CLB Interview: Anna Johnston

To celebrate Privacy Awareness Week and the anniversary of the GDPR (we're fun like that here at the *Communications Law Bulletin*), Eli Fisher, co-editor, sat down with Anna Johnston to talk about what's happening in data law.

By way of a perhaps unnecessary introduction, Anna Johnston is [redacted] Privacy joke. (Tough crowd.)

Anna is one of Australia's most respected experts in privacy law. Anna was a Deputy Privacy Commissioner for NSW, and has been commissioned to write privacy guidance publications and deliver presentations and training on behalf of other regulators including the Australian and Victorian Privacy Commissioners. She established Salinger Privacy in 2004, making wonderful use of her right to use a pseudonym (high five, APP 2!), where she specialises in privacy and data governance issues. She has established herself as a go-to expert for privacy compliance.

Anna has been called upon to provide expert testimony before various Parliamentary inquiries and the Productivity Commission. She is a lifetime member of the Australian Privacy Foundation, a member of the International Association of Privacy Professionals (IAPP) since 2008, and in 2019 was recognised as an industry veteran by the IAPP with the designation of Fellow of Information Privacy (FIP).

ELI FISHER: Anna, on behalf of all of our readers, thanks so much for chatting with us. As someone who is working in this area every day, what parts of data law are keeping you busiest?

ANNA JOHNSTON: It's a mix of the foundational concepts, and then there's always something new. So in any given week we might be running some basic privacy awareness training for a client, drafting a collection notice or giving advice about allowable data uses, but also perhaps working on a Privacy Impact Assessment of some interesting new technology project, maybe a chatbot, or the establishment of a data analytics centre. But no matter what kinds of projects we are looking at, the basic questions are the same: can and should we collect this data, can and should we use it for this purpose, to whom can we disclose it, and how do we keep it safe?

FISHER: I forgot to get my kids Privacy Awareness Week presents this year. What did you do for it? Did you make any PAW resolutions for 2019?

JOHNSTON: We did a bunch of things for PAW this year. Salinger Privacy ran a free webinar on behalf of the IAPP about Privacy by Design in Privacy Law, which was fantastic. We had over 500 attendees. Another webinar, on Privacy Law for IT Professionals, was one of our regular series of professional webinars. I wrote a piece for the NSW Law Society Journal about a couple of new cases which impact on employers' liability for the privacy harms caused by 'rogue' employees, I was a member of a panel of speakers for the launch of Deloitte's 2019 Privacy Law Index, and for our monthly blog we focussed on explaining the basics of privacy law as a kind of Privacy 101 (see https://www.salingerprivacy.com.au/2019/05/03/privacy-101/).

FISHER: Anna, you were a regulator for a number of years before moving to private practice. Given that the case law in this area is so scarce, and the law is deliberately drafted in terms of principles, it's an area of practice that requires judgment calls. To what extent does your regulator background inform the way you practise? And what can we non-regulators do to hone that instinct?

JOHNSTON: The 'fuzzy' nature of privacy law is one of the things I love about it - you do need to use your judgment, and think about what your customers would expect, and what you can do to avoid causing them any harm. Something I have carried with me from my regulator days is a passion for explaining privacy topics to a lay audience. It's easy to get caught up in the minutiae of APP this and exemption that; but mostly privacy law boils down to common sense and good manners. So my advice for lawyers is to be less lawyerly; take a step back and look at the bigger picture. Because the law might say whether your client 'can', but not whether they 'should'. Having said that, there is actually a swag of case law coming out of the NSW Civil and Administrative Tribunal, and keeping on top of that for our annotated guide is how I keep the lawyerly side of my brain functioning.

FISHER: There's a real sense, at least from where I'm sitting, that privacy has gone from being a regulatory peripherality to something that businesses, government and regulators, and social commentators are profoundly concerned about. What's changed in your view?

JOHNSTON: Things have absolutely changed. I have worked in privacy since 2000, so I have seen the pendulum swing away from privacy concerns in the wake of the September 11 attacks in 2001 and all the focus on surveillance that arose from that, and then massively swing back again in the past couple of years. First there were the Edward Snowden revelations, and then the focus on the GDPR, but the real game changer was the Facebook/Cambridge Analytica scandal, which seemed to reach into public consciousness in a way that hadn't really happening before. You

just look at the shift in tone from Mark Zuckerberg, who first developed Facebook within that post-September 11 anti-privacy mentality of "if you've got nothing to hide...". He's gone from saying about 10 years ago that privacy is no longer a social norm, to last year saying actually it's the most important thing his users value. The OAIC's community attitudes surveys back that up; people are becoming more concerned about their privacy than they were 10 or 15 years ago.

FISHER: The GDPR was obviously a very big deal. It's kept a lot of us busy in Australia, and around the world. How did you feel about it when it first came into effect a year ago, and how do you feel about it now? Was it over-hyped, or has it truly changed the game?

