# Privacy 101, for people who are new to privacy

Hey get ready people, it's almost Privacy Awareness Week!

OAIC's theme for 2019 is 'Don't be in the dark about privacy', while OPC NZ and OVIC's theme is 'Protecting privacy is everyone's responsibility'. No matter which slogan you prefer, the point is to spread awareness of the privacy message.

Much like an infectious toddler let loose in a childcare centre, we here at Salinger Privacy are doing our bit by scattering our privacy expertise all over the populace in little droplets of knowledge. We've got a webinar explaining privacy for IT professionals, a free webinar with the IAPP on Privacy by Design in Privacy Law, an article about liability for privacy breaches by rogue employees in the May edition of the *Law Society Journal*, and here, a foundational explainer for anyone new to privacy.

In this Privacy 101 post we're going to cover what is privacy, what is personal information, what privacy laws actually do, and when consent is needed.

Feel free to share this Privacy 101 for the edification

of your workmates, your family, or even the person sitting next to you on the bus. Go on, raise awareness!

Here goes…

**What is privacy?**

The first thing to know about privacy law is that mostly when we talk about privacy law we are talking about only one aspect of privacy. There is no neat definition of what privacy means. Some people call it the right to be left alone. Some people equate privacy with secrecy, solitude, or anonymity. Others think of it as control over who sees our information. All of these factors do come into play, but privacy is a very broad, and ill-defined concept.

When we deliver privacy training, we tend to break down the concept of privacy into four categories. These four categories are not set out in law and they are not black and white rules; there is a lot of overlap between them. But when people talk about something having a privacy element to it, they are probably referring to at least one of the following four things:

- informational privacy: the appropriate handling of information about you, aka 'personal information';
- communications privacy: the confidentiality of your communications, which can be invaded if

someone you did not authorise was to read your private mail, or intercept your phone calls;
- behavioural privacy: the autonomy of your behaviour, which can be impacted by surveillance or monitoring; and/or
- physical privacy: the autonomy of your body and the solitude of your territory, which can be impacted if someone touches you without your permission, or intrudes on your personal space or personal time.

Anything that impacts on any of these four aspects of our lives, we might think of as a privacy issue.

However when we start to think about privacy *law* in Australia, we are really only concentrating on the first category of privacy, which is the privacy of *personal information*.

**What is personal information?**

I have often found that people who work in information security, or people who have a lot to do with American companies or American businesses, use the phrase PII. PII stands for Personally Identifying Information. In the UK and Europe they use the phrase' personal data'. In Australia we use the phrase 'personal information', as do privacy laws in New Zealand and Canada.

Basically they all mean roughly the same thing: information about a human being, where that human

being is clearly identified or might be identifiable.

(Exactly what makes someone *identifiable* is contested, with differing legal tests and interpretations of the related concepts of *de-identified* or *anonymous* data, but let's leave that aside for another day.)

But in a nutshell, privacy laws regulate how certain types of data, described as something along the lines of 'personal information', is handled.

**What does personal information include?**

One of the common questions we get asked about the scope of privacy law is whether things like IP addresses, MAC addresses, or information about devices, is personal information.

This has been a contested area of the law for many years, but is increasingly so in this world of the Internet of Things, because information about *things* can be linked back to a human being who controls that thing. There have been cases which turned on this issue, such as the Grubb v Telstra case which sought to answer the question of whether or not information about calls made to or from a mobile phone, or messages sent to or from a mobile phone, is 'personal information' – i.e. whether it is information solely about the phone, or also information about the person who is using that phone.

Similarly, the Waters v Transport for NSW case turned on whether data about the movements of an Opal Card is personal information about the person using the card. (Answer: Yes it is.)

So with the Internet of Things, data that can be collected from different devices may start to show a pattern of a person's behaviour. To the extent that the data is about the behaviour of an identifiable person, it should be considered 'personal information' just as clearly as the laws regulate information about someone's name, home address, or bank details.

**Is it only 'private' information that's regulated?**

A common fallacy I hear about the scope of personal information is that personal information is only information that is 'private'. In fact the words 'private' and 'public' rarely come into privacy law. Information is either about a person or it's not. Whether or not that information is already publicly known is a separate question.

The scope of what's covered by the definition of 'personal information' (and thus, what is regulated by privacy law) is very broad. It is not only what you might consider to be 'private', sensitive or embarrassing, but also information that might be publicly known, such as a person's name or job title, or publicly observable, such as gender or eye colour.

Within most Australian privacy laws (yes, there are multiple privacy laws, because most of the States and Territories have one or two laws each, in addition to the federal *Privacy Act 1988*), the law starts with a definition of 'personal information', but then may also have a sub-set within that of what's known as 'sensitive information' or 'sensitive personal information'. This sub-set is often then subject to some slightly tougher rules about how you can collect, use or disclose that information. The kind of information that you typically (though not always) find in the definition of 'sensitive' information is personal information that is about a person's health or disability, ethnicity, religion, sexuality, criminal history, political affiliations or trade union membership. The law applies tougher standards to these categories of data because typically these are the kinds of information that might be used to discriminate against an individual. Unfortunately, this notion of 'sensitive information' is easily confused with data classification schemes which also use the word 'sensitive', but to mean something else.

