Reading Reflection Privacy & Security in Australia.

IST 618, INFORMATION POLICY

PARIN P PATEL

Introduction

Around the world, governments are coming to terms regarding the massive amounts of information collected and held by private and governmental bodies. Their responses are beginning to mirror the concerns of users who are becoming more interested in what information companies are collecting and how they handle the data once it has been collected. While some countries have had privacy laws in place for decades, others are just beginning to put regulations in place. This reflection will review privacy laws of Australia and how GDPR has affected Australian businesses and legislation. In addition, this review is discussing the advantages and disadvantages of how Australia collects and uses personal information. Finally, there will be a risk analysis of the way Australian government's use of surveillance on its people, and a recommendation for future policy to protect certain populations.

Background

"Just 9% of social media users were 'very confident' that social media companies would protect their data. About half of users were not at all or not too confident their data were in safe hands," states the findings of a PEW research report from 2017 on how Americans view cybersecurity in the modern age (Olmstead & Smith, 2017). At the time, for some, this report was met with apathy and disbelief that a large tech company could be regulated. Facebook had just defeated another privacy lawsuit against accusations that they track user's activity outside of the social media website. This came as another legal win for tech companies,

who at the time, appeared to be beating or emerging from every privacy-related lawsuit unscathed (Stempel, 2017).

However, for others, the report was a glimmer of hope into a future where the American public cared enough to force the technology industry to meet their demand for privacy. Because, the PEW report was just one of the many reports being published at the time that gave insights into an industry that was more than just cool gadgets and convoluted codes. For the first time in decades, the American public was beginning to personally feel the drawbacks of technology in their lives. More importantly, they were beginning to form opinions and were more willing than ever to talk openly about cybersecurity and their data. This was mainly due to 2017 being a record-breaking year for data breaches and hacks, with a 44% increase since 2016. From Equifax to Yahoo to even Cornell University, 2017 taught Americans that ransomware and data breaches do not discriminate. It highlighted the vulnerability of critical infrastructure and insecure databases that lead to an unpresented scale of leaks and breaches that effected billions of people around the world (CyberScout, 2018).

And it was not just the United States that was feeling the spiraling effects associated with compromised data and personal information. This was a global trend, where the total number of lost or stolen records all around the world had jumped to 1.9 billion in just the first six months of 2017. In other words, by just June of 2017, there were more global data breaches than there were total in 2016 (Irwin, 2017). Figure 1 below shows how while the world saw an overall increase in data loss in 2017, with North America having the largest number of breaches, the amount of data lost in Europe decreased by 3% from 9% (161 incidents) in 2016 to 6% (112 incidents) in 2017 (Gemalto, 2018). This downward trend only continued for Europe

in 2018, aided by the enactment of Europe's data protection law, the General Data Protection Regulation (GDPR) in May of 2018.

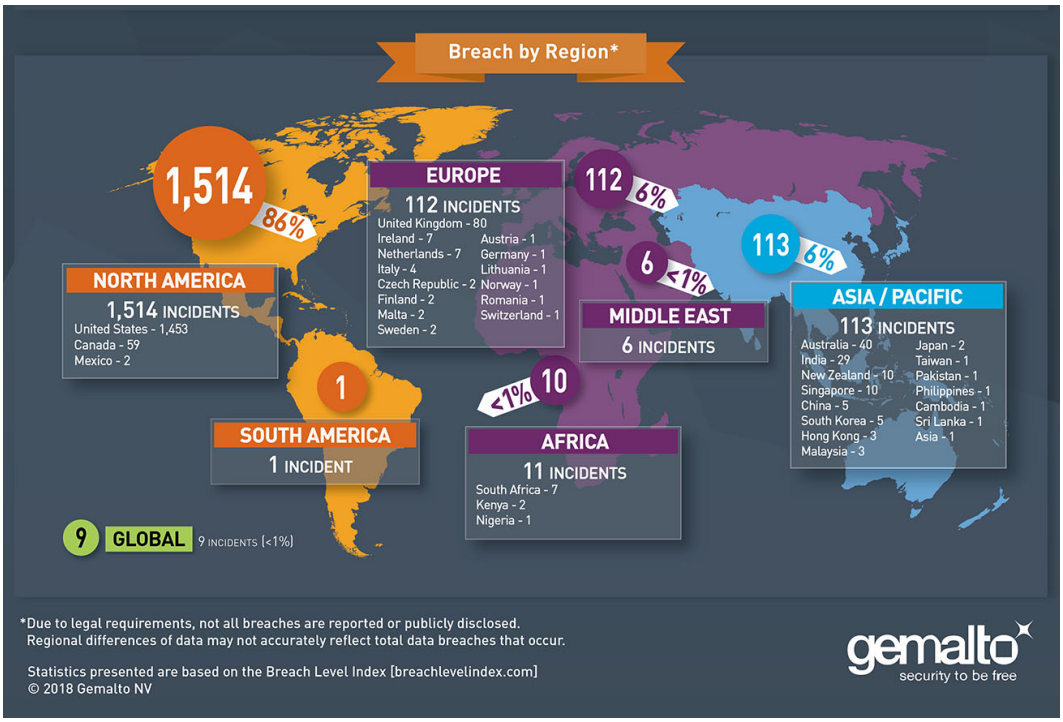

Figure 1 Breaches Across World 2017

Since GDPR went into effect, it has become a precedent-setting piece of legislation for the world. Because its stringent requirements force multinational companies to implement "privacy by design and default" policies across their global operations , in many ways, GDPR is serving as a global benchmark for privacy regulations for other nations (Benady, 2018). It is important to point out that while GDPR has a significant global influence due to its clear definitions, strict controls of data transferred to non-European Union countries or organizations, and enforceability; it is by far not the first or only data privacy law enacted by a government.

Review of Data Security & Privacy in Australia

Australia has had data privacy laws in place since 1988, through The Privacy Act of 1988. In addition, the legislature has passed multiple amendments and bills since 2012 updating the terms and obligations (Australian Government: Office of the Australian Information Commissioner, 2019). Similar to how GDPR is the central legislative regulation that sets data and privacy protection in Europe, in many ways, the Privacy Act is the Australian counterpart. The major difference is how they approach privacy conceptually (Meese, Jagasia, & Arvanitakis, 2019). The EU sees privacy and data protection as a basic human right, anchored by the principles of dignity, freedom, equality, and solidarity . This right is assured through the Charter of Fundamental Rights, specifically in Article 8 that focuses on data protection's (CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION , 2012).

This is a stark contrast to Australian data protection since Australia does not have constitutional basis for data protection. Instead, data securities follow a host of more general, broader protections regarding the privacy of Australians. Security is available through common law as the tort of breach of confidence, "centered on the management and protection of private information" (Meese & Wilken, 2014). If trust amid separate parties is violated than said parties, as well as others effected, can use tort to safeguard their privacy interests, including their personal information. However, since tort is rarely used in the case of data security, the Privacy Act, has instead, served as the principle regulation since its introduction in 1988 (Meese, Jagasia, & Arvanitakis, 2019). In addition, the creation of the Privacy Act resulted in the appointment of an Australian Information and Privacy Commissioner, whose main responsibility was to ensure the government obeyed with relevant legislation and personal complaints

brought forward by individuals. As the technology progressed into the 2000's, these standards were extended to include private and not-for-profits organizations with annual revenue exceeding AUS $3 million (Australian Law Reform Commission, 2008). In addition, in 2014 all governmental, private, and not-for-profit organizations had to also abide by the Australian Privacy Principles (APP). These principles established key consumer data rights by allowing Australians to access their personal information that governmental or private organizations have collected, however, these other organizations also have the right to deny this request if they feel that it is "not reasonable or practicable" to fulfil (Australian Government: Office of the Australian Information Commissioner, 2019).

Additionally, Australian data privacy regulations contrast GDPR policies by their definition of "serious harm" when referring to what qualifies as a significant data breach; and therefore, requires reporting. According to the Office of the. Australian Information Commissioner, data breaches that cause "serious harm" "may include serious physical, psychological, emotional, financial, or reputational harm". In addition, there is no distinction regarding who gets to make this determination, whether it be the individuals who were affected or the company that was breached (Australian Government: Office of the Australian Information Commissioner, 2019). In addition, as stated earlier, these policies are only applicable to governmental organizations and private/not-for-profits that have over AUS $3 million in revenue. This is another major limitation, because it is assuming that companies with lower annual income would not be affected or have significant data breaches (Office of the Australian Information Commissioner, 2014). This is contradictory to often prevailing practices in smaller companies that may not focus on cybersecurity. However, as stated earlier,

ransomware and data hackers do not discriminate. And even companies will less than $3 Million in income should be focused on maintaining the privacy of their information. Finally, "consent" is not narrowly defined in any Australian privacy policy. While it is broadly defined in The Privacy Act of 1988, as "express consent or implied consent.", there is no principle that requires an organization to obtain specifically consent of data subjects in relation to collection and storage of their information (The Library of Congress, 2012).

Additionally, after reviewing the privacy laws, it is clear that the Australian government has taken privacy from an economic approach. Everything from the Privacy Act to APP seemingly gives the power to Australians by allowing them to request how their personal information is being collected and used by private companies. However, these same laws also have severe limitations that undermined consumers ability to take control of their information. For example, private organizations can deny these information requests under certain guidelines. And because the privacy regulations do not apply to a large amount of the private sector, the level of data protection is deemed as inadequate, according to GDPR standards established in Article 24 (Watts & Casanovas, 2018).

By discussing how Australia's data privacy laws have lagged behind those of Europe, reveals an important limitation and challenge that faces the Australian government today. In addition, it allows for the discussion on why it is concerning that the Australian government has enacted sweeping governmental surveillance and anti-terrorism programs in recent years while continuing to avoid reforming or considering the impact of these actions of these programs on security policies. It began in 2018 with the Australian Government passing the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 that

allows government agencies to have access to encrypted messages and devices, like Google Homes. While the act has a "golden rule" that prevents law enforcement agencies from building backdoors on systemic weaknesses of software and products. The wide range of activities allowed by law enforcement agencies to conduct in the name of national security is alarming. For example, they are allowed to send a suspect a fake notice for a software update that in fact allows the agency access into the said criminal's messages. They are also allowed to install key logging software and modifying Amazon Alexa to record voices and conversations (Karp, 2018).

While, according to a 2018 report, explains that while Australians are accepting of increasing government surveillance currently, especially when due to protect them from criminal or terrorist plots, a continuous increase in the level of monitoring will result in some people adopting basic measures to "hide" themselves or ultimately lose trust in the government (Kininmonth, Thompson, McGill, & Bunn, 2018). Figure 2 below highlights some of the major advantages and concerns with using surveillance programs in Australia. As you can see, the major concern is that despite the clear public safety benefits of public surveillance by a government, there is a high risk of the system being abused and costly to taxpayers. Finally, the Australian government has given no clear definition of what they consider to be surveillance (Cayford & Pieters, 2017).

Advantages	Disadvantages
Improves Public Safety	Surveillance can be easily abused.
Reduces Crime Rate	Effectiveness of Surveillance is doubted. They do not actually stop physically theft.
Help find criminals better	Expensive to implement and maintain databases and infrastructure.
Can serve as a form of evidence	After time, Camera locations can be known found and criminals can learn to avoid them.

Can be a convenience for everyday life (easier to file insurance claim)	Can be a nuisance for everyday life .

Figure 2 Advantages vs Disadvantages of Surveillance

More concerning, is the current Bill in the Australian legislature, the "Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018." This bill, if passed, would allow for various intelligence and police agencies to request access to your internet and cell phone records. In addition, it would allow the Department of Home Affairs to share identifiable images and information "between government agencies and, in some cases, private organization." While many countries allow for this information sharing between agencies to occur when dealing with a national threat, like a potential terrorist attack, this specific Australian bill would allow for this sharing to occur to "prevent identity crime, support law enforcement, uphold national security, promote road safety, enhance community safety and improve service delivery" (Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018, 2018). This ambiguous agreement for sharing identifying information coupled with the countries vulnerable cybersecurity policies is a major privacy risk. In addition, public surveillance without checks is potentially biased against marginalized communities, mainly Australian Aboriginal populations and immigrants from Asia, India/Pakistan, or of Muslim backgrounds. A report from the University of Sydney released earlier this year reveals a bleak picture of how cultural tension and conflict have manifested in an increase in bias crime where victims are targeted solely because of their identity. The study further presents, for the first time, records from the New South Wales Police force showing that despite the increase in bias crime occurring, the number of formally

reported cases is less than 30% of all cases. In many cases, the incidents go unreported due to either fear by the victims to come forward, or because they do not believe the police have their best interest. This is further impacted by the under-reporting that commonly occurs in bias crimes when reports are finally filed. The report makes a point early on to state that the study shows that "there is much work be done to encourage bias crime reporting amongst marginalized communities and improve the capacity of police to identify and accurately record bias crime" (Mason, 2019). Internal bias is a major concern with government surveillance programs. While some argue the use of artificial intelligence and computers limit the chance of human biases to take place, as long as humans continue to program these software's and commit bias crimes, there will always be the chance that the computer is trained to include these inherent prejudices. The Australian people are putting many of their own personal security and rights given to them by the Privacy Act of 1988 at risk.

Recommendations

Moving forward, checks and policies need to be enacted to protect the privacy of the Australian people. First, I would recommend that an independent governing body, comprised of industry and government watchdogs be created. This group would be allowed to make sure the government is transparent, and honest with its citizens on what data it is collecting and how it plans to use it. It is important to prevent bad actors from accessing sensitive information, as well. This is why I would also propose that the Australian government take a look again at APP and enact clearer, binding right to consumers. The government should take an approach from GDPR and pass a bill that forces all private companies to require consent (written or verbal) from consumers before using their data. Finally, regarding with private companies, there should

be an amendment to The Privacy Act of 1988 to include all non-profit and private companies. It is unfair for majority of Australian private organizations to be excluded from previous rules that were only enforced for companies that had annual revenues over AUS $3 million. Additionally, I would repeal the "Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018." Personally, I believe the bill is too invasive to be enacted without checks in place first. I think that before a nation allows sharing of private information in the name of national security between government, law enforcement, and select-private companies, there need to be specific consumer-focused protections and authorities in place to make sure those with dishonest intentions cannot take advantage of the system. Additionally, the government needs to tread carefully and make sure that its citizens have trust and acceptance of their government.

Some potential drawbacks of these solutions are that the new consumer-focused policies will hurt companies, especially smaller ones, who do not have the capital to make adjustments to their information security system. If the change is too costly for the company to overcome, there will be layoffs or bankruptcy. Secondly, there is the chance that by stoppings these surveillance bills from being enacted, could result in another terrorist attack. Additionally, there is also the potential drawback that if these programs are rolled out, without the cybersecurity infrastructure being updated, they are still very vulnerable to outside and internal breaches. Ideally, changes to the increase surveillance of the Australian public should be rolled out slowly and with clear steps and procedures to maintain checks on the security and process. While this can be a costly method, it ensures better security and chances of data breaches.

Conclusion

In summary, governments of the world enact and update their existing privacy policies to protect private data and information from being accessed or shared by unauthorized parities. In Australia's case the government has rolled out, since 1988 several pieces of legislation protecting the information of privacy of its citizens data. Unfortunately, due to recent terrorist acts and mass shootings on Australian soil, the government has doubled down on its need for surveillance of its citizens. From being able to read encrypted messages of presumed attackers to establishing biometric identifying scanners, the government has allowed itself to trespass on the rights of its citizens. While the intentions are well-intended, checks and measures need to be enacted to these bills to prevent their abuse.

Works Cited

Australian Government: Office of the Australian Information Commissioner. (2019, July 29). *The Privacy Act*. Retrieved from Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/the-privacy-act/

Australian Law Reform Commission. (2008). *For your information: Australian privacy law and practice.* Canberra: Commonwealth of Australia.

Benady, D. (2018, May 31). *GDPR: Europe is taking the lead in data protection .* Retrieved from Raconteur: https://www.raconteur.net/hr/gdpr-europe-lead-data-protection

Cayford, M., & Pieters, W. (2017). The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, 88-103.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION . (2012, October 26). Retrieved from EUR-Lex: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

CyberScout. (2018, February 8). *2017 ANNUAL DATA BREACH YEAR-END REVIEW.* Retrieved from Identity Theft Resource Center: https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf

Gemalto. (2018). *2017 Annual Report- The Reality of Data Breaches.* Retrieved from BREACH LEVEL INDEX: https://breachlevelindex.com/data-breach-library

Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018, 110, 2017–18 (Parliament of Australia May 22, 2018).

Irwin, L. (2017, October 20). *More data lost or stolen in 2017 than all of 2016, but Europe bucks the trend*. Retrieved from IT Governance European Blog : https://www.itgovernance.eu/blog/en/more-data-lost-or-stolen-in-2017-than-all-of-2016-but-europe-bucks-the-trend

Karp, P. (2018, December 7). Australia's war on encryption: the sweeping new powers rushed into law. *The Guardian*. Retrieved from The Guardian.

Kininmonth, J., Thompson, N., McGill, T., & Bunn, A. (2018). Privacy Concerns and Acceptance of Government Surveillance in Australia. *Australasian Conference on Information Systems.* Sydney.

Mason, G. (2019). A Picture of Bias Crime in New South Wales. *Cosmopolitan Civil Societies: an Interdisciplinary Journal*, 47-66.

Meese, J., & Wilken, R. (2014). Google Street View in Australia: Privacy implications and regulatory solutions. *Media Arts Law Review*, 305-324.

Meese, J., Jagasia, P., & Arvanitakis, J. (2019). Citizen or consumer? Contrasting Australia and Europe's data protection policies. *Internet Policy Review*, 8(2).

Office of the Australian Information Commissioner. (2014, March 12). *Australian Privacy Principles — a summary for APP entities.* Retrieved from Office of the Australian Information Commissioner: http://www.awex.com.au/media/1218/35-australianprivacyprinciples_summary_v6.pdf

Olmstead, K., & Smith, A. (2017). *Americans and Cybersecurity.* Pew Research Center .

Stempel, J. (2017, July 3). *Facebook beats privacy lawsuit in U.S. over user tracking*. Retrieved from Reuters: https://www.reuters.com/article/us-facebook-decision/facebook-beats-privacy-lawsuit-in-u-s-over-user-tracking-idUSKBN19O1Q4

The Library of Congress. (2012, June). *Online Privacy Law: Australia*. Retrieved from Library of Congress : https://www.loc.gov/law/help/online-privacy-law/2012/australia.php

Watts, D., & Casanovas, P. (2018). Privacy and Data Protection in Australia: a Critical overview (extended abstract). *Data Privacy Controls and Vocabularies. Position statements & expressions of interest.* (p. 5). Melbourne: Data to Decisions Cooperative Research Centre (D2D CRC).