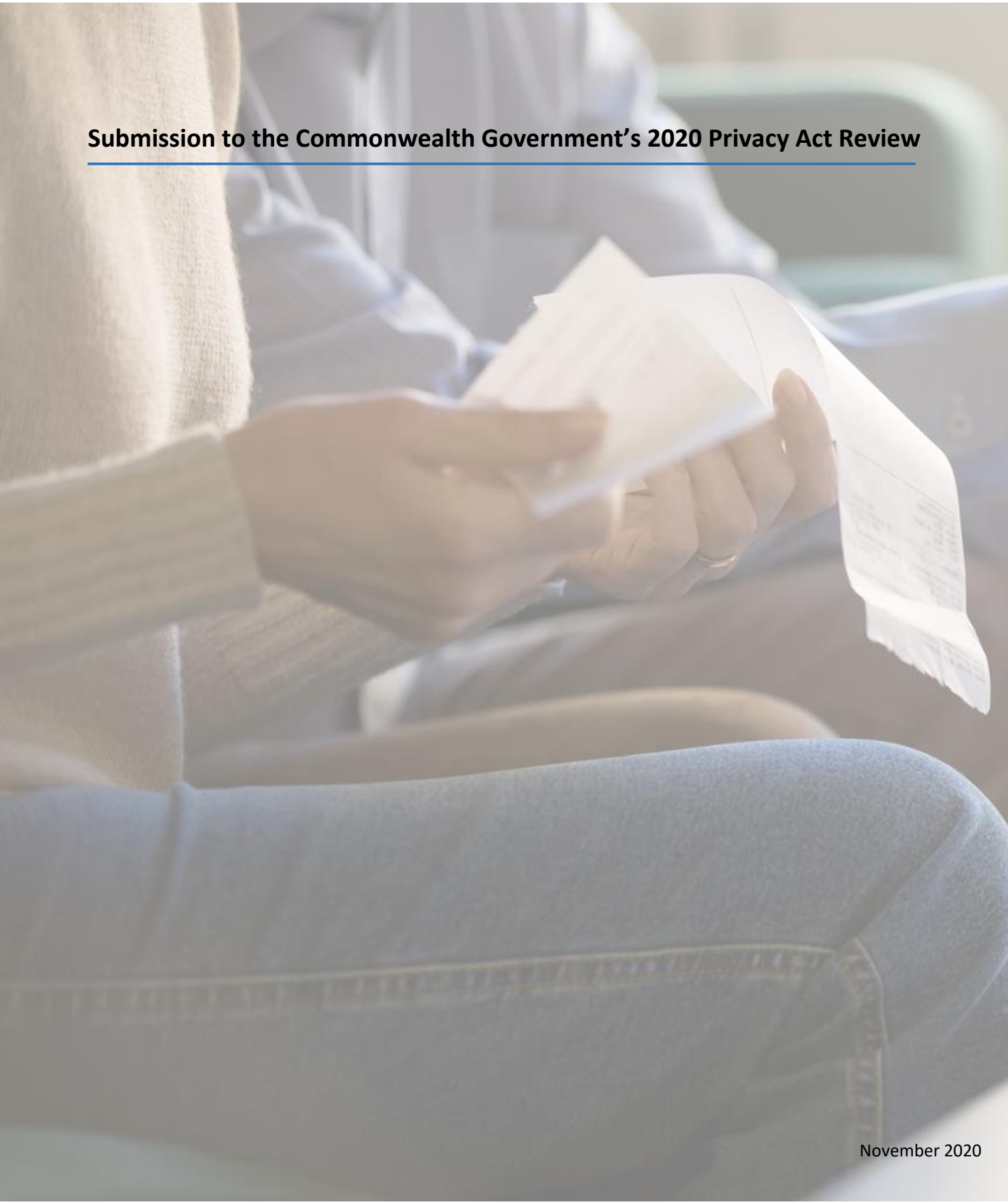
national identity and cyber support community service



Submission to the Commonwealth Government's 2020 Privacy Act Review

November 2020

Introduction

IDCARE congratulates the Government on reviewing the Privacy Act 1988 (Privacy Act). Drivers from technology and global commerce, including digital identity innovations, as well as the increasing amounts of personal information collection, commodification, and their exploitation all warrant a timely reflection on Australia's privacy laws and community expectations. It is not an easy task, and historically a topic that can attract quite extreme views that can dominant sensible discussion and consideration. IDCARE notes that the Credit Reporting Code is not within the current terms of reference, presumably because of the most recent amendments. This in our view is a mistake, as the Act and the Code are intertwined and each day our community engagements bear witness to shortfalls in its practical operations that do little to advance the community's privacy standards. We look forward to the next review of this Code to provide clear examples of these shortcomings.

