issues that will need to be considered.

Recommendation

1. **The AHRC must specifically consider the impact of new computing technologies on the financially vulnerable and those experiencing financial hardship in its recommendations.**

[11] Economic Abuses Reference Group, Good Practice Industry Guideline for Addressing the Financial Impacts of Family Violence, version 1a, 4 April 2017, https://eargorgau.files.wordpress.com/2017/03/good-practice-guide-final-0404172.pdf

3. How should Australian law protect human rights in the development, use and application of new technologies? In particular:

a) **What gaps, if any, are there in this area of Australian law?**

b) **What can we learn about the need for regulating new technologies, and the options for doing so, from international human rights law and the experiences of other countries?**

c) **What principles should guide regulation in this area?**

d) **In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?**

The misconceived Consumer Data Right

The Australian Government is currently seeking to introduce a Consumer Data Right (**CDR**). The CDR will provide individuals and businesses with a right to "efficiently and conveniently" access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties. The CDR will also require businesses to provide public access to information on specified products they have on offer. The Government has committed to applying the CDR to the banking, energy and telecommunications sectors.[12]

The development of this legislation and the CDR model more broadly emerges from the government's response to both the Productivity Commission's *Inquiry into Data Availability and Use Report* and the *Review into Open Banking* in Australia 2017 which recommended that Open Banking be implemented through a broader CDR framework.

While this approach may be appropriate to developing consistent application programming interfaces (**APIs**) and data standards for vastly different sectors of the economy and their unique data sets[13] , it fails to effectively address standard privacy and security expectations that apply equally across the economy.

By taking this approach the CDR regime creates a new set of strengthened privacy safeguards that will only apply to certain designated sets of financial data in certain limited circumstances. Over time it is expected that this will expand to cover certain other sectors in further limited

[12] *Treasury Laws Amendment (Consumer Data Right) Bill 2018*

[13] banking and financial information versus energy, telecommunications, social media, insurance and other sectors yet to be identified

circumstances. This approach in providing privacy safeguards for sensitive data use is therefore by its nature, limited and piecemeal.

The approach also stands in stark contrast with the EU. The EU have taken strong strides into bolstering consumer protections in this space with the new General Data Protection Regulation (**GDPR**) from May 2018 and the Payment Services Directive 2 (**PDS2**) coming into force early this year in January 2018.

The EU GDPR has established a list of 20 Data Protection Rights that applies to all individuals and businesses across the entire economy including the Right to Access, Right to Deletion, Right to Rectification, etc. The EU has established this baseline set of safeguards and is also systematically developing rules and data standards for every sector to more appropriately implement consumer facing data products and services such as open banking.

The draft CDR legislation however only implements one of the rights that the EU has implemented - the right to portability. In this sense then the CDR is a misnomer as it is merely a Consumer Data Portability/Transfer Right.

While this is implicitly acknowledged in the *Exposure Draft Explanatory Materials*[14] the Government is selling the CDR in such a way that suggests that the CDR is a broader right*:*

> *This Bill is a game changer for Australians. The Consumer Data Right will empower customers to use their data for their own benefit. … Customers will determine which data is shared, on what terms and with whom. The Consumer Data Right is a right for customers and not for those who wish to access or use a customer's data. …The Government is committed to ensuring that high levels of privacy protection and information security for customer data is embedded in the new regulatory framework. This Bill delivers enhanced protections, backed by well-resourced regulators with strong powers.* [15]

Counter to the sales pitch, the CDR is merely a collection of rights with respect to porting or transferring consumer data in certain designated sectors. It provides no further rights to more broadly access your data, restrict processing, object, delete, correct, or rectify your data. The CDR is therefore misleading as consumers are being sold the idea of a "consumer data right" to protect consumers in their access to and use of their own financial data.

All that is being created is a set of standards to be applied to the portability of consumer data with some strengthened privacy safeguards in specific designated sectors.

