Data security in practice

PRIVACY AND DATA SECURITY ARE IN THE SPOTLIGHT AS REGULATORY CHANGES FROM 2018 ARE TESTED OUT IN PRACTICE AND DATA BREACHES ARE INCREASINGLY REPORTED IN THE MEDIA.

BY ADAM WAKELING, MOLINA ASTHANA AND PETER MORAN

While the European Union's General Data Protection Regulation (GDPR) has reshaped how data is handled across many parts of the world, Australia is similarly experiencing change. With the roll-out of the Consumer Data Right regime in the banking sector and the federal government's new decryption powers through the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act*, Australian privacy lawyers can expect another busy year.

The use of data and consent

Who owns your personal information once you publish it on social media?

The Cambridge Analytica scandal made this one of the biggest privacy questions of 2018. Cambridge Analytica harvested data from some 87 million Facebook users through the app quiz "This is Your Digital Life". As well as collecting data from users, the app requested extended permission to access users' private messages (which Facebook advised only a small number of users had granted) and their friends' Facebook public profile pages. Cambridge Analytica used this information to profile users and sold their dataset to political campaigns for the purposes of targeted advertising, including Donald Trump's presidential campaign and the "Leave" campaign in the 2016 Brexit vote.

Cambridge Analytica did not hack any account, although the way it collected information was unreasonably intrusive and in breach of privacy legislation in several jurisdictions. This behaviour highlights the dark side of the multi-billion dollar information brokerage industry where companies trade in information obtained indirectly. Your personal information is valuable. The *Financial Times* calculator, based on an analysis of industry pricing data in the US, can determine the value of an individual's data factoring in specific variables. For example, US$1.40 (AU$1.96) is the calculated value of the data belonging to a recently-divorced lawyer who has children, suffers from allergies, back pain, headaches and high blood pressure, owns a home and is interested in foreign travel and cruises.

The UK Information Commissioner's Office issued Facebook with the maximum fine of £500,000 for processing data without proper consent and failing to take measures to guard against unlawful processing.

The issue of information sharing through social media shows no signs of going away. In February 2019, an investigation by *The Wall Street Journal* found that popular smartphone apps were sharing information with Facebook through an automatic process.[1] This further confirms a report by Privacy International that 61 per cent of apps tested automatically transferred data to Facebook the moment a user opens the app, regardless of whether they are logged in or even have a Facebook account, owing to default settings in the software development kit that developers leverage to build Facebook apps.[2]

How does Australian law apply to these activities?

Under Australian Privacy Principle 6, companies that collect personal information may only use it for the purpose which they collected it, or a related purpose which is reasonably expected by the individual, unless additional consent is obtained. Companies that fall under the small business exception are caught by the Australian Privacy Principles if they sell personal information to others for direct marketing. Australian Privacy Principle 7 sets out the requirements for direct marketing, which is permissible by companies where there is direct collection, collection is reasonably expected, and a clear and simple opt-out mechanism is provided. Where there is indirect collection, the individual must have validly consented to the information being used for that purpose, or for organisations to have shown that it is impractical or excessively burdensome to obtain that consent (inconvenience, length

ADOBE STOCK

of time and high cost are not sufficient). Historically, companies that collect personal information for marketing have relied on pro-forma tick boxes to get bundled consent. As data collection and processing become more sophisticated, it is questionable whether privacy regulators will consider tick-box consent sufficient. Consent will almost certainly be tested this year.

Cybersecurity is critical to privacy

Malicious attacks remain the largest cause of privacy breaches in Australia and are increasingly common. According to the Office of the Australian Information Commissioner's quarterly reports, malicious attacks accounted for 44 per cent of reported breaches in January-March 2018, 59 per cent in April-June 2018, 57 per cent in July-September 2018 and 64 per cent in October-December 2018. An example is the breach which befell the shipping company Svitzer. In this instance, a hacker set up an auto-forward on Svitzer's finance, payroll and operations email accounts. Between May 2017 and March 2018, up to 60,000 emails containing employee personal information were forwarded to an external recipient.