JOHNSTON: I think the focus on May 25 was over-hyped, as if you had to 'be compliant' by then or the sky was going to fall in. But the long-term reach of GDPR I don't think is over-hyped. It will take a while for the impacts to really lead to business change, but GDPR certainly has the power to reign in the excesses of the data surveillance economy. And then there's the ripple effect; I've just come home from a gathering in Tokyo of privacy regulators from the Asia-Pacific, and there is so much talk about GDPR and how it either directly affects businesses in the region, or indirectly is affecting both consumer expectations and legislators' thinking.

FISHER: Do you think that the GDPR has got its extraterritorial focus right? Is it futile trying to regulate privacy by reference to national borders?

JOHNSTON: Yes, GDPR works because of its extraterritorial reach. How effective enforcement will be across borders is a live question, but the drafting was deliberate, to catch businesses which previously avoided privacy laws based on their physical location being different to their customer base. Now what matters is the physical location of the affected individuals.

FISHER: Do you think that the GDPR has filtered into the way we interpret the APPs? So much of the APPs is based on "reasonableness" – what the individual would reasonably expect you to do with her or his personal information, what level of security you need to adopt, how long an APP Entity can take before performing an obligation. Do you think that the meaning of "reasonable" has shifted in light of stricter GDPR standards?

JOHNSTON: I think the interpretation of what is 'reasonable' is shifting all the time, and that's a good thing. It's how privacy law manages to stay relevant to both new technologies and shifts on community expectations. If the law were more prescriptive it would quickly become out of date. But it's not just the GDPR having an impact, that shift in expectations can come from anywhere. There was a recent QCAT case, *ZIL v the Queensland Police Service*, in which

the issue was whether the police service took reasonable measures in terms of data security. I found this case interesting because the Tribunal said that as the community's understanding of and attitudes towards family violence has changed, the community's expectations have increased that the police service will do more and more to protect the privacy (and thus personal safety) of victims of family violence. And that translated into a finding that a failure to prevent unauthorised access to a family violence victim's records, and a failure to monitor access proactively was not good enough anymore. The police service had not taken 'reasonable steps' to prevent the misuse of the personal information it holds. It was explicitly found that while similar cases previously failed, this one succeeded, precisely because community attitudes have shifted. And as a community we now expect more from the organisations which hold our personal information. So what is considered 'reasonable' data security measures is increasing over time.

FISHER: It seems like the biggest concern of data management is a data breach. A few months before the GDPR came into effect, Australia got its mandatory data breach notification scheme. Those entities caught by the GDPR got a second layer of data breach notification obligations with that regulation. APRA-regulated entities are now grappling with CPS 234. And of course businesses, whether they're caught by the GDPR, the Privacy Act, CPS 234 or any other data breach notification obligation, will have private contractual obligations regarding notification of breaches which may vary from contract to contract. What is a practical way to manage this tangled melange of varied security standards?

JOHNSTON: Organisations need a Data Breach Response Plan, which incorporates each of the rules applying to them. The Plan needs to anticipate who will need to be involved in any breach response, not just the privacy officer but also the risk and compliance team, lawyers, forensic IT investigators, and who needs to be briefed, like your insurer and your media or PR team. The Plan should help the right person make the right decisions at the right time, like the point when you need to assess the level of harm that might arise for affected individuals. The legal tests, and the timeframes for notifying, differ between the Australian and European schemes. The Plan also needs to help everyone in the organisation distinguish between a data breach and a cybersecurity incident; they are not always the same thing, and so your response path will need to accommodate that. And you will need templates at the ready, including a reporting format for the relevant regulators.

FISHER: Let's talk bugbears. We all have a few. I know consent drives you nuts, especially the way privacy policies are often wielded. Walk us through it.

JOHNSTON: It's the practice of dressing up other things as 'consent', when they are really not, that drives me nuts. If it's a collection notice or buried in a privacy policy, it's not consent. If it's a condition of doing business with you, it's not consent. If I had no genuine choice to say 'no', it's not consent. I describe consent as the "would you like fries with that?" question. If I can freely say no to the fries, but still get the burger I want, without any kind of penalty for saying no to the fries, then if I do say 'yes' to the fries you can call it consent.

FISHER: So what are your tips for better managing consent?

JOHNSTON: Go back to basics. Don't start from a point of thinking about consent. Instead, think about "are we lawfully allowed to collect, use or disclose this personal information?" There are plenty of grounds under which privacy law allows you to handle personal information in a lawful way, without needing to go anywhere near relying on consent. Consent is not the rule, it is the exception to the rule. But if you have no other lawful ground on which to collect, use or disclose personal information, then seeking the individual's consent is your final option. But know that they need to be free to say 'no', and if they say no then you can't do it.

Privacy policies are important from a transparency perspective. But they are not a tool for seeking anyone's consent.

FISHER: Ok, so let's turn to data becoming an antitrust issue. What are your thoughts about the ACCC's inquiry and preliminary report, from a data perspective?