While these strengthened privacy safeguards are welcome, the introduction of the CDR regime will create multiple levels of privacy standards that will apply at different times to consumers seeking protection, security and redress when something goes wrong. They include:

---

[14] Para 1.1 "*The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties."*

[15] The Hon. Scott Morrison, Treasurer, Media Release *More power in the hands of consumers*, 21 September 2018, http://sjm.ministers.treasury.gov.au/media-release/087-2018/

- CDR Privacy Safeguards as envisioned under the draft CDR legislation – essentially strengthened versions of the Australian Privacy Principles (**APPs**);
- the *Privacy Act* safeguards as detailed under the APPs; and
- general consumer protections and law applying to those holders of consumer data that are *not* "APP entities" as defined under the APPs, i.e. all private sector and not-for-profit organisations with an annual turnover of less than $3 million.

To demonstrate the complexity of what is being proposed by the draft CDR legislation, a consumer could potentially be subject to the following array of high and low protections:

1. Transactional data held by a bank that may at some point in the future be CDR data (a data holder) but has yet to be requested to be ported, is currently and will continue to be subject to the APPs.
2. This transaction data becomes "CDR data" once requested to be transferred to an accredited Data Participant where its transfer and use will be subject to the CDR Privacy Safeguards.
3. The transactional data continuing to be held by the original bank remains subject to the APPs.
4. CDR data collected and held by an accredited Data Participant will be subject to the CDR Privacy Safeguards.
5. Non-CDR Data held by Accredited CDR Participant small businesses will be subject to the APPs (as reformed by proposed Subsection 6E(1D) of the *Privacy Act*)
6. CDR data held by non-accredited parties who are "APP entities"[16] will be subject to the APPs, not the CDR privacy safeguards.
7. CDR data held by non-accredited parties who are not "APP entities" will neither be subject to the APPs nor the CDR privacy safeguards but only general consumer protections and law.

This has been made even more complex and unintelligible with subsequent "second stage" amendments released last week.[17]

The introduction of the concept of providing non-accredited CDR participants the ability to access CDR against the recommendation of the Open Banking Report provides a significant leakage point for CDR data to fall outside of the system, whereby consumers will, at a minimum, be provided fewer or lower standard protections or in some cases, no realistic privacy protections at all if or when a breach or problem arises out of the use or misuse of this CDR data.

[16] Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.

[17] Treasury Laws Amendment (Consumer Data Right) Bill 2018 (second stage) and Designation Instrument for Open Banking, https://treasury.gov.au/consultation/c2018-t329327

In fact, the draft CDR legislation is designed to encourage consumers to engage with the CDR regime with the promise of increased protections, all the while allowing this data to leak out of the CDR regime where lower or no privacy standards at all apply. In other words, the draft CDR legislation will facilitate incredibly sensitive financial and personal data to be handled by non-accredited parties with lower or protection for consumers.

This is unacceptable.

The introduction of the CDR for designated sectors are an explicit acknowledgement that the current APPs are out of date, no longer fit for purpose, and are generally weaker than required for a modern data based economy, i.e. the APPs are not good enough to provide the privacy protections that consumers require.[18] The Open Banking Report details an extensive list of modifications that will be required to boost the protections required for a modern open banking system. This includes:

- APP3 not requiring informed and express consent;
- APP 5 merely requiring reasonable steps be taken to notify consumers rather than having to notify; and
- APP 7 not requiring express and informed consent for direct marketing.

The Open Banking Report lists six changes that would be required.

Implementing the CDR alongside the APPs therefore implements multiple privacy standards. This will be confusing for consumers and industry alike. This is especially the case given the fact that as envisioned under the Act, sensitive personal financial data will be subject to these different standards in different circumstances and different stages of the data lifecycle: this is explained further below regarding financial data under the non-accredited data recipients section, below.

Financial Rights therefore believes that while designating sectors to establish and introduce data standards for the purposes of portability is sensible, the approach being taken by the Treasury to designate sectors for increased privacy protections needs to be reconsidered.

Financial Rights recommends that the CDR legislation should not be finalised nor implemented until the *Privacy Act* and the APPs are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.

