Submission
No 25

INQUIRY INTO CYBERSECURITY

Organisation: Unions NSW

Date Received: 6 October 2020

6 October 2020

Portfolio Committee No. 1 – Premier and Finance

By email: portfoliocommittee1@parliament.nsw.gov.au

Dear Committee,

Submission to the Inquiry into Cybersecurity

Thank you for the opportunity to participate in the abovementioned inquiry.

Please find **enclosed** Unions NSW's submission.

We look forward to providing further assistance in the inquiry process as required.

Yours sincerely

Mark Morey
Secretary

Unions NSW Submission

Inquiry into Cybersecurity

6 October 2020

Unions NSW
Trades Hall
Level 3, 4-10 Goulburn
Street
Sydney

F: 02 9261 3505

Introduction

1. With every passing month, increasing amounts of personal data are being created, tracked and stored by a diverse range of entities. Particularly during the COVID-19 pandemic, New South Wales has relied on the provision and storage of personal information to monitor the progress of the virus and allow the economy to re-open following various stages of lock down. In addition, the sudden surge of people working from home in early 2020 has necessitated increased access to technology and seen a commensurate increase in creation of data in workplaces which are increasingly online.

2. Unions NSW is the peak body for trade unions and union members in New South Wales with 48 affiliated trade unions and Trades and Labour Councils, representing approximately 600,000 workers across the State. Affiliated trade unions cover the spectrum of the workforce in both the public and private sectors. The union movement has a proud history of engaging in the parliamentary process to protect and represent the interests of working people. Unions NSW frequently makes submissions to inquiries involving industrial relations and other issues which may impact members. We welcome the opportunity to contribute to the Inquiry into Cybersecurity (the **Inquiry**).

3. The Inquiry's Terms of Reference seek practical information relating to the status and operation of current cybersecurity programmes in New South Wales, inevitably better provided by organisations directly involved in this sector. Unions NSW makes this submission as a means of highlighting the risks posed to workers in respect of their data being captured, particularly in workplaces. We believe governments must exercise a cautious, consumer-focused approach moving forward with the increasing use of and dependence on technology. There are secondary impacts and risks of technology, particularly in respect of who owns data and where it creates a risk of exploitation.

4. We are currently experiencing a Fourth Industrial Revolution characterised by a blending of technologies which blurs boundaries between the physical, digital and biological elements of labour[1]. Unions NSW is eager for New South Wales to adopt practices and regulations which promote equity and positive outcomes for workers, employers, consumers and government.

5. Please note this submission is intended to compliment and not supersede any submission from Unions NSW affiliates.

[1] Klaus Schwab, 'The fourth Industrial Revolution: What It Means and How to Respond', *Foreign Affairs* (online), 12 December 2015, < https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>.

Recommendations

In respect of this inquiry, Unions NSW makes the following recommendations:

(1) NSW Government to consider repatriating significant data stored offshore.

(2) NSW Government to develop additional jobs in cybersecurity and ensure these are competitively paid to attract the best candidates and boost the State's capacity in this sector.

(3) NSW Government to immediately implement legislation requiring all agencies to notify serious data breaches to a designated agency. This agency must be in receipt of adequate investment to ensure the NSW Government has the best cybersecurity experts at its disposal to protect State assets and information.

(4) NSW Government to implement regulation of workplace data, including an obligation for all workplaces to have a policy about the lifecycle of workplace data.

(5) NSW Government to designate an existing agency to regulate and enforce workplace data regulation and legislation to ensure protection of all workers and their interests.

Data: The New Oil

6. At the core of all policy schemes and concerns relating to cybersecurity is the data at risk through breaches and mismanagement. Relevantly, data held by the NSW Government which may be made vulnerable by cybersecurity breaches pertains to all citizens of New South Wales in addition to the Government's own employees. This is exemplified by the recent data breach at Service NSW[2].

7. By comparison to former newly monetizable commodities, personal data is akin to the discovery of oil in previously untapped territories. Already, data has been collected for sale through the mapping of roads and communities by Google and residential properties through play-based apps such as Pokémon Go[3]. In this sense, workplaces remain an untapped market and Unions NSW anticipates once companies begin to harvest data from workplaces in earnest, various companies will be willing to pay significant amounts of money to access the information. Unlike oil, the value of data has the potential to increase exponentially over time as this resource itself is constantly expanding.

8. Various agencies within the NSW Government hold significant data about citizens, most notably in respect of our health, education, qualifications, assets and finances and this information has quickly become a valuable resource. Whilst the value of this data is unknown, research about comparable data holdings is instructive. For example, a 2014 report by Lateral Economics showed the value of the Federal Government's open data (being that which is available to everyone) was then $25 billion annually (of the combined direct and indirect values)[4]. Open data is frequently used by governments and corporations to develop business strategy, create apps, inform decision making and to assist in the understanding of economic and other trends[5].

