# ACCANect 2018

**Session 8: 11:30 – 11:50am**

**Office of the Australian Information Commissioner – Relevant issues update**

**Presenter: Angelene Falk, Acting Australian Information Commissioner and Acting Privacy Commissioner**

**In April, the Office of the Australian Information Commissioner (OAIC) began an investigation into a privacy breach affecting Facebook. In this session we will receive an update on the progress of the investigation and address what rights consumers have when it comes to their data along with other important work of the OAIC.**

**11:50am – 12:00pm Q&A**

JULIE McCROSSIN: my apologies, I couldn't come to everybody who

wanted a question, we have quite a

tight show and I'm doing my best and lunch will be a tiny bit shorter

so I can give you more questions, but ladies and gentlemen if I

could ask Angelene Falk to head towards the chat pit of fun, shoes

from the office of the Australian Information Commissioner and

indeed is the acting Australian Information Commissioner and acting

privacy commissioner, in fact I'm prized I'm allowed to tell you her

name, she'll give us an overview of current issues including an

investigation into privacy breaches affecting Facebook and the right

of consumers, so please welcome Angelene.

ANGELENE FALK: Thank you very much and good morning. Thank

you to Teresa for having me here today to present. I'm no longer

the acting Australian Information Commissioner or privacy

commissioner, I was appointed a couple of weeks ago, thank you

Julie. A three year term, and an opportunity I hope to continue to

shape the privacy landscape. In terms of what I want to talk about

today, I was reflecting on the conference theme in term of

confidence in the connected world, and there were many things

raised by Berin the previous speaker, I think, around how we ensure

confidence from a cybersecurity perspective but also in terms of

how individuals and consumers can understand how their personal

information is being handled. And we do operate in such a

connected world now that this issue of consumer confidence is

central not only to the economic wellbeing and also the innovative

potential that personal information brings, but also in the way that

we handle it that recognises that personal information is about us.

So one of the things that's entrenched in the Federal privacy Act

that I regulate under is this multifaceted approach to privacy. The

Act recognises that personal information is a human right, that it's

an inalienable right and one that needs to be protected and

promoted. At the same time, we need to have a free flow of

information, to provide the convenience that we've all become

accustomed to so how do we strike that balance and ensure that we

achieve both? This week we saw some international developments

and it reminds us of not only the domestic landscape but the

international privacy landscape that we're operating in. That also

reminds me that I had some slides and I don't seem to have a

clicker. I might just pause there if that's OK?

JULIE McCROSSIN: There we go. Thank you.

ANGELENE FALK: Very good and it's already there. The work's done

for me in terms of what I want to talk to you about this morning.

We saw this week that my - one of the things you might have seen

in the paper is that Google challenged a decision of my counterpart

in France who ordered that Google should apply the right to be

forgotten, the right to delete personal information, not only within

France but more globally to avoid the issue of people using other

services and circumventing that right. Google has challenged that

and it does remind us of the fact that personal information knows no

borders and one of my regulatory challenges is to ensure that the

personal information of Australians is protected wherever it flows.

So in that context I want to give you a sense of the international

landscape. Many of you plight be aware of the general data protect

regulation that came into effect across the European Union in May of

this year. And it certainly has brought to the fore a global

conversation around privacy. There's a focus on consent and there's

also rights such as the right to be forgotten, the right to object, and

a data portability right. And some of those we're seeing manifest

within the Australian domestic context. There's also important to

recognise that the Australian law has many synergies with the

GDPR, both laws take a privacy by design approach, and the issue

that was raised with the doll and I didn't get to see the video earlier

but the comments that were made by the previous speaker I would

define as privacy by design, so we can build in privacy protections

by ensuring we're only collecting information that's necessary for

particular products and services and that safeguards are built in.