**What do the privacy laws require us to do?**

Privacy laws regulate both data flows and data governance. They do so by laying out a number of 'privacy principles'.

Data flows are regulated to the extent that privacy principles set the conditions under which personal

information can be collected, used or disclosed: the what, how, and why.

The rules around collection of personal information first regulate the *what*. They typically require that personal information can only be collected if having that data is reasonably necessary in order for the organisation to pursue a lawful purpose, related to the organisation's legitimate activities.

There will usually also be some rules about the *how* of collection, for example requiring that personal information be collected fairly and transparently, directly from the person who is the subject of the information.

The main reason for which the organisation is collecting the personal information – the *why* – should be thought of as the 'primary purpose' for which that information can also be *used*. Privacy principles typically allow the information to be used for the 'primary purpose', but also for a directly related secondary purpose, within the reasonable expectations of the individual.

An example would be a patient who has come into a hospital with a broken leg. The primary purpose for which personal information about the patient is going to be collected will be to diagnose and treat their broken leg, and manage their stay in hospital. A directly related secondary purpose for which their personal information might also be used internally

could be to issue the patient with an invoice, or could be to commission a quality assurance review of the orthopaedic unit. A directly related secondary purpose for which their personal information might be *disclosed* (given to a third party) would be sending a referral to the patient's physiotherapist for further treatment after they are discharged.

However the default position in privacy law is that using or disclosing personal information for any other secondary purpose is generally not allowed, unless an exemption applies. 'With the individual's consent' is one such exemption, but consent is not always a pragmatic solution, for the reasons explained below. You will usually find exemptions on grounds to do with law enforcement or national security, to prevent serious harm, to comply with another law, or to enable research in the public interest.

The other area of focus for privacy principles is data governance.

Data governance includes the need for transparency, amongst other matters such as enabling people to access the personal information held about them, and to seek correction of that information where appropriate. It also refers to having a privacy compliance program in place, with appropriate pathways for people seeking to make a privacy complaint or report a data breach.

Proper transparency includes having a Privacy Policy, and giving notice to individuals about how their personal information will be collected, used or disclosed. Giving notice is not the same as seeking consent.

**So when do we need consent?**

When thinking about data flows, my starting point is always to think about whether or not an organisation has the legal authority to collect, use or disclose an individual's personal information. The precise answer will depend on which privacy law/s apply to that organisation, but as noted above, typically privacy principles will offer multiple options for legally collecting, using or disclosing personal information. Only *one* of those grounds will be 'with consent'.

So you don't need consent to do most things. Consent should only be necessary if you are planning to do something not directly related to the primary purpose for which the personal information was collected from the individual in the first place, or sometimes (depending on the exact privacy law you are subject to) if you are planning to collect 'sensitive' personal information – and no other exemption applies.

But if you *do* need to rely on consent as the basis on which to authorise your collection, use or disclosure of personal information, make sure you know what

consent means, and how to get it in practice.

Under Australian privacy law, for consent to be valid, as the legal basis on which an organisation can collect, use or disclose personal information, it must have five elements: it must be voluntary, informed, specific, current, and given by a person with capacity.

Of these five elements, the most commonly misunderstood is the *voluntary* aspect. To be considered voluntary, a consent must be a proactive choice exercised by the individual. A valid consent must be an unequivocal 'yes' from a person who was given a genuine choice to say 'no' (without suffering any detriment), and where the default position is 'no'.

What does that mean in practice? Consent can't be 'opt out'. It can't be a condition of doing business with you. And consent must be revocable; it must be as easy for someone to later withdraw their consent as it was for them to give it.

So consent is only useful for authorising data flows if your business process can cope with a whole bunch of people saying no, or saying nothing at all, when you ask them the question: "Hey, can we please also do X with your information?"

A collection notice is not consent. Your Privacy Policy is not consent. (A Privacy Policy is not

magic. It cannot authorise you to do anything that the privacy principles don't already allow. Your Privacy Policy is solely there to inform people, in general terms, how you handle personal information. So don't ask your customers to acknowledge, agree or consent to your Privacy Policy. It's pointless.)

Clicking on mandatory T&Cs is not consent. Offering an opt-out is not consent. Pre-ticked opt-in boxes are not consent. You cannot gain, infer or imply your customer's consent to something simply because you mention it in T&Cs, a collection notice or your Privacy Policy.

So make sure you have separated out your collection notices from your consent forms and your Privacy Policy, and know when each one is needed and what they should include. They are three different things, serving three different purposes. (Check out our Compliance Kits for templates of all three if you need assistance.)

**Want to know more?**

We hope you have enjoyed this Privacy 101. Want more privacy knowledge?

Salinger Privacy has privacy training options from bite-sized webinars to professional certification programs, as well as online privacy awareness training modules. Plus stacks of useful resources in

our Compliance Kits. Or contact us to see how our privacy specialists can assist your organisation.

Happy Privacy Awareness Week.

*Photograph (c) Shutterstock*