Submission to the review of Privacy Act.

November 17, 2020

Submitted by Corch, private citizen and Director of Shogun Cybersecurity

To whom it may concern,

I am an information security and privacy consultant, and I have worked in the field for the entirety of my career which spans two decades. I make this submission both personally as an Australian citizen who highly values their privacy, and as the representative of my business, Shogun Cybersecurity, which provides services relevant to privacy and the Privacy Act. My profession has granted me the opportunity to see firsthand the poor state of Privacy practice and regulation in Australia, and also the benefit of understanding the true value of what is at stake. It is my sincere belief that the apathy within the general community regarding privacy, and particularly online privacy, is born from a lack of appreciation for the damage which inadequate privacy can do to us personally and to society in general. If they truly understood the consequences of the current status quo, they would be deeply concerned.

I will briefly address each of the topics to be considered by the review, as listed in the issues paper released by the Attorney General's Department, but first I would like to begin by addressing what I believe to be the most severe and egregious failure of the current Privacy Act – that it is not really about privacy at all.

Privacy is the right of an individual or group to keep their affairs to themselves, to participate in society without being under constant surveillance, and to control who is permitted to collect information about them. The Privacy Act and Australian Privacy Principles in their current form do not define or imply any such right, nor do they provide protection from invasions of privacy. The Privacy act merely defines a regulatory regime under which the collection and use of personal information is broadly permitted, and as such its true function is to legitimize the invasion of privacy.

The Privacy Act has done Australians a great disservice in that it has reframed the debate around privacy from being about the right of individuals to live free from constant scrutiny and be in control information about them, to being simply about how their information is handled. The clear implication is that the government believes people have no legal right to privacy and that regulation is the best they can hope for. It strongly implies that the Privacy Act was written not to protect the privacy of individuals, but to protect the vested interests of corporate Australia and preserve their ability to collect, use, and abuse personal data for their own ends.

Actual protection of privacy, as it applies to personal information, requires one thing above all else – the ability for individuals to control who is allowed to collect and retain their personal information. Without this ability, individuals have no privacy. They are at the mercy of any entity with the capacity to collect information about them, with virtually no recourse under the current regulatory regime as to how that data is used or who else it is shared with. It defies belief that a framework as explicitly named as the Australian Privacy Principles does not actually contain anything that empowers an individual to prevent this from happening.

I acknowledged that the APPs do currently contain some provisions intended to allow individuals to interact anonymously or pseudonymously "where it is practical to do so", however in practice this loophole is widely abused. In every instance where I have complained to an entity about unnecessary collection of PII, I have been dismissed with responses claiming this exemption. In every case, their justification was weak as

best, but as an individual I have no ability to take legal action under the Privacy Act, and the OAIC has neither the time nor resources to handle complaints of this nature.

We live in a time when information has been weaponized and people's PII is being used against them and society more broadly in ways that are becoming increasingly difficult to perceive, let alone defend against. Look to the influence of social media on elections and spreading social unrest for all the evidence you need. In this respect, protection of privacy has become a matter of national security, the potential for mass collection and automated analysis of personal information to facilitate manipulation of public opinion and corrupt the democratic process cannot be ignored or dismissed.

If the Privacy Act is to become an effective tool for people to protect their privacy in today's age of mass surveillance (by both commercial and government entities) and advanced data analytics, it must at the very least define a legislated requirement for entities to obtain informed consent before they are permitted to collect information about an individual. It must also define penalties of sufficient deterrence and an enforcement regime which is not hobbled by inadequate government funding.

If the current situation is allowed to continue, the fundamental concept of privacy will soon disappear, and Australians will lose the ability to even have privacy. In its place we will be left with constant anxiety, fear, and eternal distrust of every institution we must deal with on a daily basis.

Scope of the Privacy Act

Definition of personal information

I consider the current definition of "personal information" to be generally sufficient, but use of the term "reasonably identifiable" injects ambiguity into the concept which leaves too much up to individual interpretation. A more concise definition which is less discretionary would better serve the Australian public.

Current Exemptions

Exemptions to the Privacy Act are overly broad, and outdated. They perhaps were appropriate when the Act was first created and information was not primarily stored in digital format on networked computers where it can easily be stolen by hackers, but as they stand now the exemptions pose a significant risk to the Australian public.

The current situation with COVID contact tracing provides an excellent case study – thousands of small businesses which are exempt from the Privacy Act are now required to collect PII for contact tracing purposes. They have no experience in handling PII, and are doing so with either complete disregard or ignorance for OAIC guidance. Every café I have been into has a clipboard with a list of names and phone numbers on it, clearly visible for any customer to come in and take a photo of with their smartphone.

When I have tried speaking to a manager about this I have been rudely dismissed on every occasion with comments like "feel free to go elsewhere". This attitude is emblematic of the SMB perception of Privacy – they believe they have no obligations at all because the Act doesn't apply to them, and they don't care about complaints because there are no consequences for their behavior. In other circumstances a customer might be able to take their business elsewhere, but under COVID contact tracing requirements, everywhere is the same, there is no commercial or regulatory motivation to be better. The public are blindly writing their names and phone numbers on these clipboards for anyone to see, simply because they are desperate to sit down with friends over a meal.

Another unjustifiable exemption is the one granted to political parties. If anything, they should be held to a higher standard than anyone else because of their influence on the democratic process. This exemption must be removed, there is no justification for its existence in the first place. Politicians are not above the law, neither should political parties be.

Generally speaking, I do not believe any exemptions to the Privacy Act are useful or warranted. With modern technology, the power and pervasiveness of personal information means we cannot, as a society, afford to let anyone collect PII without being subject to the law. There is an argument that law enforcement and security agencies to retain some exemptions to avoid compromising their duties to protect public safety, but even if we accept this, outside this limited scope there is no justification for anyone to be exempt.

General Permitted situations for collection, use, and disclosure of PII.

I have partly addressed this point in my opening remarks. I do not believe that general collection, use, or disclosure of PII should be allowed by just anyone who has the ability; A more privacy-centric approach would instead define a specific list of circumstances under which each activity is permitted, including what information can be collected/used/disclosed, and by/to whom. At the very least, there must be some pre-existing relationship and/or informed consent between the individual and the collecting entity before collection is permitted.

Vested interests would argue such an approach is impractical, that it is too hard to define such a list, or that it would be too complicated, an unsustainable burden on their operations. This is a strawman argument, in reality what they mean is it would upset the cost-benefit equation for them to make their continued abuses of PII cost prohibitive. That being the case, the rule would work exactly as intended.

The minimum acceptable alternative to the above approach would be to define a broad list of situations in which collection/use/disclosure of PII is NOT permitted. This would be a substantial improvement over the current vaguely stated and poorly enforced wording around anonymous interaction “where practical”. For example, a person who buys a batch of event tickets for their friends must not be required to provide names and/or other PII for all attendees; there is no justifiable reason why a venue needs this information other than for their own commercial benefit.

Does the Privacy Act effectively protect personal information and produce a practical and proportionate framework for promoting good privacy practices?

As stated in my opening remarks, the Privacy Act does not actually protect personal information, it only regulates it. This is not the same. Nor does it promote good privacy practices, because it is not really designed to; the intent is not to stop or limit the collection of personal information, but to provide a framework under which any and all collection, use, or disclosure is explicitly allowed as long as one follows the rules. This is self-defeating and directly opposed to good privacy practices.

Notification requirements

Notification requirements for collection, use, and disclosure of PII are of little value by themselves. It does not help a person to know that their information is being collected when there is literally nothing they can do about it. In many cases, it’s not even an option to avoid using a service or participating in an activity. Social structures “demand” that everyone uses Facebook for example. Buying things online requires agreeing to store T&C, and even going into an actual store requires agreeing to be filmed by CCTV.

Value aside, the notification requirements have resulted in wordy and complicated privacy policies which no one reads because they are boring, difficult to understand, and ultimately don’t communicate anything of practical use to the individual. I believe many entities have abused these circumstances to create privacy policies which are actively intended to discourage individuals from reading them.

Consent Requirements and default privacy settings

The very concept of consent when it comes to privacy and personal information has been distorted well beyond its original meaning. Consent requires a real choice between plausible alternatives, but in today’s world where our lives are ruled by smartphones, apps, and social media networks, there is no longer a plausible alternative for people who do not consent – you simply get cut off from the rest of the world.

When the options are “agree to terms of service to be spied on” or “be digitally cut off from all your friends and family”, the majority of people will choose the former and feel their privacy is a an unfortunate but necessary sacrifice. This kind of abuse of power dynamics cannot be allowed to continue if any kind of privacy is to exist online.

Lack of plausible alternatives notwithstanding, the current rules on obtaining consent are so limited as to be useless. In the most cases, an entity does not need to obtain consent, express or implied, to collect personal information. This in and of itself effectively renders most of the Privacy Act meaningless, as it deprives an individual of any agency over whether an entity can collect data on them, regardless even of whether the entity has any kind of relationship with the individual. In this way, the Privacy Act has legitimized the exact opposite of privacy as law.

For the Privacy Act to be useful to individuals in any meaningful way, it must require that an entity obtain express consent before collection of personal information is permitted. Additionally, there must be safeguards that prevent the requesting entity from denying service based on this refusal. Admittedly, this is a complicated problem, as many services require provision of personal information by their nature. However, there are many more which do not require it, but it has somehow become acceptable for them to demand it, or to demand much more than they legitimately need, leaving the individual with the false choice of acquiescing or going without.

For example, there is no legitimate reason for a nightclub to be scanning and keeping records of patrons’ government issued IDs (e.g. drivers licenses). Arguments are put forward saying it is necessary for safety so that police can identify people that were present in case there is an incident. Aside from the fact that this argument is based on an outright lie pushed by law enforcement agencies that making police work easier is always greater benefit to society than preservation of individual rights, it clearly violates the most fundamental concept of privacy – that people should be able to go about their business without having to identify themselves every time they go somewhere.

Even the current Privacy Act, in all its impotency, says a person should be able to deal anonymously with a business unless it is impractical to do so. It is not impractical in this circumstance; it just means that the business wouldn’t get to keep tabs on the demographics of people coming through the door, police might have to do some actual investigating rather than relying on private business operators to hand them all the answers.

For consent requirements to have any meaning, individuals must have the ability to say no to the collection, use, and disclosure of their personal information without impacting on their ability to access the products and services they need to work and socialize. There must be a legislated requirement for vendors, services providers, and other organisations to facilitate engagement without requiring people to identify themselves or provide other personal information.

Default privacy settings are also a false choice, at best they provide an individual with a false sense of control over how their information is used. Typically, they only allow a person to decide which users can see their information – friends, everyone, etc. They do not allow a person to decide not to provide personal information, which third parties will get access to their information, or how their information can be used. These tools further serve to reinforce the incorrect perception that privacy is about how people handle your information rather than who you let have access to it.

Overseas data flows

In my experience, the Privacy Act has created much confusion about what was allowed with regards to sending and storing PII outside Australia. There is certainly a strong argument for requiring entities to keep PII about Australians within Australia, however from a practical standpoint it is almost impossible to track this, let alone guarantee. The proliferation of multi-national cloud services with opaque data storage

systems means that most organisations have no means to even determine whether any PII they hold remains in Australia or not. It's entirely possible that a third party to a third party somewhere in the service provision supply chain exports the data in ways that are invisible to the organization that is responsible for the data.

Any regulation of overseas data flows must be matched by transparency reporting requirement such that users of online services can clearly and easily determine how and where a service provider stores its data and what third parties have access to it. In practice this would likely be difficult to enforce.

Erasure of personal information

As with the right to deny collection of personal information, the right to demand its erasure is a critical component of any effective regulation of real privacy. This is especially true in cases where the individual has no relationship with the collecting entity (in which case the information was collected without consent), where the relationship has been terminated (e.g. deleting an online account), or where it has "expired" after a long period of inactivity (e.g. an account which has not been accessed in over 12 months).

Currently, there are no restrictions on how long an organisation may keep an individual's PII, as long as they can come up with some vague reason as to why the organisation still needs it. For example, a person who applies for a job but does not get it may have their resume retained by the employer indefinitely under the pretext that the organization needs to keep track of previous applicants. If the applicant objects to this, they have no means to force the employer to delete their CV from their system even though there is no on-going relationship between the two.

Should individuals have direct rights of action to enforce privacy obligations under the Privacy Act

Absolutely and without question. Privacy is a property of individuals, it should be enforceable by individuals, not left up to a poorly resourced regulator who does not have the inclination to get into costly legal battles with wealthy international tech giants. Additionally, groups of individuals should be able to lodge class actions to enforce obligations and penalties under the Privacy Act against entities which have failed to meet their obligations, or caused harm to individuals as a result of a data breach. Perhaps this would finally provide a meaningful deterrent to prevent unnecessary collection and abuse of personal information by corporate interests.

Should a statutory tort for serious invasions of privacy should be introduced into Australian law.

This kind of provision would further serve as a valuable deterrent for unnecessary collection and blatant abuse of personal information that is rife today, and is one of the key things missing from the current regulatory regime around privacy.

The impact of the notifiable data breach scheme and its effectiveness in meeting its objectives.

The NDB scheme was a step in the right direction, but the exemptions to the Privacy Act for small business have hampered its effectiveness, and the reluctance of the regulator to pursue penalties has given the scheme and the regulator a reputation as a toothless tiger in many circles.

As a someone who consults with SMBs on information security and privacy, I initially had good traction with clients in getting privacy risks onto risk registers, but in time these risks were watered down in severity as it became apparent to the client that the true probability of any intervention from the OAIC, let alone significant penalties, was actually close to zero. With this change in perception, the motivation of businesses to be proactive in addressing information security from a privacy perspective effectively disappeared.

The effectiveness of enforcement powers and mechanisms under the Privacy Act and the interaction with other Commonwealth regulatory frameworks

As alluded to under previous points, the enforcement powers under the Privacy Act provide little value in terms of deterrent. They are rarely used to their full extent, and their use is generally restricted to the OAIC which is insufficiently resourced to handle complaints and launch enforcement actions.

The desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws.

I do not think that such certification schemes provide much value in terms of real assurance. They tend to be tick-box compliance exercises that can be easily passed without having to demonstrate actual capability and on-going activity. For example, many organisations have documented policies and procedures for compliance reasons but in practice they don't actually follow them. Unless a scheme can be put in place to measure compliance based on actual day to day activities on a continual basis (not just once a year, or even once a month), such a certification is only going to provide individuals with a false sense of security.

This concludes my submission. I appreciate the consideration of the Attorney General and the opportunity to contribute to the debate on privacy.

Regards,

Corch
Managing Director
Shogun Cybersecurity