CaptionsLIVE
Captioning, Stenography & Transcription

www.captionslive.au | captionslive@outlook.com | 0447 904 255

Australian Communications Consumer Action Network (ACCAN)

ACCAN Communications Consumer Congress

Wednesday, 13 September 2023

Captioned by: Bernadette McGoldrick & Kasey Allen

ANDREW WILLIAMS: We might bring it back together, if that's OK? We still have a few people coming in. In the interests of time, we will get back underway. Our next keynote is from the Australian Information Commissioner and Privacy Commissioner, Commissioner Angelina Falk. I suspect she is well-known to quite a few people in this audience. Commissioner Falk will speak about the OAIC's research on community attitudes to privacy, the commission's privacy priorities and set out opportunities to strengthen privacy protections through reform of Australia's privacy laws. Please welcome Commissioner Falk to the stage. (APPLAUSE)

ANGELINA FALK: Thank you, very much, Andrew and thank you to ACCAN for the opportunity to speak with you today. It is great to be here on Gadigal land. Amongst many friends and colleagues and also some new faces as well.

Just to share a bit of personal information about me. In days gone by, I was actually a backing vocalist for my sister in a band and I have maintained that language when I speak about my speaking engagements. I call them "gigs" and she was very impressed last night when I said to her I have a gig today here on Broadway. I feel like I have really made it.

It is great to talk to people who are at the coal face of the intersection of privacy, telecommunications and emerging technologies and the online environment and some of the issues that I am seeing as a regulator are really fundamental to our society and the way in which human rights are protected into the future and individuals are protected from harm.

I wanted to talk with you this afternoon about the role of the Office of the Australian Information Commissioner, particularly our role in terms of telecommunications and the online environment and our recent study

that we have conducted into community attitudes to privacy. This is a survey that we conduct every three years and it gives us a great insight into what has concerned the community in the handling of personal information. I have also just recently released a report into the Notifiable Data Breaches scheme which reports on the causes of data breaches and that's obviously a very hot topic following the Optus and other breaches. I will give you some insights around what we are seeing there also.

Then I will talk about law reform, because we really are at the cusp of a great opportunity for this country to ensure that we have the kinds of privacy laws that will be fit for purpose into the digital age, with the report being finalised by the Attorney-General's Department looking into the way in which our privacy laws need to be upgraded for the future.

Just starting with the role of the OAIC. We regulate the handling of personal information and also access to information. We are an independent body that's located in the Attorney-General's Department portfolio. Our purpose is to promote and uphold privacy and information access rights. We have a number of regulatory functions and powers to maintain and uphold those rights. That includes dealing with individual complaints, where a consumer may have an issue with the handling of their personal information by, for example, a telecommunications provider. Regulating the Notifiable Data Breaches scheme, as well as the opportunity to conduct investigations on my own initiative, and to conduct audits. We have a long history of conducting audits of telecommunications providers, particularly their record-handling obligations when they're releasing information to law enforcement authorities. We also audit them, in terms of their compliance with security requirements under the Privacy Act. I was very interested to hear the comments of the previous panel about the need for a register for those who are operating in the telecommunications space and we think that would be very helpful. One

reason is that under the current Privacy Act, any operators who have an annual turnover of $3 million or less, and that might be the case for some new start-ups, won't actually be covered by the privacy law. Knowing who's in the sector will assist us with our regulatory activities.

We have got three regulatory priorities relating to privacy that I would like to touch on today. The first will be of no surprise and that is the security of personal information. If we look at the Australian Community Attitudes to Privacy Survey, it tells us that 47% of Australians who were surveyed had experienced a data breach involving their personal information in the previous 12 months. Privacy has become personal for millions of Australians through the significant data breaches of Optus, Medibank, Latitude and Australian Clinical Laboratories. To step you through our regulatory response to these matters. Firstly, just to point out that the Notifiable Data Breaches scheme has been in operation since 2018 and I have provided six monthly reports on the causes of data breaches, so it's been very consistent from the start of the scheme, and that is cyber intrusion is the major issue, and the issue that relates to cyber intrusion is ransomware, compromised credentials and phishing. What we see there is an exploitation of our human vulnerability in terms of hackers seeking to trick individuals into providing their credentials and then seeking access to systems.

These causes have been called out for a number of years and my messages have been to corporate Australia that they need to ensure that they're only collecting the minimum amount of information, keeping it secure in accordance with the Australian cyber securities essential eight and also deleting that information when it's no longer required. Then if we fast forward to last year, where we saw that the cyber environment changed quite markedly and these intrusions happening, my office was working closely with those entities that suffered breaches to make sure

they were notifying individuals, that they were providing information on the steps people could take to protect themselves from further risk, like changing passwords, notifying financial institutions, getting a stop put on their credit report.

I then opened investigations into each of these matters. The Latitude investigation is a joint investigation with the New Zealand Privacy Commissioner and we are looking at whether these entities in fact had reasonable steps in place to protect Australians' personal information and in some cases we are also looking at how long information was retained and whether it was deleted in accordance with privacy laws. Those investigations are advancing and I am hoping to have more news on all of those in coming months. What we seek to do is to ensure that we're taking steps on behalf of the community to ensure that entities both have guidance on how to protect personal information but are also held to account when data breaches occur.

Our community attitudes to privacy survey told us that as well as those 47% of people who had experienced a data breach, their experience of harm was quite diverse. The major harm experienced was the need to replace identity documents, like passports and licences and you might be interested to know that, under the current Privacy Act, there is no legal obligation for breached entities to actually assist individuals to do that, or to pay for the cost of replacement, so one of my proposals in the law reform agenda to the Attorney-General's Department is there should be a positive obligation on data custodians to assist people who are impacted to navigate those risks and harms.

52% of people saw an increase in scams and spam and if we think about what that means, 180,000 reports of scams were reported to Scamwatch at the ACCC with over $300 million in financial loss in this calendar year alone. What we are seeing is that cycle of data breach is

then having that flow-on effect to consumers around scams and a financial impact. We are also seeing 29% of people who experienced other kinds of harms, like identity theft and fraud that resulted and some also experienced psychological harm around 10%.

As we see more information circulating in the economy through these breaches, we are also seeing an increase in impersonation, so there is criminal actors who are very able to make use of this data and to then impersonate themselves as a legitimate entity and then scam people on that basis. It is wonderful that we have got the National Anti-Scam Centre now set up with ACCC and the efforts of the ACMA also to try and stop these scams occurring but the Notifiable Data Breaches scheme and the prevention of data breaches in the first place is also really fundamental.

What can individuals do in individuals also need to be vigilant in deciding who to provide personal information to, making sure that that padlock is always present when you're dealing with entities online, but also thinking about what information is put out publicly on the Internet and how that might be used into the future.

The second regulatory priority I wanted to touch on relates to online platform, social media and high privacy impact technologies. I think this area raises a number of complexities as we see a greater interconnection of technology we are wanting to ensure that the public benefits of technology are realised but that we're minimising the risks of harm from those technologies. We can see from our community attitudes to privacy survey that the community is concerned about the use of artificial intelligence in a range of areas across business and government. There's only a 20% level of comfort of government using AI and less for business at 15%. So there's much that can be done to improve that level of trust and confidence to actually harness the benefits of AI.

The survey also tells us that people would be more confident if

there was greater protection under the Privacy Act for the use of artificial intelligence, so, for example, being advised when AI is going to be used, having the opportunity to have meaningful information about how AI is being deployed and also the ability to contest that information.

Facial recognition was another area of great concern for the community, but that's contextual, so the survey tells us that the community is fairly comfortable with using facial recognition to unlock our phones or our personal security, that there's a level of comfort with using facial recognition for border security and other law enforcement purposes but less so in terms of commercial uses, using facial recognition to detect our moods, for advertising purposes or for entering venues and entertainment areas.

They do see 27% of Australians see facial recognition technology as one of the biggest privacy risks faced today and it intersects fundamentally with our sense of self, our autonomy and our human right to be able to go about our day to day activities without being subjected to surveillance. That's why one of the priorities of my office has been to take regulatory action around the use of FRT, particularly in commercial settings. You might be aware that I made a determination against Clearview AI which had data scraped billions of peoples' information from the Internet, created a facial recognition technology database and then sought to sell that for law enforcement purposes. We are seeing the issue of publicly available information being used for purposes that people wouldn't expect and without our consent and our facial recognition templates are sensitive information and are immutable.

I also have regulatory actions relating to Kmart and Bunnings and their use of FRT in commercial settings. Generative AI is an area that's not only emerging but is solidly with us now and brings great benefits but also risks. One of those risks is the data scraping from the Internet and

using personal information in ways that aren't expected, and I recently released a statement with a number of my international counterparts setting out our expectations of social media platforms to ensure that they're actually detecting unlawful scraping of personal information from the Internet.

We also work really closely with the ACMA and the eSafety Commissioner as well as the ACCC in our digital platforms regulators forum, which is a grouping of regulators to ensure a cohesive approach to the regulation of the online environment in the interests and benefits of consumers.

The third regulatory priority, just to touch on really quickly, is the consumer data right. This is a data portability right where individuals can have their information transferred, say, from one bank to another, or to a third party to see if they can get a better deal. It's underpinned by strong privacy and security obligations that's coregulated between the OAIC and ACCC. It is also being rolled out in the energy sector. It has been paused in the telecommunications sector and this will allow a detailed review of the way in which the consumer data right is protecting consumers' interests in the current industries in which it is operating.