This submission highlights our distinctive lens on the identity and cyber security environment. As part of the response and support services offered by IDCARE, we receive reports from members of our community directly impacted by events where privacy has been breached and cyber security measures have failed. Thus, IDCARE is uniquely placed to inform this legislative framework as we actively engage with individuals impacted by data breaches, as well as the organisations responsible for the exposure and exploitation of Personal Identifying Information (PII). From this perspective, we have focused our submission on the areas that we feel our views would most contribute, including:

- The small business exemption;
- The impact and effectiveness of the Notifiable Data Breaches (NDB) Scheme;
- The definition of Personal Information;
- Emerging digital identity and the protection of non-traditional PII;
- The need for the General Data Protection Regulation (GDPR).

To assist with our contribution we have compiled from our National Case Management Centre anonymised case studies provided with the consent of individuals that serve to inform the review process.

We welcome a reviewed national framework, which takes into consideration the balance between the personal identities of Australian residents and an organisation's responsibility concerning the collection, protection, usage and sharing of personal information. The value of privacy today, where individual's data and metadata have become tradable commodities, cannot be underestimated. Privacy is a universal right and there is a shared responsibility in how personal information is handled by Government agencies and businesses of varying sizes. This shared responsibility is emphasised by the increasingly pervasive threat of actors that seek to illegally obtain and exploit private information domestically and abroad. However, it is not merely the existence of the threat itself and their actions that should give rise to discussions and reflections about privacy as a universal right. The threat actors, the consequence of which IDCARE deals with each day, is merely antithesis of why such information in any number of forms it takes should be identified as private.

Our Service

IDCARE was launched in 2014 in Australia by the Commonwealth Minister for Justice as our national identity and cyber support community service. The organisation embodies what can be achieved when Governments and industry listen to the needs of our community in building a response service that addresses the emotional and pragmatic issues confronting people when their personal information is exposed and misused. Our role is unique and not one that duplicates others, nationally or globally. To afford transparency and consideration of this submission, it is important to recognise that IDCARE is a registered not-for-profit organisation and Australian charity.

We are not a Government agency, nor do we benefit from receiving annual government appropriations despite doing a large amount of work performed on behalf of governments and their impacted staff and customers. Our funding streams, albeit a constant challenge, come from a few organisations in industry and government that demonstrate leadership and genuine concern for the well-being of their staff and customers, and who take an ethical stance that referrals to IDCARE should be accompanied by a financial contribution to assist our charity cover the costs of delivering our community services. We simply could not survive as an organisation without this funding support. Sadly many government and private sector entities do not share this ethical view, so as an organisation we do what we can with what we have to support the community in responding to threats to their privacy.

Since 2014, IDCARE has responded to over 275,900 client engagements from members of the Australian and New Zealand communities who have experienced cyber-enabled crimes either resulting in the compromise of personal and account information or its misuse and exploitation. The demand for our service continues to grow exponentially, with a growth of 75% in the last year alone (October 2019 to October 2020). Despite this growth, our client satisfaction rating remains the strongest of any organisation in the Australian privacy response system (average 8.7 out of ten). We believe the reason for this enduring community sentiment is because we have found the right mix of empathetic care with the provision of the most up-to-date pragmatic response advice aimed at reducing harm for each person tailored to their needs and concerns. It is not uncommon for community members to feel powerless, unheard, and for their response efforts to feel unattainable when their personal information exposed and exploited. IDCARE could double in size and still operate at more than a hundred percent capacity in delivering our services to the community, so high is the demand. This remains a constant challenge and one that continues to demonstrate the need and value of our service and ensuring we continue to advance volunteer programs and other measures necessary for many Australian charities and contemporary community support services.