Both the international law and the Australian law have that as

central concepts. It's also important to appreciate that global

landscape for businesses who might be in the loom, those who

operate in the EU or provide services to the EU are required to

comply with that law. And closer to home, domestically one of the

big developments has been the notifiable data breaches scheme that

came into operation in February this year, and that does require all

businesses and Australian Government agencies to notify consumers

where there has been a breach of the their personal information,

that's likely to result in serious harm. And also to provide

information about what consumers can do to try and mitigate

against further harm occurring. They're the two things that I'd like

to give some focus on. I also wanted to reflect on the community's I

think expectations of regulators, and we've seen I think quite a lot

of criticism of regulators with the Royal commission, and other

public forums that have occurred this year, and there's certainly an

expectation to be effective and efficient and also to utilise the full

range of regulatory powers available and I think that's right.

Certainly, the approach that I'm looking to take. I also wanted to

just reflect back a little bit on the landscape that we're in and also

my time at the office so I've been in privacy for over ten years and

when I first started the first iPhone had just been announced,

Twitter had its first birthday, YouTube was turning two and

Facebook has been open to the public for just a few months, so now

if we flash forward to today, many of you will be aware that I

opened an investigation into Facebook in April of this year, following

allegations that potentially over 300,000 Australians' data was

potentially misused. And that is certainly I think elevated

community expectations of privacy and this issue about how our

information is used in secondary uses or to whom it's disclosed to.

You might be aware that the UK information commissioner's office

has an extensive investigation into Facebook and that in July this

year, my counterpart Elizabeth Denham announce her intention to

between Facebook $500,000 pounds which was the maximum fine

under the UK law at that time. Under the GDPR those fines will

increase significantly to 4% of annual global turnover, so it's quite a

significant change. But whatever I think of the outcome of my

investigation into Facebook, it's certainly I think elevated this

conversation and I think it's wonderful that today and tomorrow

there's going to be I think themes of privacy that are going to

resonate throughout your program. I'd like to talk a little more then

about those community attitudes which I think define the way in

which both business needs to approach personal information

handling but also can inform us as consumers and our constituents

in terms of the kind of approaches we need to take to ensure that

our perm information is handled appropriately. One key element of

good privacy practice is to have meaningful privacy policies and

notices, so privacy policies are not just a formality, they're a

transparency and communication tool, they should tell consumers

about how the organisation is dealing with their personal

information, in a broader sense. And they should be supported then

by plain language notices that are contextual and the previous

speaker spoke about Apple and the fact that just in time

notifications that occur when you want to access particular apps that

then ask you for your permission in order to do so. So last year we

conducted a community attitudes to privacy survey and we found

that almost two thirds of Australians agree that they didn't regularly

read privacy policies, there's been some more recent research from

the Consumer Policy Research Centre that has found that people are

at least reading privacy policies once in the last 12 months so we're

hoping that things are starting to improve. But it does - the privacy

law does really require both consumers and businesses to be

engaging in this space actively so businesses needs to make it

easier for to us understand how our information is being used, and

at the same time consumers need to being active in term of making

some informed decisions and choices about how their information is

used. There's another interesting study from the Norwegian

consumer council and they recently analysed privacy practices after

large international companies including Google and Facebook and

you might be interested in their report, it's called deceived by

design and concluded that consumers are being steered into sharing

vast amounts of perm information through default settings. There

are issues, that the business community needs to reconsider. And in

privacy law in Australia, really it's only necessary personal

information that should be collected and that fundamental principle

about data minimisation only collecting what's necessary in order to

deliver a service, is also a security mechanism because you can't

lose what you don't collect in the first place. Same time consumers

need to understand what information is being gathered about them

and not only because it's a consumer expectation or a compliance

issue, but it goes beyond compliance and it goes back to that issue

around consumer confidence and consumer trust. And there is some

evidence to suggest that if businesses are not dealing with personal

information in the way that aligns with consumer expectations that

consumers Ma may take matters into their own hand so our survey

did show that 58% of Australians will avoid dealing with a business

in order to protect their data, 44% would refrain from using an app

on a mobile device and 8% said they'd provide false personal

details. I want to just put this slide up which is a snapshot of privacy

regulation in Australia and it's really to draw out those - the issue

I've touch on so far around the requirement of transparency, having

the policy, having a notice that speaks to consumers, but also

there's principles around direct marketing and many of you will be

aware that there's a requirement that if an entity is providing direct

marketing material they also need to have a prominent notice that

allows you to on the out of that kind of material. There's a number

of rhymes under the privacy law which seem to give consumers

control over how businesses are using their personal information.

Security is a key principle and I'm going to talk about the notifiable

data breaches scheme a little more in relation to that but I also

want to draw attention to some other laws that I have a regulatory

role under that relate to the telecommunications space the in

particular so many of you might remember a couple of years ago

the Government introduced mandatory data retention laws for law

enforcement purposes that metadata had to be retained by

telecommunications and I've got a regulatory role to conduct

assessments of the telecommunications providers' handling of that

information and how it's secured. Also want to give you a sense of

the work of the office for those who may not be as familiar with it.

We provide a service to the community in terms of a call centre and

we deal with over 20,000 calls a year in relation to privacy and also

to access to information issues. We deal with complaints from

individuals, so many complaints already go to external dispute

resolution teams such as the telecommunications industry

Ombudsman, those that are not resolved there come to my office

and we seek to resolve them through conciliation and where that's

not successful then I can investigate and make a binding decision

that's enforceable in the Federal Court. These are some of the

regulatory powers and one of the powers that's yet to be used is an

able to go to the federal court to seek civil penalties of up to $2.1

million for repeat or service breaches of privacy. To date we've

entered into a number of enforceable undertakings with entities in

term of getting some systemic changes for consumers and there's

three that I just want to draw your attention to that you might be

familiar with. The Red Cross blood service data breach that occurred

in 2016 where what happened was the Red Cross had a third party

provider looked after their website and it became open to the public

and sensitive health information was revealed. And one of the big

lessons from that was the way in which the Red Cross responded to

that and the fact that they were very transparent in relation to what

had happened, took responsibility and then worked with my office in

term of building in a good strategy to ensure it didn't happen in the

future. The Ashley Maddison case which was a joint investigate with

the Canadian office where that office was housed and Telechoice

which some of you might remember was a telco that had - found to

have a shipping container full of telecommunications contracts with

consumers and identifying information like driver's licences and

passports that were found in bushland in Victoria, had been there

for two years waiting for destruction so again another big lesson in

term of not storing information that's no longer required, making

sure it's destroyed securely, and the outcome of that enforceable

undertaking was that consumers were reimbursed for credit

reporting monitoring but also some real systemic changes in term of

processes. I'm going to turn to the notifiable data breaches scheme,

it's a real opportunity for transparency and accountability. So it

gives consumers an opportunity to understand when there has been

a breach of their personal information, and to be accountable

for - for organisations to be accountable. Accountable both to my

office as the regulatory but also to consumers. There's a real

imperative for organisations to ensure that they build security

protection of personal information in, preventions better cure but

also if something does go wrong to make sure that there's a good,

strong system in place to respond, to let consumers know, but very

importantly to let consumers know what actions can be taken in

order to further mitigate the risk of harm whether that be identity

theft, or whether it be financial harm and the kinds of steps that

could be taken in those circumstances. There's a test that needs to

be met so it's not every breach of data that needs to be notified and

importantly there is this threshold of a likelihood of serious harm

which means it needs to be more probably than not. Partly that

mitigates also against notification fatigue so we really want

consumers to be paying attention if they receive a notification of a

data breach taking it seriously and following the steps that are

advised in order to protect their information. These are some of the

things that consumers can do in order to protect their information

and some of them were canvassed in the previous session. They are

still simple things in term of making sure that we're not using pass

words across services, making sure that pass words are sufficiently

robust and consumers ensuring that our personal devices have got

protection on them and that we're patching and updating our

systems at home, for organisations, there's many things that they

need to do to take really steps to secure personal information but

what we've found since the scheme came into operation and looking

at the 305 notifiable breaches that came to my office since February

is that the human factor is the central issue, so most of the

breaches that have occurred have involved some element of the

human factor, so emails being sent to the wrong recipient with the

wrong attachment but in terms of cybersecurity very interestingly,

the majority of them have been around compromised credentials so

an individual may have been sent a fishing email and tricking into

providing their logon and password details that is then provided

access more broadly to systems. So again that aspect of the human

factor is very prevalent and in term of what we can do to mitigate

against that it really does go to the issue of training, and the issue

of culture, that the previous speaker raised. So important for that to

be embedded that protection of personal information is not just an

issue for the IT people, it's an issue right across the organisation.

And really an organisation is only as strong as its weakest link and

the human faliability that we all have is a known risk and one that

we need to mitigate against. I just want to finish on this slide

around what we can do into the future. And I started with the

concept of privacy by design. And really I think that's where we

need to ensure that organisations are embedding privacy, that the

fintechs, that the start-ups are thinking about data minimisation

from the oust, thinking about how they're going to use the

information, to whom it will be disclosed, how it will be secured and

how long it will retained and when it will be destroyed. The

consumer data right that I'd hoped to have an opportunity to talk

with you about is an example of trying to build in privacy by design,

in how banking data will be transferred between institutions and

censuring that issue of consent and security are central to the

design of that new right which my office will have a central role in,

the other factors is to ensure compliance with the regulatory

framework that I've outlined but really to go beyond that and to

think about the community and cultural conversations, and one of

the things that I'm saying to business is to think beyond can we

from a regulatory perspective do something but turn the question

around to should we? Is it ethical, within the community's

expectations and will it be accepted? Thank you and I'm happy to

take some questions.

JULIE McCROSSIN: Thank you very much. Thanks. And if you can

just introduce yourself and I'll have the mike.

>> Chris, Phelps chair of the low income measures assessment

committee. Can I start by saying that regulators can only be as

good as the regulations, and my question is about the consent that

consumers are required to give to access apps. I think it's a bit

weak to say consumers have to make a choice, there are a ring of

things that if you want to live a life, like other people, and I don't

use Facebook very much but I keep up with my extended family

through it, and it's the only way I do keep up with my extended

family, I have to join Facebook, in my job at the energy

Ombudsman's office I looked at price comparison sites because

we're concerned about some of the advice they were given, I had to

give personal information then I had to tick a box giving permission

for that information to be used by associated companies and to be

associated overseas companies which meets the regulation, I agreed

to that, but it was the only way I could use that price comparison

site so right across consumers' every day life if they want to

participate in society, whether they read it or not, they're giving

away permission, because that's the only way you can get to

participate. I think it's a failure of the regulations that allows

consumers to sign away their privacy rights, the ACCC and the

Australian consumer law recognised unfair conditions in standard

contracts and incites high time that the privacy law took into

account standard usage and restricted the use of that personal

information to the purpose that it's given for, not have a clause

where to use it you have to sign everything awake, your comment?

ANGELENE FALK: I think you've hit on the issue and how it becomes

as meaningful as possible for consumers one of the principles in the

privacy act that I talked about was collection and that only

necessary information should be collected. The other part of that

principle is that the collection of information needs to be lawful and

fair, and the issue of fairness I think is very central, the ACCC has

its digital platforms inquiry that it's looking into at the moment,

which came about really as a look into whether or not there's a

monopolisation and the impact on journalism in the country but it's

also started to look at the handling of data and the way in which

that is a consumer issue, so I've had conversations and

collaboration with the ACCC exactly around this issue, around the

fairness of terms and the fairness of collection, one of the things

that I'm watching very closely is a requirement under the GDPR in

the EU which allow for businesses to adopt a system of certification

or a seal or a trust mark, and whether or not something like that

which would be potentially open in Australian context could help to

build that consumer confidence and trust. The privacy law is one

area where much of the burden does fall to consumers to make that

choice, you're right, would something like a trust mark where

organisations have actually been certified by a third party to have

complied with the law, to have demonstrated that they deal with

personal information in the way that they hold themselves out to do

so, give consumers an ability to engage and choose on that basis?

We see that in many aspects of our life, the former commissioner

from some years ago, talks about the fact that we walk into

buildings, we don't need to give concept because we know that

there's standard and it's fit for purpose, is there something we can

learn from that in our dealings.

>> Ellie Rennie from RMIT. I agree with the previous point about

the difficulty of calling this something that consumers need to deal

with because when it comes to data we're not the consumers we're

the product and really the issue is an economics issue. It's the age

of surveillance capitalism and within that to see this under this

choice model that we are choosing how our data is used is false, and

I mean, I suppose my question is in terms of regulation, I'm

interested in this ACCC work that you're doing because I think it is

about competition, but my question is really around how can the

regulators look - perhaps use technological solutions as opposed to

putting it back on us and/or regulatory solution which are about

dealing with Google's monopoly for instance so that's my question?

ANGELENE FALK: My response to that I suppose is to try and

balance it out a little bit. Whilst I'm calling out the issue around

consumers and needing to make informed decisions which is a part

of the privacy law, I'm also calling out to businesses that they need

to make that easier, that businesses need to be ensuring that the

way in which they're communicating with consumers is clear and

transparent that there's an opportunity to opt in and out of certain

uses of information, that there's not a requirement to have Bundled

consent and consenting to a whole bunch of uses of information,

that you may not wish to or need to consent to for a particular

transaction. But I also agree with you in term of technological

solutions to this. Data 61 from from the ceasefire have done some

very good work in term of this, people are talking about whether we

need a lexicon in term of how we talk about the way in which

personal information is being handled so there's - exciting for the

future in what we can achieve.

JULIE McCROSSIN: A right of rely and one more person.

>> There's been some interesting work around the failure of the

privacy pledge in America which was an industry code for the

education system where they signed up around the use of children's

data so I think that - I think those approaches are interesting but

there's also a lot of failure within that too.

JULIE McCROSSIN: Could I just put in a big tick to the idea of a big

tick? I happen to know two women in their 90s who are active social

people and very active on social media who both have been recently

ripped off quite significantly in what looked obvious to me and I

suppose touches on older person that we often lose our I don't know

what the right word is but as we get older row can lose your instinct

for danger in some way that makes people more vulnerable whereas

a tick would be more helpful.

ANGELENE FALK: I think you're right. A tick would be great.

>> I'm from Melbourne law school. Just to carry on from the

previous speak speakers, you're absolutely right. We need to move

away from formal bundled consent to the idea of dynamic consent

with the use of data and the like but when we talk about concepts

such as transparency and privacy has thought been given to

transparent to who and to clear for who because of course we've

heard again and again there's people in this room who often aren't

asked about is that transparent to me, is that clear to me, that - I

think privacy design means we need to design from within; has

thought been given to that?

ANGELENE FALK: There certainly are businesses that are giving

thought to that and in terms of having focus group and checking

their policies we very much encourage that. The reading age level

for notices and policies should be such that they're understandable

by the whole community, there's a need to be innovative in the way

in which these things are presented so we've seen some of the

banks using videos, I saw the previous news reader from SBS do a

fantastic privacy notice which was really dynamic and engaging a so

elicited people's attention more than the written word, the use of

cartoons, I've seen in other aspects so it does need to be engaging

and informative and it needs to address the broad range of the

community.

JULIE McCROSSIN: Thank you so much for coming, would you give

Angelene Falk a warm round of applause? (APPLAUSE)