I think there is a few more minutes left. In that time, I would like to touch on privacy law reform and I said at the start that we are at a pivotal moment. The Attorney-General's Department has conducted an extensive review of the Privacy Act and in February this year released a final report. Then conducted some more consultation and I understand that the next steps are for government to respond to that report and I hope that we will see draft legislation sooner rather than later, because we are at a point where some of the risks and harms to Australians as a result of the handling of personal information are particularly heightened and, as a regulator, I require additional regulatory tools to address those

issues but also, as consumers, there needs to be a greater array of rights. Our community attitudes to privacy survey told us that 93% of Australians want the right to ask businesses to delete their personal information. 90% would like to be able to object to certain data practices, whilst still being able to access the service and 89% would like to be able to seek compensation directly through to the courts and 89% would also like the right to ask government agencies to delete their information.

This would align us more closely with the European position on the general data protection regulation and it would ensure that Australians can engage in digital platforms, social media but also telecommunications and other services, safe in the knowledge that they do have that right to have their information deleted. But there's two other aspects to reform that my office sees as really critical. The first is to ensure that there's greater accountability on organisations who are entrusted with our personal information, to handle it in a way that is fair and reasonable. Just as we don't have to be experts in food safety, or engineers to be in this building and have a degree of safety about our built environment, we shouldn't have to be experts in information flows or to traverse 6,000 word privacy policies to make multiple decisions each day on the way in which our information is being handled.

We say that there should be a positive duty on organisations to consider the individual up-front, to think about whether the acts and practices of handling personal information in a particular way could cause harm to individuals and, if so, how that harm can be mitigated. Looking at whether the use of personal information is proportionate, or whether there's another way the information could be handled.

Perhaps an example of that is the case that I took regarding 7-Eleven where they were conducting a survey through iPads in their stores to ask individuals how they rated the service that they received.

In doing so, they were collecting without consent the facial templates of individuals and that, I found, was a disproportionate response to a survey of customer engagement. A fair and reasonable test would make that front and centre and to require organisations to actually think about that. It really is taking the notion of privacy by design, like safety by design, building in protections up-front to that next level.

The other is to ensure that individuals do have more choice and control about the handling of their personal information. That doesn't mean moving to a consent model where we have to tick "Yes" every time we want to do something online. It means having a baseline standard of fair and reasonable data handling practices and then using consent where it really can matter and be meaningful.

The other aspect of law reform is the need to bring in more entities into the scope of the Privacy Act. 95% of businesses operating in Australia are in fact not covered by the current privacy law and we see that this is really fundamental when we're talking about the use of apps and small businesses that are engaging in technology, where they can be handling very large amounts of personal information, so that risk-based approach of small businesses not being really a risk to Australians' personal information, as was the case in 2000 when this exemption came in, is really no longer the case and we need to shift our regulatory frameworks.

Finally, the reforms do seek a direct right of action to the courts and this would allow representative complaints to be made to my office. We could attempt conciliation, if that was unsuccessful, then consumers could go directly to the court for a breach of the Privacy Act. Currently there's no direct avenue. The other is to introduce a statutory tour of privacy and would be for serious invasions of privacy. We see that's really important given that there's no redress if individuals are dealing with personal information in a way that breaches privacy law. If we think about that

Clearview AI, the example I gave, if you partner that with, say, Smart Glasses, we could have a situation where we can all walk down the street wearing Smart Glasses and have peoples' identities revealed to us in real time. That has real implications for our personal autonomy and our safety and something like the statutory tort would be a way to ensure that we address the emerging technologies that have the potential to have real consumer harm. Thank you very much for the opportunity to speak with you today. I think we have some time for some questions today.

ANDREW WILLIAMS: Thank you, very much, Commissioner Falk. (APPLAUSE) We have a couple of minutes before lunch and the Commissioner has kindly agreed to answer a few questions. Holly.

>> One thing you didn't discuss was changing the definition of personal information in this country. It is about personal information which leaves out a whole area of metadata that actually can concern people, that isn't protected under the Act.

ANGELINA FALK: Thank you, Holly, and good to see you. One of the key proposals is the definition of personal information be expanded, so it's not just about information that's about an individual but where you can be reasonably identifiable through metadata, through IP addresses and other digital transactions, so that's really important to ensure, again, that the legislative framework is fit for purpose in the digital age.

>> Thanks for that Angelina. That was terrific. Some scary points at the end. One of the things that has run through this whole conference has been around scams and one of the causes is inadequate ways of proving who you are. We have to hand over multiple documents. There is debate

around digital ID, biometrics, more controversially, what do you think is needed and where are we at with actually getting a decent one piece, safe way of identifying ourselves?

ANGELINA FALK: Great question, thank you Delia. Data and digital ministers from around the country agreed earlier this year that steps would be taken to develop a national plan for dealing with this issue of identity. There is work being done to establish a digital identity and, as a Privacy Commissioner, I am supportive of it, in the sense that it allows for data minimisation. So rather than all of our telecommunications providers collecting drivers licences and passports, there would be a way to verify identity but not actually collect those documents and that removes a huge risk. Of course, there needs to be the right safeguards in place and the oversight and legislative framework to ensure that we have got the assurance that is needed for Australians to be confident in that kind of an identity management scheme but it is heading in the right direction and we do need to move beyond the proliferation of identity documents that are collected throughout this country.

ANDREW WILLIAMS: We have Alexi.

>> Alexi Boyd. Thank you, it was an informative presentation, Commissioner. I want to ask you a philosophical question. How do policy makers find that balance for small businesses, being both consumers and holders of information and making sure that both of those - the way that they are looked after in legislation is maintained, because that is something that needs to be thought of in the data privacy laws?

ANGELINA FALK: Yes, great, thank you, nice to meet you. Under the

consumer data right, for example, small businesses have rights to access data in the same way as individuals, so where we are seeing small businesses access to data and the competition issues associated with that being brought to the bear in new legislative regimes, I think with privacy, we need to remember that it's a risk-based framework, so small businesses need to be supported to comply with the law. We need to make privacy simple for small businesses and to calibrate their requirements according to the risks that they pose. I think if we take that risk-based approach and a consultative approach, collaboration, my office can make privacy easy for small business and assist them to mitigate their own risk and potentially their own commercial risks. Some of the things that I am seeing is - I am trying to think of the word, when we have got processes, where we have got small businesses in the middle, the down stream effects, where my regulatory remit won't reach into a small business, and they might be a service provider for other larger businesses, so we have got some real regulatory gaps there.

I also found during the pandemic, when small businesses were asked to collect peoples' personal information on note pads, you will remember at the start, I didn't have any authority to go and assist. We tried to assist but bringing them within the legislation means that we can provide the kind of regulation and guidance that can uplift the security posture of the whole economy and if we want to be the most cyber secure economy by 2030, and that is this Government's ambition, then small business needs to be brought along and supported in that.

ANDREW WILLIAMS: One more up the back.

>> Beth Baker, I am the chair of the Older Women's Network. Privacy is a big issue for my members. It is the breach and the abuse once that

privacy has gone. We have no idea who holds our data. Last night I received three phone calls from the No campaign. I don't know how they got my data. I didn't opt into that data. What I heard coming down the line, and I work for the Aboriginal Education Council in my day job, so I actually know this stuff. I got a tissue of lies, fear campaigning and absolute outrageous statements that were fed into my ear. I knew the truth but what about all of my members who didn't and who got this phone call coming down? How can we absolutely ensure that people who don't have our permission to feed us rubbish don't get access to the data to feed us that rubbish?

ANGELINA FALK: Thank you. Nice to meet you and thank you for all your work. It is a very, very good question. I think the answer lies in a couple of different avenues. We obviously have the "Do not call" register that is administered by the ACMA but what we're finding is that data brokers are harvesting personal information and selling that and currently there is limited ability for individuals to find out how that data was acquired. One of the reforms to the privacy law is to enable individuals to actually ask "How did you get my data?" Then the right to deletion, would you allow them to delete that information? That is consumer-led. You obviously need to have skills and expertise to be able to navigate that, which is why we think that the fair and reasonable test about positive duties around only using data in a fair and reasonable way will help to balance that with accountability of organisations. I think it is a complex question. It is a great one to raise and that more thinking needs to be done in relation to it. Thank you.

ANDREW WILLIAMS: One last one, David if it is quick.

(INAUDIBLE QUESTION)

ANGELINA FALK: Thank you for that question. A great reminder. The other exemption under privacy law is political parties are completely exempt. For the last five years, I have been advocating for that political party exemption to be removed from the Privacy Act that political parties should be transparent about the way in which they are collecting and holding information, make sure they are keeping it secure and allow people to have access and understand how their information and where it's been derived from by political parties. That transparency also then allows our democracy to be underpinned by a clear understanding of the way in which we might have been profiling by political parties and why we are seeing particular ads online or other messages that are being targeted to us, based on that kind of profiling.

ANDREW WILLIAMS: We have run into lunch, so on behalf of everybody here, thank you to Commissioner Falk. (APPLAUSE)

ANGELINA FALK: Thank you. Enjoy lunch.

ANDREW WILLIAMS: It is lunch now. Back in here at 1.30 and we have got a presentation by video from the Shadow Minister then. Thank you.