Turnover and size as a precondition of compliance.

Historically the estimated compliance burden, that is the cost of compliance, for businesses with an annual turnover of $3 million or less has been the stated reason for excluding most within this cohort from needing to comply with Commonwealth privacy laws. Exclusion based on size limits an individual's rights, protection measures and persistent risks from threats. Increasingly IDCARE has noticed a growing volume of businesses exempt from current Privacy laws request assistance in responding to events that would otherwise have met a serious risk of harm threshold. The same can be said of some State and Territory government agencies that do not have equivalent notifiable breach provisions. Put simply, the threat environment is not overly selective of its target based on an organisation's annual turnover or whether it impacts a particular jurisdictions, but by law, the responses remain quite selective.

Presently the size of the business or the entity's jurisdiction does have an influence on the risk to the privacy to the impacted person. It is our observation that this influence presents principally from two perspectives. First, the actual ability to reasonably protect personal information against risks to the personal information it collects is influenced by its size and available resources. Second, the risk of exploitation persisting and remaining untreated for impacted persons will be contingent on the person being notified of such risks. Notifiable breaches are just that, notifiable, where the real work of protecting against future exploitation and misuse rests almost entirely on the actions and inactions of the impacted person. Without such knowledge, the impacted person remains exposed and IDCARE knows that the numbers of organisations operating outside of the Privacy Act 1988 are growing in terms of those experiencing breaches that would otherwise be

notifiable for entities operating under this regime. Both observations are important considerations for policy makers when examining the merits of extending the reach of the Commonwealth's privacy legislation.

Criminal exploitation of personal information is both discriminatory and indiscriminatory in nature. Discriminatory attacks, such as "spear phishing" or "whaling" are planned efforts to exploit through biographical information an organisation's systems and information holdings. Common efforts include access to payroll and invoicing decision-making processes and email systems. Indiscriminate efforts include the proliferation of malware that may commence with a specific organisation in mind, but then seem to behave in ways that are akin to biological viruses, spreading to hosts without any pre-vetting of their size or status.

The impacts on individuals for the non-disclosure of breach events should not be underestimated as the following two case studies highlight:

CASE STUDY 1: Unknown Privacy Breach

'Sharon' received a debit card in the mail she did not request. When her bank informed her there was an email address and phone number linked to her accounts that wasn't hers, she did a credit report and discovered multiple accounts had been set up using her driver licence. She has no idea how someone had been able to obtain a copy of her driver licence as she is careful when sharing this information. If it was a result of a data breach, she would "really like to have known". "I would have taken action immediately," she said.

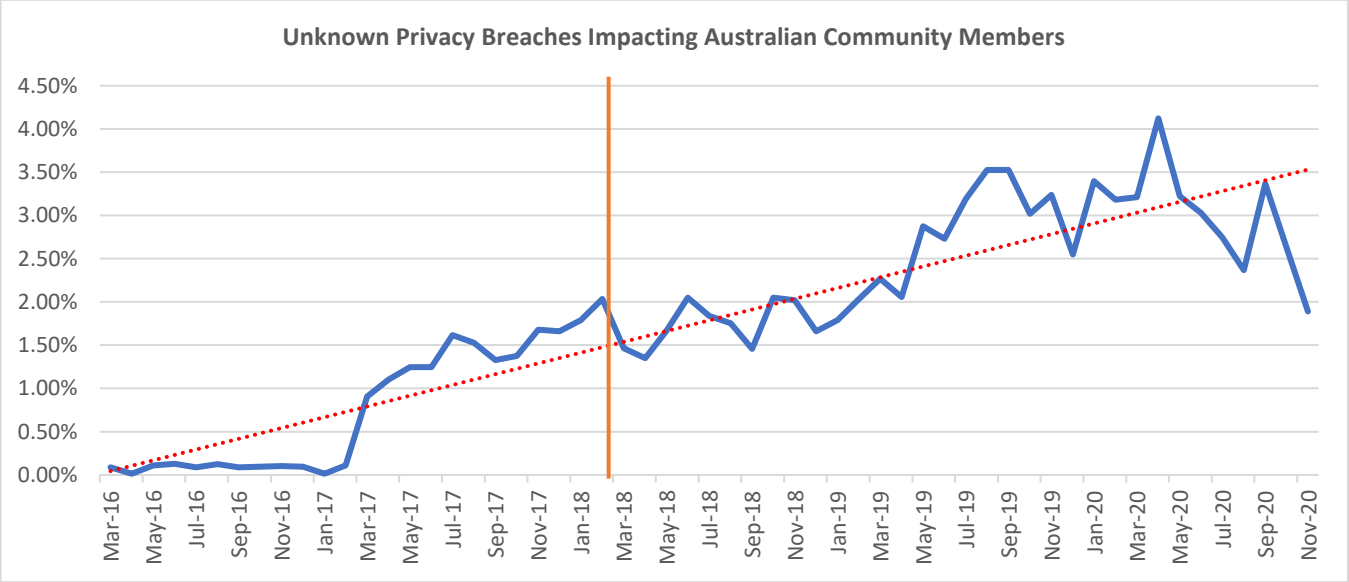
CASE STUDY 2: Dealing with the Unknown

'Jo' is careful about securing her identity documents. She does not take them around with her and she does not give them out easily. When she started receiving messages from her Telco concerning a new plan she had never requested, it was a case of "why are they sending me this". When Jo investigated it, she discovered someone had been using her driver licence to create accounts in her name. She has not been able to establish how the scammer got hold of her driver licence. In her mind, the only logical conclusion was her details had been involved in a data breach somewhere and she had not been informed. This has made her frustrated and stressed as she feels she had little control over the situation. If she had been informed of a breach, she would have taken protective measures immediately.

IDCARE has seen a steady growth in the "unknown" compromise category from community reports into our National Case Management Centre. This "unknown" category effectively means that the community member is experiencing the exploitation of their personal information but has no knowledge of how the criminal obtained their information in the first instance. It is true to say that in some of these cases the individual themselves may have unwittingly exposed such details, such as via an infected device or email account, but for many others this may not be the case.

IDCARE's Cyber First Aid service provides community members with a health check on their device and online accounts for signs of compromise and exploitation of personal information. It advances what the "local IT shop" does, and focuses on the key things we know cybercriminals and malicious actors do in exploiting a person's information through their device and online accounts that would otherwise not show up in an anti-virus check. In many cases where clients have reported an "unknown" compromise and completed our Cyber First Aid treatment process the cause of the exploitation discounts exposure relating to persistent threats on their device. In other words, these cases tend to point to some other external breach event that remains

unreported to the person. The following graph highlights the portion of community engagements IDCARE has experienced from individuals that have no awareness of how their personal, account and credential information was exposed in the first instance. A portion of these will relate to events caused by unreported data breach events.



The orange line in the above graphs represents the commencement of the Privacy Act 1988 amendments to reflect the introduction of notifiable data breach scheme. The trend line reflects the growing rate of community engagements from individuals that are not aware of how their personal information was stolen by criminals that have subsequently misused and exploited such details.

The total financial loss value for these unknown events was approximately $180 million. IDCARE does not hear from every community member. We estimate that only around one in ten people who experience such events reach our specialist staff. From our knowledge and testing of the response system, around two thirds of these losses could have been prevented if the individual impacted was forewarned at the time of the initial breach of their personal information. Even if only half of these events related to data breaches involving organisations currently outside of the notifiable data breach scheme, the annual loss value prevention saving from reports to IDCARE alone would be in excess of $40 million a year. If we were to consider what IDCARE does not see, this figure would be much more.

A further consideration relates to the opportunity costs associated with lost productivity from individuals and their employers when having to respond to such events. IDCARE knows that for individuals that experience breaches of personal information where the cause remains unknown, they will typically spend on average three to four weeks longer responding to such events. Some of their work will be necessarily focused on trying to understand what information was compromised and how this may have been breached. This is likely to place even greater financial costs to employers and the economy more broadly as employees experiencing unknown compromise events will need to take time from work to address risks to their breached personal information.