In addition to the problems identified by the Open Banking review which demonstrate how the APPs are inappropriate for a modern, data based economy, there are other issues with the APPs. The last time privacy laws in Australia were comprehensively reviewed was ten years ago.[19] The way Australian consumers and businesses use and supply data has changed dramatically since then. Australians' expectations for privacy have also increased markedly, in line with increased awareness of the importance of personal data and increased breaches in their personal data. Add to this, significant international developments in privacy protections

[18] Pages 54-56, Recommendation 4.2 – modifications to privacy protections.

[19] ALRC, *For Your Information: Australian Privacy Law and Practice*, Report 108 , 12 August 2008. Available at: https://www.alrc.gov.au/publications/report-108

and the APPs stand as a relic of a former time and are in no way fit to address community expectations with respect to the use, security and protection of their data.

Finally, in examining the impact of privacy concerns arising from the use of big data technologies on the insurance sector, the Actuaries Institute highlighted further need to review the current APPs as they apply to the insurance sector. They state that:

> *The Government may want to consider whether any restrictions should be placed on what information an insurer may seek. It could require insurers to be more transparent about the use of data and whether it will be sold or passed on. It might also confirm the right of the insured to understand whether their social network footprint or internet browsing history is being used.*
>
> *Enhancing and maintaining individuals' confidence and trust in the way data is held and used is important, and is currently being explored by the Productivity Commission's inquiry into data availability and use. The security and confidentiality of these increasing volumes of information has to be maintained.* [20]

We believe that the government must consider these specific issues if and when the Consumer Data Right is applied to the insurance sector.

A ban on screen-scraping technologies

We note that the draft CDR legislation does not ban screen scraping and other technologies. Providing access to this 'screen scraping' technology can amount to a breach of the terms and conditions of a customer's bank account, and can put customers at risk of losing their protections under the E-Payments Code[21] This will impact harshly upon financially vulnerable consumers. These incredibly unsafe data access technologies have been banned in other countries like the UK. Without a ban on these technologies, there is very little incentive for businesses such as pay day lenders and debt management firms to become accredited under the CDR system and will be left to exploit Australians freely. Financially vulnerable people will of course continue to be desperate to access credit and will not concern themselves with the nuances of privacy protections to do so. If that means engaging with non-CDR accredited entities like pay day loan operators, financially vulnerable people will do just that.

Privacy by Design

Article 25 of the EU GDPR implements rules for data protection by design and by default.[22] Privacy by design is a proactive approach to protecting privacy during the design of a project and as well as throughout its life.

---

[20] Page 26 Actuaries Institute, The Impact of Big Data on the Future of Insurance https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf

[21] See discussion in the Final Report of the Small Amount Credit Contract Review, March 2016, at p. 76-77, available at https://static.treasury.gov.au/uploads/sites/1/2017/06/C2016-016_SACC-Final-Report.pdf.

[22] Art. 25 GDPR Data protection by design and by default

Privacy by Design was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian,[23] The principles were a part of a Resolution by International Data Protection and Privacy Commissioners in 2010; followed by the U.S. Federal Trade Commission's recognition of Privacy by Design in 2012 as one of its three recommended practices for protecting online privacy; and as mentioned, incorporated into the European Commission plans to unify data protection within the European Union.

There are seven foundation principles to privacy by design are summarised by the CPRC summarises as follows:

1. ***Proactive not reactive; preventative not remedial:*** *Be proactive rather than reactive, to anticipate and prevent privacy problems in advance.*
2. ***Privacy as the Default Setting:*** *Personal data is automatically provided with the maximum degree of privacy protection in IT systems or business practices.*
3. ***Privacy Embedded into Design*** *Consider how to embed privacy in the design and architecture of IT systems and business practices rather than treating privacy protection as a subsequent add-on feature*
4. ***Full functionality – Positive-sum, not Zero-Sum:*** *Accommodate all legitimate interests and objectives in a win-win manner, where privacy and security can both be achieved without unnecessary trade-offs.*
5. ***End-to-End Security – Full Life-cycle Protection****: Ensuring strong security measures prior to collecting the first element of information, as well as securely retaining data, and destroying data at the end of the process.*
6. ***Visibility and Transparency – Keep it Open:*** *Businesses practices and technology involved should be subject to independent verification, to assure stakeholders they are operating according to stated promises and objectives.*
7. ***Respect for User Privacy – Keep it User-Centric:*** *Take a user-centric approach by protecting the interest of individuals, for example: offering strong privacy defaults, appropriate notice, and user-friendly options.*

Embedding this approach into the CDR and any other broader re-thinking of the *Privacy Act* and the APPs is critical to ensure that all businesses demonstrates their respect for consumer data and personal information to provide greater security and privacy protections from day one.

Insurance and discrimination

As notes above insurers are using genetic testing technology in their underwriting. While a genetic test currently does not impact upon someone's ability to obtain health insurance, life and travel insurance companies are allowed to use this genetic test information because of the insured's duty of disclosure under section 21 of *Insurance Contracts Act 1984*.

[23] Information & Privacy Commissioner of Ontario, Privacy by Design, https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

Here, the insured has a duty to disclose every matter that is known to the insured and that they know to be a matter relevant to the decision of the insurer. The failure to share such information may be regarded as a breach of contract and result in an insurance policy being cancelled. This is not the case in other jurisdictions. The US, Sweden, Germany and France, all prohibit genetic discrimination.

The Financial Services Council representing life insurers and other financial service providers in Australia, however do have a Standard Genetic Testing Policy regarding the use of genetic tests in providing these insurance services. Travel insurance is however not covered by the standard.[24]The standard does not make up a part of the Financial Services Council's Code of Practice.

A self regulatory standard however is in our view not enough to protect the interests of consumers moving forward. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry have demonstrated that the insurance industry can no longer be trusted to self-regulate in the best interests of consumers.

We note that the Australian Law Reform Commission's 2003 Report *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC Report 96) found that:

> *at this time, there is insufficient evidence to justify a departure from the fundamental principle underlying the market in voluntary, mutually rated insurance in Australia, namely, equality of information between the applicant and the insurer. However, given developments in other jurisdictions, including the introduction of two-tier systems in some European countries, the Inquiry is of the view that the Human Genetics Commission of Australia (HGCA) should keep this matter under review.*

We strongly recommend that now is the time that the Government should step in and undertake a review of the use of genetic testing technologies in insurance underwriting and s 21 of the *Insurance Contracts Act*..

More broadly though, we believe that it may be timely to review not just the use of genetic information in insurance underwriting but the nature of discrimination and the exemption under the *Disability Discrimination Act 1992* (**DDA**) for insurers in an age of big data technologies

As the AHRC will be well aware, the *DDA* makes it against the law to discriminate against a person because of disability when providing insurance. The DDA also recognises that some discrimination may be necessary in insurance and subsequently includes a partial exemption for insurance and superannuation providers under s 46. Specifically it states that such discrimination must be based upon actuarial or statistical data on which it is reasonable for the insurer to rely upon. It also contains a general defence which may apply to providers where not discriminating would cause them unjustifiable hardship.

[24] https://www.fsc.org.au/resources/standards/11s-genetic-testing-policy-final.pdf

The AHRC has also produced a specific guideline for insurers and superannuation companies to assist better understanding of rights and obligations under the DDA.[25]

However the sector itself has already started a dialogue amongst themselves on the impact of new technologies on insurance and discrimination. We note that the Actuaries Institute in its 2016 Green Paper: raises a number of public policy implications that the Government needs to consider with respect to the impact of new technologies on insurance. In "dealing with the undesirable impacts of insurance pricing" the Actuaries Institute states:

> *Where appropriate, and in the light of prevailing community standards, Government could consider restricting the use of certain data on uncontrollable risks for pricing, whilst maintaining the principle of disclosure and avoiding the potential for consumers' adverse selection against insurers. An overseas example helps to bring these potential challenges to life.*
>
> > *Like Australia, Canada currently requires insurance applicants to provide the results of previously undertaken genetic tests to requesting insurers. The Canadian Institute of Actuaries constructed a model to assess the impact on companies and the public if underwriters were prohibited from accessing the results of genetic tests known to applicants. In separate studies for life (term) insurance and critical illness, they concluded that as a result of the genetics test prohibition the average claim rates within the term insurance portfolio were likely to increase by about 35% for males, and 60% for females in the age range 20–60; and that there would be a concomitant increase in term insurance premium rates. Critical illness claims would go up 26% if insurers were not allowed to use genetic test results for a selected six causes of claim.[26]*
>
> *This leads to the question of where society believes it is appropriate to draw this line of controllability, and what risks (or elements of risk) might fall under this banner? As an example, the EU has decided to disallow rating on gender in insurance. In Australia, despite gender and age being non-controllable, it is generally accepted as reasonable to price on them (subject to the pricing being based upon actuarial or statistical data on which it is reasonable to rely). As a society the question becomes important when insurance is unaffordable or unavailable.*
>
> *Some statistics may act as a partial proxy for race, e.g. certain genetic dispositions. Whilst it may be argued that increasingly many factors could in some way correlate with race (for example where you live and what type of food you purchase at the supermarket), there needs to be careful consideration by insurers specifically exploring the data and extracting these*

---

[25] Guidelines for providers of insurance and superannuation under the *Disability Discrimination Act 1992* (Cth) (revised 2016) https://www.humanrights.gov.au/sites/default/files/AHRC_DDA_Guidelines_Insurance_Superannuation2016.pdf

[26] *(W. (Bob) Howard, R., Canadian Institute of Actuaries, (2014) Genetic Testing Model: If Underwriters Had No Access to Known Results. Available at: http://www.cia-ica. ca/docs/default-source/2014/214082e.pdf (Accessed: 29 July 2016).*

links. Using such data for pricing insurance may be statistically valid but run contrary to anti-discrimination laws.[27]

And of course it is not just data that is a cause for concern in the discrimination space – it is the use of algorithms based on certain assumptions (as described above) that may embed discrimination into their decision making systems.

We believe given technological developments described in our submission and the proposals paper it is time to re-examine both s 21 of the *Insurance Contracts Act's* disclosure regime as it applies to genetic testing and the exemption of the insurance and superannuation sectors under s 46 of the DDA to consider whether such an exemption is warranted.

As noted, many jurisdictions have outlawed discrimination on the basis of genetic information – the same must be considered in Australia.

Ultimately the Australian government needs to consider the following basic question: Do we want to live in a world where insurers will continue to be able to discriminate on the basis of genetics and other personal information captured by insurers using powerful technologies that mine data?

Financial services and price discrimination

As noted above the use of big data technologies in insurance is likely to lead to increased granularity of risk profiling leading to great price discrimination. Many policyholders –in flood zones, those with genetic dispositions to certain diseases, those who brake too slowly when driving or those who have not installed a smart battery in their home - will have their risks assessed as so high that the price will either be prohibitive or insurers will simply decline to provide cover. This is very likely lead to significant financial losses when events occur that they cannot cover the costs.

The Government needs to examine the use of big data technologies in insurance and consider intervention in the insurance market. The Actuaries institute in its Green Paper, for example asserts that:

> *Government may want to provide [people priced out of insurance] with support, particularly if the risk could not have been reasonably avoided or mitigated. That support could be provided 'after the event' through grants or other financial support to those in need e.g. post-disaster compensation or 'before the event' by risk mitigation. Alternatively Government could make insurance affordable by:*
>
> - *Placing limits on premiums. Currently, the Australian Government restricts pricing and underwriting for insurance viewed as a "social good". Health insurance and Compulsory Third Party ("CTP") motor insurance are examples. This could be managed by requiring that a certain portion of an insurer's portfolio covers these high marginalised risks. Doing so would increase premiums for the lower risks.*

[27] Page 28, Actuaries Institute, The Impact of Big Data on the Future of Insurance https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf

- *Implementing risk sharing mechanisms so that the costs of high-risk customers are shared amongst all insurers in that market. Such an approach could assist when placing limits on premiums, mandating that insurers provide some level of cover for high risk groups or facilitating community insurance. Again, this would increase premiums for the lower risks.*

The Government could become the "insurer of last resort" for those risks that no insurer will cover or take part of the risk. For example, The Australian Government covers commercial property and associated business interruption losses from terrorism as administered under the Terrorism Insurance Act 2003. In New Zealand the New Zealand Earthquake Commission shares earthquake losses with insurers.

These are all policy interventions that require consideration by Government.

In the financial services sector more broadly, price discrimination will arise when low income consumers are likely to be unfairly charged higher amounts for credit, or be pushed to second-tier and high cost fringe lenders.

It is therefore critically important that regulators are empowered to keep tabs on a financial services sector that is increasingly fuelled by data. This means that regulators such as ASIC need be resourced and empowered to harness the FinTech revolution itself and use regulatory technology (or RegTech) to provide them the tools they need to monitor and regulate appropriately. Technology must be harnessed in regulatory monitoring, reporting and compliance and could be used to in numerous ways.

For example, RegTech could provide regulators with confidential and protected access to commercially sensitive algorithms and other black box technologies to examine automated decision making programs. This way they can interrogate such technologies more closely to identify price discrimination and discriminatory practices more generally.

As a rule, financial services providers across the board should be providing more and more data to regulators via RegTech systems to enhance regulatory monitoring. The first step regulators need to take is to develop template data requirements for each sector. For each source of data, the financial services provider would provide a name/description of the data, the source of the data and the use or uses of the data – pricing (including underwriting), marketing, defaults, claims settlement (in insurance), etc.

A periodic survey should be conducted (along with random surveys) to provide regulators with the basic overview of what data is being used by industry and what it is being used for. This information is essential for supervisors to respond to policy makers and to foster public discussion over potentially controversial types of data.

RegTech can also be used to develop market analyses that examine actual consumer outcomes in the finance services market. Regulators should be provided with detailed market monitoring tools with transaction detail data for everything from default data, claims, sales and quotes data to transaction information.

The information gathered by regulators could also be used to provide information to empower consumers and promote competitive markets. For example, claims data insurance could be used to provide claims ratios for consumers at point of sale. Interest rate practices could be provided to consumers to seek out better deals.

The information gathered via RegTech could also assist:

- evaluating existing and proposed public policies
- evaluating affordability and availability of financial services and products and

competition issues.

Recommendations

2. **The *Privacy Act* and the Australian Privacy Principles are reviewed and strengthened to reflect the needs of a modern economy based on access to and use of consumer data.**
3. **The EU GDPR should act as a model for consumer protections and regulation of consumer data and strengthen privacy rights and consumer protections.**
4. **The CDR legislation should not be finalised nor implemented until the *Privacy Act* and the Australian Privacy Principles have been reviewed and strengthened.**
5. **The CDR legislation must ban all screen-scraping and other unsafe data access, transfer and handling technologies.**
6. **The principles of Privacy by Design should be embedded in all legislative, regulatory and self-regulatory approaches to consumer data and the impact of new technologies.**
7. **The Government should undertake a review to regulate the use of genetic testing technologies in insurance underwriting and consider reform to s 21 of the *Insurance Contracts Act 1984*with respect to disclosure of such information.**
8. **The Government should review the *Disability Discrimination Act 1992* and reconsider the partial exemption for insurance and superannuation providers in s 46, in the light of new technologies.**
9. **The Government needs to consider policy interventions in the insurance market to ameliorate the impacts of new big data technologies in producing an insurance market which will increase the number of consumers who cannot afford insure or to which insurance is no longer available.**
10. **The Government must fund financial services regulators to increase their use of RegTech to identify discrimination, price discrimination and improve industry monitoring.**

Concluding Remarks

Thank you again for the opportunity to comment. If you have any questions or concerns regarding this submission please do not hesitate to contact Drew MacRae, Policy and Advocacy Officer, Financial Rights on (02) 9212 1386.

Kind Regards,

Karen Cox
Coordinator
Financial Rights Legal Centre
[redacted]