9. The NSW Government is the largest public sector employer in Australia with 407,999 employees in 2019[6]. As a market leader based on size alone, it is imperative protections are put in place by the NSW Government to ensure employees do not become a factory for monetizable data. Unions believe there is a need for restrictions to prevent governments and related entities misusing the data they have collected to guarantee transparency and ethical treatment and use of data.

[2] NSW Government, 'Service NSW cyber incident', *Service NSW* (September 2020) <https://www.service.nsw.gov.au/cyber-incident>.

[3] Cecilia D'Anastasio and Dhruv Mehrotra, 'The Creators Of Pokémon Go Mapped The World, Now They're Mapping You', *Kotaku* (online, 30 December 2019) <https://www.kotaku.com.au/2019/12/the-creators-of-pokemon-go-mapped-the-world-now-theyre-mapping-you/>.

[4] Lateral Economics, *Open for Business: How Open Data Can Help Achieve the G20 Growth* Target (Report Commissioned by Omidyar Network, June 2014) 32.

[5] Australian Government, 'About Open Data' *data.gov.au* (accessed 28 September 2020) <https://data.gov.au/page/about-open-data>.

[6] NSW Public Service Commission, *Workforce Profile Report 2019* (Workforce Profile Report, 2019) 2.

10. It is currently difficult to ascertain what information the NSW Government is collecting about its workers and the impacts of surveillance capitalism on workers[7]. To this end, it is a real concern that information beyond workers' basic personal details (those necessary for the purpose of employment) are being collected, including but not limited to the financial information they may access through work devices, movement and transport choices, their search terms on internet browsers, political engagement and their consumption habits. Unions NSW believes government must implement protocols to deal with the collection and use of this data to ensure worker data is not being sold without its creators' knowledge and consent.

11. Unions NSW's affiliate unions have raised concerns in respect of workplace and employee-generated data. In addition to privacy, unions have detailed instances where data created by workers is used to assess workloads, determine Key Performance Indicators and formulate rostering, leading to a reduction of required duties and significant risk of job cuts. The saleable value of this information will require a simple upscale upon which other employers can engage in workforce planning.

12. In addition to regulatory measures, Unions NSW believes there are significant sovereignty concerns, particularly highlighted during the recent COVID-19 pandemic, which requires the NSW Government to consider the repatriation of significant data currently stored offshore. In addition to maximising the control over and commensurate security of the data, this measure will create jobs for local people; something the State undeniably needs in the wake of the economic disruptions caused by the COVID-19 pandemic. Despite a focus on improving cybersecurity, Unions NSW believes it is vital all Government servers are physically within the State's borders to ensure their security.

13. When creating additional cybersecurity jobs, Unions NSW urges the NSW Government to invest in competitive rates of pay to ensure the most skilled professionals are employed by the Government and our State afforded the best possible protection. This will also assist the NSW Government to become a leader in cybersecurity and extend support and security models to local government and other organisations.

Recommendation: NSW Government to consider repatriating significant data stored offshore.

Recommendation: NSW Government to develop additional jobs in cybersecurity and ensure these are competitively paid to attract the best candidates and boost the State's capacity within this sector.

[7] Donell Holloway, 'Explainer: what is surveillance capitalism and how does it shape our economy?' *The Conversation* (online, 25 June 2019) <https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158>.

Mandatory Reporting Requirements

14. Unions NSW welcomes the NSW Government's announcement of their intention to develop a new Cyber Security Strategy in 2020. We understand the current Cyber Security Strategy, released in 2018 (the **2018 Strategy**), was created as a means to "guide and inform the safe management of the NSW Government's growing cyber footprint"[8]. However, it is clear any new policy must expressly operate to protect the interests of citizens and workers across all sectors.

15. The 2018 Strategy sought to establish mandatory reporting requirements for cyber incidents with the intention information about such an incident would be disseminated to other agencies to mitigate repercussive or associated harm. However, a September 2020 report by the Information and Privacy Commission NSW demonstrates New South Wales continues to operate without mandatory reporting requirements and instead relies on voluntary reporting schemes[9].

16. In practical terms, an agency's decision to not report a data breach may result in:

    (a) reduced ability of other agencies to respond to similar risks or to coordinate a response;

    (b) loss of opportunity to strengthen data breach and privacy processes to avert future breaches and associated loss;

    (c) reduced public confidence and trust; and

    (d) workers' and/or consumers' data being compromised, leading to secondary risks including but not limited to identity theft, financial loss and increased risk of physical, psychological and/or reputational harm.