JOHNSTON: It's going to be really interesting to see how the final report from the ACCC turns out. I was originally sceptical of the role a consumer protection and competition regulator would play in this space, and I saw the ACCC's involvement as a symptom of the sidelining of the OAIC. (The US model of privacy regulation is to rely on their consumer and competition regulators, and I think that has utterly failed as a regulatory model.) But the preliminary report from Rod Simms was spot on in its understanding of the interplay between data collection as the business model driving big tech, and the impacts that has on us as consumers and as citizens, both from a privacy perspective and from an economic perspective, in terms of Google and Facebook in particular having effective monopolies. Their market worth is entirely based on exploiting our personal information.

FISHER: And what are you hoping for in terms of a final report and legislative consequences? We've seen moves to increase funding of the OAIC and the amount of penalties. What else needs urgently to be addressed?

JOHNSTON: Oh my wishlist is long! I would like to see some tightening of the Use and Disclosure principles in Australian privacy law, because too many privacy invasive practices scoot under the radar by saying they are related to the

purpose of data collection. That's a potential outcome of the ACCC enquiry. And I would like to see more public enforcement by the OAIC. Too many cases are declined without a public determination. The State privacy laws are better at allowing individuals to pursue their complaints in a Tribunal, so I would love to see some change there too in relation to the federal Privacy Act. And given the impact of GDPR on Australian businesses, I think Australia should look at beefing up the Privacy Act so that it can be recognised as 'adequate' by the European Union. An 'adequacy' decision would open doors for Australian businesses trying to reach European markets, because then personal information could be exchanged freely.

FISHER: CSIRO's Data61 just released a Discussion Paper 'Artificial Intelligence: Australia's Ethics Framework' to encourage conversations about AI ethics in Australia. What were your thoughts about the Government's approach to machine learning and AI technology, from a data governance perspective?

JOHNSTON: I have been very critical of the CSIRO's discussion paper. I think that it suffers from a misbelief that privacy law requires consent for everything, but also that getting consent is easy. In the world of AI and ML, consent is actually pretty useless, in terms of a legal ground on which to base your collection, use or disclosure of personal information. Much of the data used to train machine learning will have been collected for some other purpose (like, being a patient in a hospital, or riding a bus), so typically the data subjects were not asked to consent to the use of their data for a different purpose (training a computer to recognise patterns of behaviour). And even if we are to be asked for our consent, how can we possibly give an informed consent, when the whole point of ML and AI is to throw all the data in the mix and see what pops out? They don't necessarily start with a hypothesis for testing. It's not like say a clinical trial, where I know I am being offered a new kind of medicine to treat my disease, and I've been informed about the possible side effects, and I've had the chance to say 'no thanks'. AI and ML are based on different kinds of research practices, which don't usually involve that kind of one-on-one, structured discussion with an individual, or a clearly defined and time-limited purpose for using the data.

So it really concerned me that the government didn't get the basics of privacy law right in this discussion paper. Also, it didn't really get into the ethical dimensions in detail, or questions about social licence. I actually organised a loose coalition of privacy experts to prepare a joint submission to the CSIRO and the Department of Industry (see https://www.salingerprivacy.com.au/2019/04/27/ai-ethics/), because I was so worried that their discussion paper would lull businesses in the tech space into a false sense of security about what they needed to do, in order to comply with privacy law. Risk management in terms of privacy compliance doesn't start or end with getting consent, even if it were feasible in the first place.

FISHER: Some scholars suggest that law needs to work in tandem with technology to regulate undesirable uses of technology. For example, you can prohibit spam legally but you can also devise a technological solution – a filter, for example – to prevent or minimise the adverse consequences of undesirable uses of technology. Do you hold high hopes for the prospect of law being able to protect privacy in the digital age? And what are some of the best technological solutions you have seen?

JOHNSTON: The law can only ever achieve so much on its own. If tech is designed to allow or encourage users to do things they shouldn't, whether in order to protect their own privacy or that of others, then of course the law and regulators should step in. But it's so much better to bake privacy controls into the design of systems from the beginning. A lot of effort goes into the cybersecurity side of things, keeping out the external bad actors. But when designing, configuring or implementing tech, you also have to think about the authorised users of your system, and design the tech so that authorised users only see the minimum amount of personal information they need to do their job. Saying "oh but we've got a Code of Conduct for our employees" is not nearly enough. The legislation says it's not enough, and case law backs that up. Privacy controls can be built into tech, whether that is filtering out certain data fields from entering a data warehouse, setting role-based access controls on a CRM, masking certain data fields from view of certain users, requiring users to pass certain tests before they can access data (like entering which customer case file they are working on to justify this particular search), audit trials and proactive monitoring of them, just-in-time collection notices or permission requests ... there's plenty you can do. We use eight privacy design strategies to guide our advice to clients when we do Privacy Impact Assessments.

But sometimes the things that stick or that change user behaviour are not high tech at all. I had a client who enforced their policy of staff logging out when leaving their desks in a really novel way. If anyone saw a desktop unattended, they would send an all staff email from that person's email account, saying 'Friday night drinks are on me!' Apparently that changed staff behaviour pretty quickly.

FISHER: Nice tip! Anna, thanks so much for this. It's a pleasure as always to get your thoughts about these issues. I know the entire readership is grateful for your insights.

JOHNSTON: You're very welcome Eli.