This reinforces the importance for policy makers in their re-consideration of whether annual revenue or turnover is an appropriate and natural dividing line between notification and compliance with the Act or not. On the basis of the growing rates of identity theft and misuse that remain unexplained from the victim's

perspective, in addition to their financial and broader economic costs to the Australian economy, IDCARE does believe it is timely for Government to reflect on how all businesses respond to such events. Even if there were consideration of a "Privacy Act lite" version for businesses under the current revenue / turnover rate to limit the perceived compliance burden, the impacts on the individual that confront breached personal information could be profound.

A secondary consideration was the efforts relating to compliance and associated costs. It is true that many small businesses would be unlikely to collect much personal information. Many would use transaction systems that encrypt data from customers as the main intersection with a customer's information. The requirements under the pandemic to capture personal information, including name, phone or email, and address has witnessed several innovations being deployed to the market, such as the use of apps and QR codes, that can further advance privacy safeguards in some instances. However, these practices are variable, and certainly anecdotally the capturing of information has presented concerns from the community as to awareness of privacy, security, and accessibility by business owners collecting such information for the first time. COVID-19 response measures in and of themselves may present a good opportunity for small businesses to be engaged on broader privacy and security dialogue. They present a largely common thread for many of Australia's small businesses and a starting point for their consideration of privacy rights and protections. In our view, there is no better time to engage small business on the topic and learn from their experiences and ideas on privacy, security, compliance and needs.

IDCARE holds a firm belief that knowledge of "reasonable" measures and threats to privacy is largely held within government, either because of reporting measures that capture such events or because of government capabilities that detect adversaries and their methodologies. Many millions of dollars are committed each year to government agencies to advance our country's resilience and response to threats, such as malicious cyber actors, that pose a direct risk to entities that seek to comply with privacy laws. The imposition of these regulations and failure to comply must continue to be proportionate. If government agencies, with the resources of government, continue to be breached of the personal information it holds, it is a reasonable question to ask as to what chance Australian small business owners have at preventing such attacks? Knowledge of the risk and knowledge of its treatment and response, is not something that should be retained only with government. It is our strong belief that a networked threat to our community needs a networked response. This includes not just advancing a legislative requirement to ensure organisations adopt reasonable security practices and take reasonable measures to treat risks, but that the tools and capabilities to achieve these outcomes are also shared and supported from government to these organisations. This is vitally important for small businesses that may be considered under amendments to the existing legislation. Efforts to encourage small business to enhance their cyber security posture have had mixed results. But the market and awareness of the threat is evolving. Market incentive measures should be considered, rather than purely the negative impacts from non-compliance. But these should not be at the cost of government agencies needing to play a much more direct and tangible role in sharing the knowledge about such risks.

The same can be said of notifiable data breach reporting. The regulator is aware of standards of response. If this is similar to the window of IDCARE, it is fair to say that standards are variable, as are the treatments afforded to impacted persons. Public guidance on these from the regulator would be welcome for both responders, but more importantly, for the public and those impacted. There is general confusion amongst many responders on topics that involve what measures are effective, what can be done proactively ahead of notification (such as informing parties where identity misuse can occur), and the changing nature of risks

relating to serious harm. For example, if a Victorian driver licence was compromised in a notifiable data breach, VicRoads will not change the driver licence number. In effect this means that the impacted person from that breach will carry a significant and enduring identity theft and misuse risk going forward. However, if a New South Wales RMS driver licence was compromised by Service NSW, the driver licence number in NSW may be eligible to change. This act significantly reduces the risk of identity theft and misuse involving the impacted person in this situation. This example highlights both the complexities involved in responding to data breaches, but also the variability in response treatments.

Assessment and notification challenges and opportunities.

Since IDCARE's commencement we have worked alongside more than a thousand organisations that are having to respond to data breach events as well as tens of thousands of people who receive notifications and express concerns about what these exposures mean. Given the very nature of our community service we know intimately what the real risks are to individuals when their privacy information is exposed or exploited. We know intimately what "good" looks like from the impacted person's perspective and equally what "bad" looks like. We have found a shift in approaches and market influences since the introduction of the notifiable breach provisions in February 2018. The market now is dominated by law firms, some of which appear to have no real connection or knowledge of impacts on individuals, creating issues around conflict and the appropriateness of response. This disadvantages the community, and without stronger regulation of the response sector, IDCARE fears that responses to such events into the future will continue to be variable and harmful to impacted persons.

We do not believe that a General Data Protection Regulation equivalency in Australia is warranted in its entirety. There are some useful considerations around the rights of data subjects and the inclusion of most organisational types, but in the context of breach notifications, the application of GDPR in some cases has proved harmful to the Australian community. For example, the requirement for organisations to notify the relevant European privacy regulator within 72 hours well ahead of Australia's requirements, particularly at a time when not all is understood about the actual breach, not only creates a double reporting requirement, but in many cases in our view a distraction for responders, unhelpful speculation and emotional harm to impacted persons. Quite usefully, the regulator in such cases in Australia could play a representative role in such matters. In other words, Australian entities that are caught up in the GDPR breach notification scheme would benefit from having the regulator in Australia act vicariously as their European equivalent. The same could be said of Transman arrangements where New Zealanders are captured within Australian breaches and vice versa. The thinking here relates to the need for organisational responders to spend less time worrying about multiple regulator notifications and more on initial treatment, assessment and notification to impacted persons. The same could extend to the prudential requirements with the Australian Prudential Regulation Authority. Notifying a regulator does nothing to address the risk to impact persons. Whilst we don't advocate the removal of any such measure, we do advocate for a re-think on whether one could act as a point of focus on behalf of many.

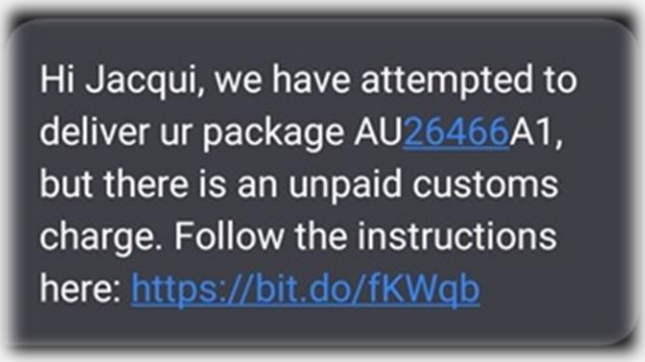
IDCARE's engagements with clients who have experienced compromise or misuse of their personal information that was exposed through a data breach event has provided valuable insight into our submission. Clients have expressed sentiments of relief once they become aware of the specifics surrounding their identity compromise, in particular the source of exposure and attributes that were exposed.

In instances where the source of compromise is unknown to the client, blame is typically attributed to unrelated entities. Furthermore, a lack of knowledge on which credentials have been involved in the misuse of an individual's identity can impede their response, resulting in an inadequate or incomplete response plan.

The identification of a person of today and tomorrow.

In addressing the questions outlined in the privacy review under the 'Definition of personal information' section (Question 4 – additional protections in relation to de-identified information), it is our view that de-identification should not be used as a means to circumvent the destruction of personal information by APP entities. Despite the commercial benefits that personal information may possess for certain organisations, de-identification is required such that the involved individuals may not be easily identified in the event of a data breach. It is our view that the de-identification standard is not adequately suited to countering the current methods employed by cybercriminals engaged in the harvesting of Australian PII. We are of the belief that if personal information is preserved for some commercial or security purpose, that anonymisation (irreversibly treating the data so that no individual may be identified) is favoured over current de-identification methods. This would best combat the emerging methods of discovery IDCARE is witnessing in the exploitation of information that would once have been assumed to be quite innocuous.

We find that common reasons for belief among victims of phishing scams are the direct engagement by scammers who have their personal details on hand. SMS scams that address Australian citizens by their name or other PII, such as the example below, often increase the scam's apparent legitimacy and the chance of engagement and further identity compromise.



Exposed contact information can be easily identified by criminals with specialised tools and enough motivation, even in instances of "de-identified" information. Paid and free services exist that return all social sites, forums and other accounts associated with a given email address or username, creating pathways for further exploitation that could be employed by fraudsters.

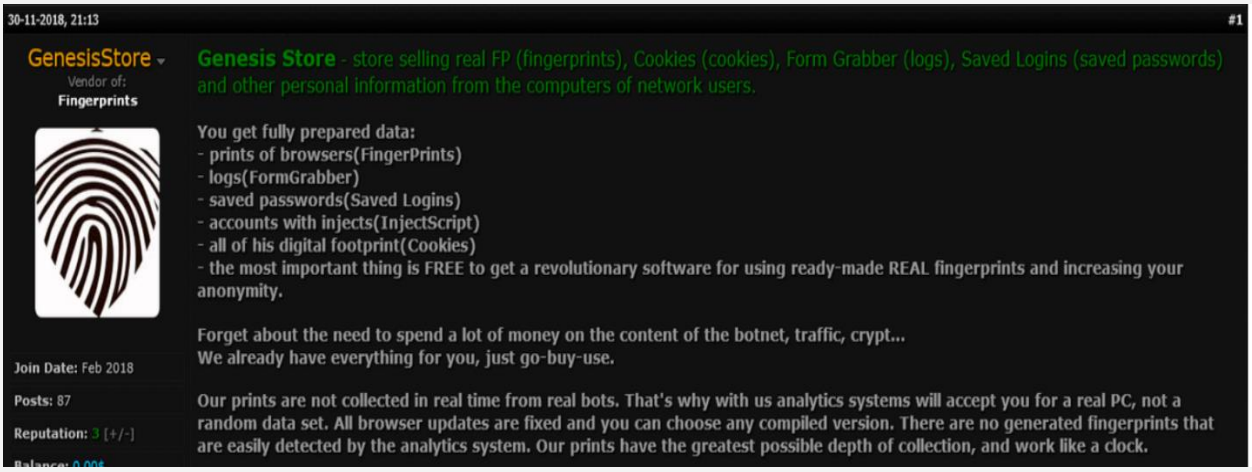
When the Privacy Act was enacted in 1988, the concept of a digital identity scarcely existed. The rise of the internet and the ubiquity of digital platforms into nearly every facet of life has fundamentally shifted the definition of identifiable personal information.

It is becoming more common place for institutions to create detailed digital profiles or 'fingerprints' of customers to aid in the prevention of fraud. This process combines the system attributes, unique to a user's device, and behavioural analysis to create a detailed individual profile. Technical data, such as IP addresses, device identifiers, location data, screen information, browser plug-ins and other technical information are used in this process and are not covered by the Act.

Unfortunately, cybercriminals have been successful in circumventing these controls by capturing both the traditional personal information and the digital fingerprint. In the past two years, IDCARE analysts have noted a rise of dark net and surface net markets listing these combined attributes of Australian customers for sale. This information is then purchased and used by cybercriminals to exploit individuals. Expanding the definition of personal information to include these digital footprints may help in preventing the exposure of these details and may enforce the implementation of stronger protection measures to guard them.

Section 2A of the Act seeks to balance protection of the privacy of the individual with the interests of entities carrying out their functions and activities. In the experience of IDCARE, the lack of definition and protection of personal information in the Act skews the balance away from the individual. It is IDCARE's view that including inferred personal information and technical information based on a user's interaction in the digital system would address this imbalance.

IDCARE supports Recommendation 16(a) of the Australian Consumer Commission (ACC) *Digital Platforms Enquiry:* The definition of personal information in the Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.[1] Examples of markets and sites such as GenesisStore and Russian Market, that list for sale compromised traditional personal information covered by the Act, combined with technical information not clearly covered by the Act (see below).



1 https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf Page 458.

Concluding Remarks

A review of the Privacy Act 1988 is a welcome development from Government. The approach taken to circulate a discussion paper and invite submissions will contribute to a focussed new strategy better equipped to address the evolving digital landscape and balance the inherent privacy expectations of individuals. We hope you find our thoughts and ideas useful in considering the many questions you have posed in the discussion paper. We acknowledge this is a complex domain, made more difficult by the fast pace with which technology evolves. We would welcome the opportunity to expand further on the specific areas we feel most qualified to comment.