Australian Government

Australian Small Business and Family Enterprise Ombudsman

17 January 2019

Manager
Consumer Data Right Team
Structural Reform Group
The Treasury
Langton Crescent
PARKES ACT 2600

By email: data@treasury.gov.au

Dear Sir/Madam

DRAFT PRIVACY IMPACT ASSESSMENT – CONSUMER DATA RIGHT

We commend the Draft Privacy Impact Assessment (PIA), which provides a rigorous framework for the assessment of impacts on privacy associated with the Consumer Data Right (CDR). Our submission highlights additional risks and governance processes we believe should be captured within this framework.

It is likely that over time much of the CDR data processing will be automated through use of algorithms, customer facing web portals and APIs. These have the potential to increase risks of accidental data sharing and/or vulnerability to mass data phishing where fully automated systems are unmonitored. The PIA should specify that the Data Standards Body will seek to address security and transparency standards for algorithms and APIs, together with the data security standards already identified in relation to data storage and transfer of data.

The requirements for a *registered person* and/or CDR Participant should seek to minimise the risk of fraudulent companies being established and registered to phish for data with the apparent sanction of the CDR system. This risk does not appear to be identified in the Draft PIA.

The privacy protections and penalties will only be effective if there is a strong 'cop on the beat' to investigate problems and enforce compliance. The current proposals excessively rely on enforcement action being triggered by customer complaints following notification of their CDR data being shared. It is unlikely that customers will have the information, nor technical ability, to determine that their CDR rights have been breached. It seems likely that notifications to customers may be misunderstood, ignored or lost in junk email.

It would be desirable for metadata relating to each instance of CDR data exchange to be reported to a highly secure and confidential record keeping authority designed to hold transaction records such as Data Holder, Data Recipient, Customer, Date, Type of Data Transferred. Access to this data should be permitted only for such purposes as identification of rogue operators phishing or receiving CDR data, tracking of aggregate statistics, identification of trends (such as percentage of foreign CDR transfers), and tracing of customer data history in the event of dispute or investigation.

Thank you for the opportunity to comment. If you would like to discuss this matter further, please contact Jill Lawrence on 02 6121 5312 or at jill.lawrence@asbfeo.gov.au.

Yours sincerely

Kate Carnell AO
Australian Small Business and Family Enterprise Ombudsman

T 1300 650 460 E info@asbfeo.gov.au
www.asbfeo.gov.au

Office of the Australian Small Business and Family Enterprise Ombudsman
GPO Box 1791, Canberra City ACT 2601