17. Unions NSW believes the NSW Government must immediately create and enforce mandatory reporting requirements for all Government agencies. Through these reports, New South Wales will be better placed to respond to cyber threats and strengthen cybersecurity capabilities of the whole State.

Recommendation: NSW Government to immediately implement legislation requiring all agencies to notify serious data breaches to a designated agency. This agency must be in receipt of adequate investment to ensure the NSW Government has the best cybersecurity experts at its disposal to protect State assets and information.

[8] NSW Government, *Cyber Security Strategy* (Report, 2018) 3.

[9] Information and Privacy Commission New South Wales, *Data breach guidance for NSW agencies* (Report, September 2020) 3.

Use of Worker Data

18. Transparency must be the overarching principle in developing cybersecurity policy and regulation in the interests of promoting a positive workplace culture and managing the data created by and collected through labour.

19. New South Wales needs stronger workplace regulation to protect workers as technology advances and more personal data is collected in the workplace. In developing this regulation, it is imperative greater visibility is provided in respect of:

    (a) the form and extent of data being created by workers;

    (b) how this data is collected;

    (c) how this data is being stored and where;

    (d) who is storing the data;

    (e) how this data can be accessed and by whom;

    (f) what purpose the collected data is being put to; and

    (g) who benefits from the data.

20. We also believe employers should be required to gain the explicit permission of workers before sharing or using any data produced by them during the course of their engagement or employment.

21. Unions are calling for a legal framework which provides every worker in New South Wales the right to know what data is held about them and the opportunity for workers to benefit from any secondary uses of data created by them. For example, if workplace data is sold to a third party workers should be entitled to any associated monetary gains.

22. Additionally, unions believe all workplaces in New South Wales should have to develop and implement a policy which clearly outlines the ways data is collected, stored and used, and an agreement about who benefits from the sale or other monetizable use of any data created by employees or contractors. As with workplace surveillance, it is imperative workers are actively informed about the lifecycle of data created by them.

23. Finally, the NSW Government needs to ensure sufficient enforcement of laws and regulations pertaining to workplace data. Unions NSW believes the NSW Government should delegate an agency to have responsibility for this task.

Recommendation: NSW Government to implement regulation of workplace data, including an obligation for all workplaces to have a policy about the lifecycle of workplace data.

Recommendation: NSW Government to designate an existing agency to regulate and enforce workplace data regulation and legislation to ensure protection of all workers and their interests.

Conclusion

24. Unions NSW acknowledges the constantly changing nature of cybersecurity concerns and the significant uncertainty of the future of this element of the NSW Government's operation. However, it is also clear New South Wales is significantly resourced and a small enough economy that with adequate regulation and prioritisation of resources we can feasibly address the problems and become a leader in cybersecurity protections and responses.

25. Unions NSW calls for better regulation of workplace data and a framework of transparency to guide the handling and use of worker-generated data. Technological developments are inevitable, and the benefits of increased capacity and productivity must be shared between all parties.

Reference List

Australian Government, ‘About Open Data’ *data.gov.au* (accessed 28 September 2020) <https://data.gov.au/page/about-open-data>

D'Anastasio, Cecilia and Dhruv Mehrotra, ‘The Creators Of Pokémon Go Mapped The World, Now They’re Mapping You’, *Kotaku* (online, 30 December 2019) <https://www.kotaku.com.au/2019/12/the-creators-of-pokemon-go-mapped-the-world-now-theyre-mapping-you/>

Holloway, Donell ‘Explainer: what is surveillance capitalism and how does it shape our economy?’ *The Conversation* (online, 25 June 2019) <https://theconversation.com/explainer-what-is-surveillance-capitalism-and-how-does-it-shape-our-economy-119158>

Information and Privacy Commission New South Wales, *Data breach guidance for NSW agencies* (Report, September 2020)

Lateral Economics, *Open for Business: How Open Data Can Help Achieve the G20 Growth* Target (Report Commissioned by Omidyar Network, June 2014)

NSW Government, *Cyber Security Strategy* (Report, 2018)

NSW Government, ‘Service NSW cyber incident’, *Service NSW* (September 2020) <https://www.service.nsw.gov.au/cyber-incident>

NSW Public Service Commission, *Workforce Profile Report 2019* (Workforce Profile Report, 2019)

Schwab, Klaus ‘The fourth Industrial Revolution: What It Means and How to Respond’, *Foreign Affairs* (online), 12 December 2015, < https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution>