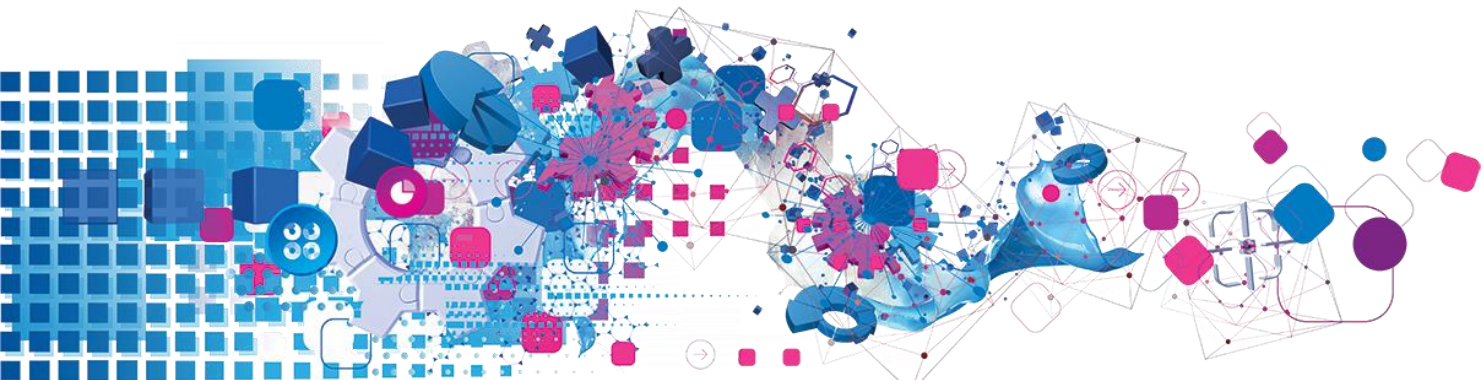
Economics Legislation Committee 15 May 2018

National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018

Questions on notice

For Senator Chris Ketter
22 May 2018



1. Broader use of data and privacy

a) Between current legislation and this proposed legislation – what safeguards exist about how CCR data would be handled?

Positive Data is regulated by Part IIIA of the Privacy Act 1988 (**Privacy Act**) which is supported by the Privacy Regulation 2013; the Privacy (Credit Reporting) Code 2014. In addition, most of the CCR obligations on Credit Providers (CPs) and Credit Reporting Bodies (CRBs) will be found in the National Consumer Credit Protection Act 2009 (Cth).

b) What purposes is CCR data allowed to be used for?

The permitted uses of CCR data are prescribed by the Privacy Act. Under the Privacy Act, authorised entities (i.e. credit providers) can request a copy of consumer credit reports. Section 20F strictly governs the permitted CRB disclosures in relation to individuals and the conditions by which the information may only be requested, with Section 21H detailing the permitted CP uses in relation to individuals.

Experian will only provide consumer credit reports to CPs and authorised entities that comply with the above and the consumer credit reporting system as per the Privacy (Credit Reporting) Code 2014 (Version 1.2).

Furthermore, under the Principles of Reciprocity and Data Exchange (PRDE) as set by the industry body Australian Retail Credit Association (ARCA), a CP signatory only receives information that they supply into the PRDE data pool. As stated on the ARCA website: "Credit Providers contribute the same information to all Credit Reporting Bodies with which they have service agreements, and Credit Providers contribute all of the credit information across each of their consumer credit portfolios. It is necessary to be a PRDE signatory in order to exchange PRDE signatory Consumer Credit Liability Information (CCLI) and Repayment History Information (RHI) with other PRDE signatories."

c) Will your companies be able to use CCR data (even if depersonalised) across other business elements?

Experian can only use and disclose CCR data (including de-identified CCR data) in accordance with the permitted uses set out in the Privacy Act, including section 20M in relation to de-identified credit reporting information. As such, our employees and by extension our clients in the Data Quality and Targeting area of our business do not have access to the CCR data held within the credit bureau.

d) Do you use depersonalised data, derived data etc. (for example, credit scores) and on-sell or combine this data with other data sources? Is there any legislative or regulatory barrier to prevent you from legally partnering with Google, Facebook etc. to legally provide "insights" to companies which in part are based on information obtained from CCR data?

In line with section 6N of the Privacy Act, Experian is permitted to collect, and hold, certain types of information about a consumer (i.e. "credit information") but does not combine this credit information with other personal information about the consumer as part of our credit services business.

Under the Privacy Act, derived data is subject to all the same restrictions that apply to the raw data. Accordingly, the restrictions in the Privacy Act and CR Code would not permit the use or disclosure (i.e. the 'onsale') of derived data by either the CRB or CP: except as set out in the Privacy Act.

Part IIIA also directly restricts a CRB's ability to use de-identified credit reporting information. Section 20M Privacy Act provides that a CRB that holds de-identified credit reporting information must not use or disclose the de-identified information except for the purpose of conducting research in relation to credit in accordance with rules made by the Australian Information Commissioner.

e) Credit providers and data

i) Will any credit provider be able to purchase credit reports on individuals? If not, which ones will be allowed to access reports? Why will they be given access?

Under the Privacy Act, CPs can request a copy of consumer credit reports however Experian will only provide consumer credit reports to CPs that adhere to the consumer credit reporting system as per the Privacy (Credit Reporting) Code 2014 (Version 1.2).

Furthermore, under the Principles of Reciprocity and Data Exchange (PRDE) as set by the industry body Australian Retail Credit Association (ARCA), a CP signatory only receives information that they supply into the PRDE data pool. As stated on the ARCA website: "Credit Providers contribute the same information to all Credit Reporting Bodies with which they have service agreements, and Credit Providers contribute all of the credit information across each of their consumer credit portfolios. It is necessary to be a PRDE signatory in order to exchange PRDE signatory Consumer Credit Liability Information (CCLI) and Repayment History Information (RHI) with other PRDE signatories."

ii) What in your view will be the kind of cost that credit providers will have to pay to access these reports? (a range is acceptable)

The commercial agreements we have with CPs are commercially sensitive and can vary – for example it can either be a fixed fee agreement or transactional (i.e. pay as you use). In addition, the price can also vary based upon the volumes being consumed and also the agreement may be for a bundle of service offerings.

iii) Under what circumstances could a credit provider request a report on an individual?

- **Only if the individual approaches the member and requests credit?**

- **Could a credit provider pay for a report if the member has had contact with, but not received a request for credit from, a credit provider?**

- **Could a credit provider purchase a report with no prior contact of the individual? (if so, could a credit provider purchase credit reports on everyone in Australia?)**

A CP can only request a consumer's credit report once the individual's permission is granted.

- **Could direct "cold call" marketing occur as a result of this legislation? Under what circumstances? What might the outcomes be?**

- **Given "credit scores" developed by credit reporting bodies are a derived number based on CCR data, is it possible that a credit provider could request a credit reporting body to contact individuals (e.g. via a mail out) within a given credit score range and invite them to apply for a particular credit product? Can this happen today? Could this happen if the CCR legislation is passed?**

Experian refers Senator Ketter to the Privacy (Credit Reporting) Code 2014 (Version 1.2) (Office of the Australian Information Commissioner): "Part IIIA restricts a CRB's use of credit reporting information to facilitate a CP's direct marketing. It does, however, permit a CRB at the request of a CP to undertake pre-screening of a list of individuals provided by the CP using eligibility requirements nominated by the CP".

Experian can only undertake pre-screening to remove individuals from a marketing list if, for example, the individual has defaulted and the CP states this is their eligibility requirement. The purpose of pre-screening is to ensure that marketing material is not sent to consumers who, because they already have defaults and other adverse information on their credit report, are unlikely to be approved if they take up the offer and apply for the product.

It is important to note that under the pre-screening process a CRB must not use any CCR data in the pre-screening – it is limited to using 'negative only' data (e.g. defaults, bankruptcy information). See section 20G (2) (c) – 'Use or disclosure of credit reporting information for the purposes of direct marketing'.

- **Could credit providers conceivably store credit reports on their own computer systems? Or are there electronic measures that stop the copying/storage of these reports?**

Experian cannot comment on behalf of CPs, however we note that CPs have an obligation to destroy or de-identify credit eligibility information it holds once it is no longer needed for any purpose for which that information may be used or disclosed by a credit provider (see section 21S (2) Privacy Act).

- **Can these reports be passed between employees within credit providers in your opinion?**

Experian cannot comment on behalf of CPs, however we note that the law strictly limits what a CP can do once they receive CRB or CRB derived information (see section 21S (2) Privacy Act).

2. Data security

a) What requirements are placed on your companies currently in terms of data security?

The safe and secure passage of data is paramount. Experian is trusted with securely managing more than 989 million consumer records globally. Once we collect data, Experian Credit Services holds the information in a local high security data centre.

In terms of data security practices, Experian follows ITIL to ensure overall support, zero downtime to data infrastructure. The Experian Credit Services data centre and systems are only accessible by authorised Experian employees who are specially trained in security and data handling policies and protocols to Experian Credit Services business standards and adhere to credit reporting obligations under the Privacy Act.

To ensure the data held is secure and protected from unauthorised access, Experian follows ISO 27001 standards and utilises industry standard encryption processes and technology.

This is translated into the controls that are put in place to ensure data is secured using the highest level of security while in storage, in transit and in motion to its final destination. This also ensures that access to personal information is only provided to those employees who need to have access in order to perform their role.

b) Do you have independent third party audits of your systems for both data security and proper use of data? Who are these reports given to? To what standards are they conducted against? Who pays for these independent reports? Please provide a recent report – acknowledging that sensitive elements contained in the report can be redacted.

Experian has engaged E&Y, KPMG and Booz Allen among others to conduct independent audits. These are on top of the annual and bi-annual penetration tests and also quarterly application codes integrity checks. Experian bears the cost of these independent audits to demonstrate its integrity and commitment to itself and clients.

c) What new requirements will be in this bill? Illion – you say in your submission that the addition of major banks withholding data on grounds of suspected non-compliance is superfluous – can you explain?

This question not relevant to Experian.

d) If there were to be a data breach at one of your companies – assuming this legislation is passed and the rest of the legislative and regulatory framework stays the same – what are the requirements on your companies to report the breach? When do you report? To whom? Is it made public? Who can make this decision? Are there different tiers of breaches that have different approaches? (e.g. are small breaches treated one way, large breaches another?)

Privacy is at the heart of what we do and the way we work. As a highly regulated business, we work closely with regulators and strictly comply with data protection laws in all countries that we operate in, and we remain vigilant when it comes to data security and integrity. This includes our own commitment to strict compliance regarding permissible uses of data.

In the unlikely event of a data breach incident, a crisis management committee (Gold Team) which comprises of the CEO, CISO, CIO will mobilise. The breach will be made public upon the advice of Experian legal counsel – please refer to the Notifiable Data Breach scheme (Office of the Australian Information Commissioner) that is now in place under Part IIIC of the Privacy Act.

Through Experian's Global Information Security Incident Response Plan (IR Plan) and all related security policies, Experian seeks to minimise the frequency of such incidents.

The objective of the IR Plan is to enable Experian to immediately respond to a data compromise in a manner that demonstrates appropriate due diligence; to protect the integrity of our system, defend against potential litigation, maintain confidence in the Experian brand, and ultimately preserve shareholder value and customer privacy.

Experian has a Global Cyber Incident Response Team (GCIRT) who are primarily responsible for executing, maintaining, and testing the IR Plan. GCIRT is further responsible for the coordination, management, and maintenance of the core processes surrounding Information Security Incident Management and is responsible for 24x7 response.

The IR Plan scope covers any information security incident which affects the confidentiality, integrity, and availability of Experian's information assets. The IR Plan will provide corrective action(s) for the compromise of Experian data.

An information security incident may involve any or all the following:

- Data Loss (Lost or Destroyed)
- Data Theft / Breach
- Unauthorised Access
- Exploitation of System / Application
- Lost / Stolen Devices
- Application / System Misuse
- Denial of Service / Impact to Availability
- Malware Infection

- Network / System Recon
- Phishing

i) What fines/penalties/legal action could result if a breach was to occur?

Privacy is at the heart of what we do and the way we work. As a highly regulated business, we work closely with regulators and strictly comply with data protection laws in all of the countries that we operate in, and we remain vigilant when it comes to data security and integrity. This includes our own commitment to strict compliance regarding permissible uses of data.

Experian refers Senator Ketter to the Notifiable Data Breach scheme (Office of the Australian Information Commissioner) that is now in place under Part IIIC of the Privacy Act.

e) Will this data be stored in Australia in each of your companies? Or will it be stored overseas? What regulations are required in each of these instances?

Once we collect data, Experian Credit Services holds the information in a local high security data centre. The Experian Credit Services data centre and systems are only accessible by authorised Experian employees who are specially trained in security and data handling policies and protocols to Experian Credit Services business standards and adhere to credit reporting obligations under the Privacy Act.

To ensure the data we hold is secure and protected from unauthorised access, at a minimum we utilise industry standard security and encryption processes and technology. This ensures that access to personal information is only provided to those employees who need to have access in order to perform their role.

Access is also provided to users and subscribers of the products and services we offer and any law enforcement agency with whom we are required by law to provide personal information.

f) What kinds of requirements will credit providers, and particularly the major banks be likely to place on your companies through contractual arrangements?

The high standards that ensure Australian banks and CPs manage consumer's data securely are regulated by the Australian Prudential Regulation Authority (APRA). APRA provides advice on these standards within its Prudential Practice Guides (PPGs) (234 and 235), which it explains are not "enforceable requirements", but rather advise on the regulator's "view of sound practice".

As such it is the responsibility of regulated Australian banks and CPs to "manage data risk in a manner that is best suited to achieving its business objectives" in line with APRA's requirements.

To maintain consistency of data security across the industry, Australian banks and CPs build security standards into their contractual agreements with consumer credit bureaus like Experian, which we are regularly audited against.

The result of this contractually-led data security arrangement is that the security standards of any of the more than 100 banks or CPs that Experian partner with in Australia become the default minimum standard that must be complied with. In fact, the market-driven data security requirements mean Australian credit bureaus' security procedures are consistently measured against the highest industry benchmark: policies and security controls adhere to global accepted standard e.g. ISO 27001, PCI:DSS.

Furthermore, many clients have the right to audit Experian upon agreed notice. Clients may also have rights to view security testing results, for example penetration test results and code integrity checks.