The two most common types of cyber attacks are brute force attacks and phishing scams. In a brute force attack, a hacker uses a computer to try multiple combinations of a username and password to guess the correct one. In a phishing attack, the hacker sends a scam email with a link that when clicked installs software.

Fortunately, both types of attack can be limited with business-grade IT security systems and employee awareness. Secure systems will lock up when multiple unsuccessful attempts to log-in are detected, while two-factor authentication can make key systems even more secure. Employees can be trained in the importance of creating sufficiently long and complex passwords – an eight-digit password using numbers and upper and lowercase letters has more than two hundred trillion combinations. Staff can also be trained in how to identify phishing emails. A key take-away for lawyers is that these obligations don't just apply to their clients; they apply to their practices as well. Lawyers who are unfamiliar with basic cybersecurity – and there are many – risk taking on liability if they don't educate themselves. "Email is an inherently insecure means of communication[3] and one of the biggest challenges faced by most law firms is the need to find more secure ways of sending client information using email," says Ignite Systems managing director Ian Bloomfield who specialises in cybersecurity for the legal services industry. "In today's environment, a law firm sending client information in the body of an email that is subsequently compromised, could reasonably be considered to be in breach of their professional duty to maintain client confidentiality."

The internationalisation of privacy laws

The enactment of new European privacy law that restricts how personal data is collected and handled heralds a new era in the international privacy arena. The EU GDPR, enforced in May 2018, focuses on ensuring that users know, understand and consent to the data collected about them. It aims to harmonise data privacy laws across Europe, protect and empower the data privacy of all EU citizens and reshape the way organisations across the region approach data privacy.

Though the GDPR is applicable within the EU, its jurisdiction extends beyond as it applies to all companies processing personal data of data subjects residing in the EU regardless of the company's location. The applicability of GDPR is clear as it applies to the processing of personal data by controllers and processors in the EU regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.[4]

The GDPR applies to organisations including tech giants, publishers, banks,

SNAPSHOT

- There are significant developments in privacy law.
- These affect different areas of legal practice.
- They include the use of data and consent, the relationship between privacy and cybersecurity, the internationalisation of privacy law, and the legal issues around cyber-warfare.

universities, Fortune 500 companies and ad-tech companies that track consumers across the web, devices and apps. Australian organisations that process data of EU residents may also fall foul of the GDPR.

More significant though is the push by other countries to follow suit with similar laws which will lead to international uniformity in privacy laws and standardised application. The GDPR has already spurred changes in data collection and handling practices worldwide. No country can afford to work in isolation anymore.

The GDPR includes the right-to-be-forgotten, according to which individuals can force search engines to delete certain links on them. The issue of how far this right should be applied was raised by Google last year in the case brought against it by France's privacy regulator CNIL in the Court of Justice of the European Union.[5] One of Google's arguments is that the right in effect impinges on rights guaranteed by other jurisdictions. In this case, if Google was forced to remove all references to the information at hand, Google would infringe free speech rights guaranteed to Americans – laws which are prioritised in that country over the right to privacy. The final ruling by the Court, expected later this year, will determine if national governments and local agencies have the authority to apply their own standards to the rest of the world or whether the global internet remains above legal challenges from any individual country. The implications may be far reaching.

Cyber-warfare and the law

While much focus has been on cybersecurity and fraudulent activity at both the corporate and individual level, Australians can also no longer ignore the risk of cyber-warfare and espionage attacks by foreign states. There is no tyranny of distance in cyberspace. Russia's ability to shut down power plants in the US via hacking,[6] the ability of the US to damage Iran's nuclear program via the Stuxnet computer worm and North Korea's attack on Sony by releasing embarrassing emails and unreleased movies all seem far removed from the day to day of most Australians. However, a foreign government's recent attempt to hack the parliamentary network in Canberra[7] reinforces that Australia is as much at risk of cyber-warfare and espionage as other countries.

The incident has also fuelled concerns about whether our government can reliably provide all protection required.

The battleground in cyber-warfare is data, in particular, personal information. Governments and businesses alike realise the significant value and power of access to the enormous amount of personal data now available in cyberspace. Tim Berner-Lee, known as the internet's inventor, has expressed concern at our loss of control over personal data.[8] While most of us worry about use of data by corporations, governments or malicious individuals, we rarely turn our minds to the harm such data could cause if used by foreign states against Australia's interests.

What does this mean for Australian lawyers? As cyber law expert Helaine Leggat is at pains to state, "the laws we enact and enforce can shape norms of societal behaviour".[9] We, as lawyers, should recognise that laws allowing greater access to data could increase our exposure to cyber risk, not only as individuals, but as a society. If privacy is not defended as a core individual right, the risk of data misuse is potentially far greater than being spammed by corporations or spied on by our government. Apple famously refused to comply with a court order obtained by the FBI to create a process to allow back-door access to an iPhone belonging to a terrorist. Apple released a statement describing the demand as "an unprecedented step which threatens the security of our customers . . . which has implications far beyond the legal case at hand".[10]

The Data Encryption Bill[11] passed by the federal government in December 2018 received widespread criticism, including by the Law Council of Australia which stated:

"The Law Council acknowledges that there is significant value to public safety in allowing law enforcement and national security agencies faster access to encrypted information where there are threats to national security . . . [but the government should] balance achievement of that objective with the need to ensure that the proposed measures are reasonable, necessary and proportionate, including by incorporating reasonably transparent and verifiably reliable safeguards and controls".

Governments naturally want to redress the power imbalance created by the advent of big data and its controllers. They also want to protect our national security from terrorists and malicious players. However, losing control of our personal data could have ramifications beyond an invasion of our personal privacy: it could put our collective security as a society at risk. Lawyers play a crucial role in advising and lobbying legislators to find the right balance of upholding a right to privacy and mitigating risks of cyber attacks and cyber espionage against us collectively.

Conclusion

Continued privacy developments pose wide-reaching implications in the public and personal sphere. Key take-aways for lawyers include:

- the importance of obtaining consent for collecting and using personal information
- the responsibility to guard clients' information from malicious cyber attacks
- the growing trend of uniform privacy laws and standardised application
- the need to defend privacy as a core individual right.

Lawyers globally clearly play an important role in shaping and upholding the right to privacy. ■

Adam Wakeling is acting team leader of Audit, Risk and Compliance at State Trustees and co-chair of the LIV Technology and the Law Committee.

Molina Asthana is principal of Swarup Asthana Lawyers and Business Advisors, a member of the LIV Council, a board member of Graduate House, University of Melbourne, and a Commissioner with the AFL South East Commission.
Peter Moran is principal at Peer Legal, founder of the Steward Guide, an online technology guide for lawyers (www.stewardguide.com.au) and *LIJ* Technophile columnist.

1. Sam Schechner and Mark Secada "You Give Apps Sensitive Personal Information. Then They Tell Facebook", *The Wall Street Journal*, 22 February 2019, www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.
2. Privacy International, "How Apps on Android Share Data with Facebook – Report", 29 December 2018, https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report.
3. The Office of the Australian Information Commissioner, "Guide to securing personal information" includes this statement – "Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email".
4. https://eugdpr.org/the-regulation/.
5. www.politico.eu/article/top-eu-legal-advisor-sides-with-google-in-right-to-be-forgotten-case/.
6. "Russian hackers penetrate US power stations", BBC News, 24 July 2018.
7. "Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers", ABC News, 18 February 2019.
8. "Tim Berners-Lee: I invented the web. Here are three things we need to change to save it", Tim Berners-Lee, *The Guardian*, 12 March 2017.
9. "Cyber Warfare: An Enquiry into the Applicability National Law to Cyberspace", Helanie Leggat.
10. "FBI-Apple Encryption Issue", Wikipedia.
11. *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth).