https://www.privacy.org.au

Secretary@privacy.org.au

16 December 2021

Dear Hon. Members, Senators and Ministers,

Open Letter: Frontier software data breach and Ambulance SA data breach

This open letter from the Australian Privacy Foundation (APF) primarily responds to the recent *Frontier software data breach*[1], which rapidly followed on the heels of knowledge about the *Ambulance SA data breach*.[2] As of yet, no publicly available response or remedial follow up has occurred in the context of the Ambulance breach, nor have affected individuals been contacted about the data loss.

The APF, as the nation's preeminent civil society body concerned with privacy, voices community concern regarding both the data breaches.

Information about the Foundation appears at the end of this letter.

We ask for state government ministers to be held to account, by voters and/or through the SA State Records Department[3], for authorising digital platform policies that 'trust for the best rather than anticipate the worst' over recent times.

SUMMARY

Key public and private sector entities, who should be regarded as data custodians rather than data owners, have, in November and December this year, experienced substantive data breaches impacting on thousands of South Australian (SA) individuals: 32,000 people who used the SA Ambulance Service between 2000 and 2003, plus 87,000 current SA public servants.[1,2] The community should hold successive State government ministers into account, electorally and/or through the SA State Records Department[3], for authorising digital platform policies that 'trust for the best rather than anticipate the worst' over recent

decades. The opaque and unwieldy SA privacy protection process is complex, not user-friendly and demonstrably broken.

DETAIL

The Frontier software data breach

The Frontier data breach[1], evidently a ransomware attack, affects around 87,000 SA public servants. Ransomware attacks on Australians, which involve encrypting files so the data custodian cannot use them[4], have risen by 15% in 2021.[5] The SA government acknowledges that the range of information 'ransomed' in the breach includes affected individual's first and last name, date of birth, tax file number, home address, bank account details, employment start date, payroll period and salary (including all tax, superannuation and overall remuneration information).[1] Given that employers often store COVID-19 vaccine certificates, replete with everyone's unique Individual Health Identifier (IHI), on payroll platforms[6], the Foundation is deeply concerned that the compromised SA information includes the most sensitive pieces of government data or metadata about individuals we have to uniquely identify patients for healthcare and taxation.[1] Evidently, some of the 'hijacked' information is currently available for sale on the 'dark web', exacerbating APF discomfort.[7]

The SA government has swiftly attempted to 'mop up' the data breach by offering a range of assistance strategies to employees affected by the breach.[1] These strategies depend upon individual's understanding that their personal information has been compromised and the ways they are likely to be injured in real life as a result of the breach. The government strategies also rely upon individuals to take a range of actions to protect themselves from identity fraud fallout despite the Frontier's contracted stewardship of the sensitive information. Regardless of poor quality security and privacy mechanisms, ostensibly audited in the past, the SA government remains silent about whether they will continue to use Frontier for payroll in future:[1] all care and no responsibility. Unlike in other jurisdictions, where breaches of privacy and data security can and are litigated, in Australia, the price of failure is paid by the data subjects, not the stewards/custodians.

Ambulance SA data breach

The Foundation is concerned the contracted consultancy firm, involved in the breach, that held the lost or stolen legacy data for around 18 years, had stored sensitive and revealing health information supplied by Ambulance SA for research purposes beyond its practical lifetime.[2] The Foundation is concerned that sensitive health information is retained by Ambulance SA to enable service-based research, not the data's primary purpose. The situation is worsened by the fact that unusable data is not apparently audited regularly or securely destroyed after use.

There are no explicit South Australian health data retention laws at present. Instead, the State relies on the interplay between other legislation to protect individual's health data.[8] As this breach demonstrates in the public domain, the current legal situation does not 'work' for those people it directly affects, individual members of the public, while letting the Ambulance Service SA 'off the hook'. This practice is unprofessional and fuels community scepticism about the capacity of all Australian governments to protect the privacy and security of aggregated digital data holdings.[5]

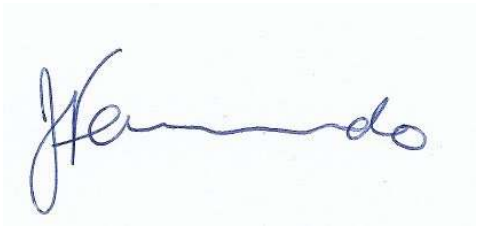
A list of further Foundation concerns about the Ambulance SA data breach are listed in the APF media release attached to this letter.

A thorough analysis of SA government digital privacy strategies is beyond the scope of our letter, but it is disappointing to see no recognition or discussion of the issues of the failure of IT security in the face of common threats communicated on their web site/s.[1] Aggregated data breaches regularly occur country-wide[5], and routinely permit State, Territorial and Federal governments to be certain of escaping responsibility. The singularly weak privacy position of Australians, when their sensitive data is breached, is unacceptable.

CONCLUSION

The urgent need for transparent data collection and storage mechanisms to be implemented across the State, given the rapid pace of technological security and privacy threats, is urgent if the community is to trust digital service implementations into the future. I look forward to your reply, and would be happy to help with developing further responses to these issues.

Yours sincerely,



Dr. Juanita Fernando
Chair, Health Committee, APF
0408131535
Juanita.Fernando@privacy.org.au

ACKNOWLEDGEMENT

I thank the Board of the Australian Privacy Foundation for their contribution to this open letter.

REFERENCES

1. Department of Premier and Cabinet, SA. Frontier software data breach, Available from https://www.sa.gov.au/topics/emergencies-and-safety/types/cyber-security/frontier-software-data-breach
2. ABC News. SA Ambulance Service patients' personal information stolen from consultancy firm, 10 November 2021. https://www.abc.net.au/news/2021-11-10/sa-ambulance-service-data-stolen/100608028
3. State Records. Making a Privacy Complaint, Attorney-General's Department, Government of South Australia. Available from https://archives.sa.gov.au/general-information/privacy-committee/making-privacy-complaint
4. Australian Cyber Security Centre (ACSC). Ransomware, Australian Signals Directorate, Australian Government. Available from https://www.cyber.gov.au/ransomware
5. Davidson, J. 'Terrible mistake' could send execs to jail over vaccine certificates, AFR, . https://www.afr.com/technology/terrible-mistake-could-send-execs-to-jail-over-vaccine-certificates-20211015-p590am
6. Barbaschow, A. The list no one wants to be on – The biggest Australian data breaches of 2021, Gizmodo; December 7 2021. https://www.gizmodo.com.au/2021/12/2021-data-breaches-australia/
7. Barbaschow, A 80,000 workers could be caught up in SA Government payroll provider breach, Gizmodo; 10 December 2021. https://www.gizmodo.com.au/2021/12/sa-government-data-breach/
8. Johns, D. & Smith, R. Storage of Health Records, HWL Ebsworth Lawyers; 28 April 2020. https://hwlebsworth.com.au/storage-of-health-records/#:~:text=In%20South%20Australia%2C%20there%20is,medical%20records%20in%20particular%20circumstances

https://www.privacy.org.au

Secretary@privacy.org.au

https://privacy.org.au/about/contacts/

14 November 2021

MEDIA RELEASE

APF:
Kiss your privacy goodbye when you use an ambulance? The Australian Privacy Foundation says No.

People in South Australia need real answers and real responses to yet another data breach.

The SA Ambulance Service has disclosed that the personal details of 28,000 patients have been stolen.[1]

Those details include people's name, date of birth, age, address, and in some cases, their pension number and health notes.

Juanita Fernando, chair of the Australian Privacy Foundation's (APF's) Health Committee said, "That's prime fodder for identity theft and something we all need to take seriously."

The Ambulance Service says the data was on a storage device that was stolen from a consultancy firm in July. The consultants had apparently held the data since the early 2000s.

There's no indication that the device was encrypted – a basic security precaution.

Neither is there any indication that a proper risk assessment occurred before the Ambulance Service handed over the sensitive personal details about lots of South Australians to the consultants.

Fernando continued, "If you use an ambulance you should be able to have confidence that your private data will not end up in the hands of a consultant and disappear ten years later."

She added, "Those people had no control over the data. The first they knew about the problem was reading it on the ABC website."

The APF calls on the Ambulance Service to provide full disclosure of what has gone wrong. It is insufficient for the Service to say it "regrets" the theft.[1]

The Foundation calls on the Service to immediately take steps to prevent similar problems.

Fernando concluded, "South Australians are entitled to solutions, not regrets and excuses."

Media Release contact for Australian Privacy Foundation Board:

David Vaile, Chair, Australian Privacy Foundation, chair@privacy.org.au. 0414731249

Juanita Fernando, chair, Health Committee, juanita.fernando@privacy.org.au, 0408 131 535

Reference:

1. ABC News. SA Ambulance Service patients' personal information stolen from consultancy firm, 10 November 2021. https://www.abc.net.au/news/2021-11-10/sa-ambulance-service-data-stolen/100608028

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base.

The APF's contributions to policy are based on the expertise of the members of its Board, Committees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Committees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies https://privacy.org.au/publications/by-date/
- Media https://privacy.org.au/home/updates/
- Current Board Members https://privacy.org.au/about/contacts/
- Patron and Advisory Panel https://privacy.org.au/about/contacts/advisorypanel/ The following pages provide outlines of some of the campaigns that the APF has conducted:
- The Australia Card (1985-87) https://privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) https://privacy.org.au/campaigns/consumer-credit-reporting/
- The Census (2006) https://privacy.org.au/campaigns/census2006/
- The Access Card (2006-07) https://privacy.org.au/campaigns/id-cards/hsac/
- The Media (2007-) https://privacy.org.au/campaigns/privacy-media/
- The MyHR (2012-) https://privacy.org.au/campaigns/myhr/
- The Census (2016) https://privacy.org.au/campaigns/census2016/