Cite as: Thompson, N., and Bunn, A. 2020. "Should Australian Government Websites Be Taking More Steps to Protect Privacy and Security?," *Internet Law Bulletin* (23:5), pp 78-81.

Should Australian Government websites be taking more steps to protect privacy and security?

Dr. Nik Thompson. Curtin University
Dr. Anna Bunn. Curtin University

E-Government continues to be embraced by the global community as more public services transition online. Advances in ICT have enabled the delivery of new types of government services, through a variety of digital channels such as email, smartphones, tablets, and smart cards. Central to e-government is the ability to deliver government information and services to support business and the wider community, while also saving time and reducing cost.[1]

However, the expectation for e-government systems to connect to the Internet brings with it many cyber security challenges. According to the Australian Cyber Security Centre (ACSC), 427 security incidents affecting Commonwealth Government entities occurred in 2019, many of which were 'high-profile and complex' and 'had the potential to affect the ability of the Australian Government to effectively serve the public and keep their trust.'[2] State government entities have also experienced cyber incidents: in 2020, for example, Service NSW, the State's official portal for various government services, reported that the personal information of 186,000 customers and staff had been exposed following a cyber-attack.[3] Despite the increased adoption of digital services by Australian government entities, it is clear from the Commonwealth Government's investigations that the cyber maturity of Federal government agencies needs to be improved.

The United Nations E-government Development Index ranks Australia second out of 193 countries in the world.[4] Alarmingly, Australia is also the most targeted country in the Asia Pacific region for cybersecurity attacks[5] and in June 2020 the Australian prime-minister revealed that Australia was subject to an increasing level of sophisticated cyber-attacks across all sectors, including every level of government.[6] Given the Australian Government's goals of making all government services digitally accessible by 2025 and earning public trust through being 'strong custodians' of data,[7] there is a clear need for appropriate security measures within e-government.

[1] France Bélanger and Lemuria Carter, 'Trust and risk in e-government adoption' (2008) 17(2) *The Journal of Strategic Information Systems* 165

[2] 'The Commonwealth Cyber Security Posture in 2019' (2020) *Report to Parliament*

[3] Matt Bungard, *Data of 186,000 customers leaked in Service NSW Cyber Attack* Sydney Morning Herald <https://www.smh.com.au/national/nsw/data-of-186-000-customers-leaked-in-service-nsw-cyber-attack-20200907-p55t7g.html>

[4] United Nations, *UN E-Government Knowledgebase* <https://publicadministration.un.org/egovkb/en-us/data/compare-countries>

[5] Cisco Systems, *Cisco 2018 Asia Pacific Security Capabilities Benchmark Study* <https://www.cisco.com/c/dam/global/en_au/products/pdfs/cisco_2018_asia_pacific_security_capabilities_benchmark_study.pdf>

[6] Prime Minister of Australia, *Prime Minister, Minister for Home Affairs, Minister for Defence, Media Statement* <https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks>

[7] Digital Transformation Agency, 'Digital Transformation Strategy' (2018)

Though this is a topic of widespread interest and relevance, actual data from security audits are scarce. Members of the public have a reasonable expectation that their private data will be protected, but in reality, this expectation is not always met.[8] The following sections of this paper report on an audit of HTTPS (website) security in a sample of government websites in Australia.

Website Encryption

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the protocol used by browsers when accessing and loading web pages over the Internet. Though the name may be unfamiliar, users may recognise the padlock symbol typically displayed in their web browser to indicate that the connection can be considered secure. Originally developed in 1994, this is a mature technology and is compatible with all modern web browsers and smartphone devices. The use of HTTPS provides protection against two major classes of security vulnerability when transacting on the web: eavesdropping and impersonation.

Eavesdropping attacks are possible on the Internet due to its open nature, and the mechanism whereby user data is passed through many intermediaries en route to its destination. Without the encryption provided by HTTPS, any one of these intermediaries can eavesdrop on the communications that are taking place.

Impersonation can occur when a convincing forgery of a website is placed online by an attacker. Users may mistake this website for a genuine service, and unwittingly share their personal or financial details with the attacker. HTTPS can also protect this class of attack through the deployment of website certificates. These certificates provide a chain of trust, enabling a trusted certification authority to vouch for the authenticity of a website.

Sites using Hypertext Transfer Protocol (HTTP) as opposed to the encrypted HTTPS standard are therefore considered a security risk due to the possibility of exposing sensitive data.[9] Unencrypted connections can be vulnerable to eavesdropping and website impersonation, thereby allowing unauthorised access to user data such as ‘browser identity, website content, search terms, and other user-submitted information’.[10]

Survey of Australian government sites

Twenty Australian federal and state government websites were selected at random and audited during 2019 to catalogue the presence of privacy policies, and the use of encryption. Interested readers may also find a more detailed security audit linked in the footnote.[11]

All sites generally fared well in terms of policy coverage, with every site containing a privacy policy, and all but three sites also containing an additional security policy. Privacy policies uniformly covered the main topics around the collection of personal information, the reasons for collecting

[8] Nik Thompson, Ravi Ravindran and Salvatore Nicosia, 'Government data does not mean data governance: Lessons learned from a public sector application audit' (2015) 32(3) *Government Information Quarterly* 316
[9] J. Franks et al, ‘Http Authentication: Basic and Digest Access Authentication’, 1999.
[10] United States Government, *The HTTPS-Only Standard* <https://https.cio.gov/>
[11] Nik Thompson, Antony Mullins and Thanavit Chongsutakawewong, 'Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand' (2020) 37(1) (2020/01/01/) *Government Information Quarterly* 101408

information, and the use of cookies. They also provided further information on how to access personal information held by the relevant department, and how to seek the correction of that information. As expected, these policies align with the requirements of the Australian Privacy Principles (APPs) as set out in the *Privacy Act 1988* (Cth). Universal uptake of privacy policies indicates that this is a well-understood requirement and is standard fare for a government website.

Website encryption, on the other hand, was alarmingly under-utilised, as only half of the tested Australian government sites forced the use of encryption in the form of the HTTPS protocol (in other words, these sites allow only encrypted communications). Some sites provided optional encryption by running both HTTP and HTTPS accessible sites, leaving room for what are known as 'downgrade attacks' in which attackers simply target the least secure protocol available.[12] Further investigation also revealed technical deficiencies in the form of misconfiguration. Five websites which did not force encryption provided it as an option, yet these contained misconfigurations such as expired or invalid certificates leading to a browser error.

Implications for practice

The results of this survey of HTTPS encryption are cause for concern, as they suggest that this fundamental and easily implemented form of security protection is not widely adopted. The fact that only half of Australian government services sites forced the use of HTTPS contrasts with figures from the US, where there is 74% adoption of HTTPS protocol across Federal Government.[13] The US position can be attributed to a combination of legislation in the form of the HTTPS-Only Standard,[14] and transparency, as compliance of federal government websites is publicly displayed.

In terms of the Australian legislative framework, all federal government agencies are bound by the Privacy Act. State government agencies are subject to state-based privacy frameworks, some (but not all) of which contain principles similar to those of the APPs. APP 11 relates to the security of information and provides that a relevant entity that holds personal information 'must take such steps as are reasonable in the circumstances to protect the information (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure'. In determining what protective measures are reasonable in any given case, the OAIC advises that consideration must be given, among other things, to the nature of the entity holding the information — including its size, available resources, and complexity of operations; the amount and type of information held; and the 'practical implications of implementing the security measure, including time and cost involved'.[15]

Given that HTTPS encryption is supported on all modern computers and mobile devices and that the forcing of HTTPS is a measure that is both easily and cheaply implemented, it would seem that the use of HTTPS for all government websites is a reasonable step to secure personal information.

[12] Eman Salem Alashwali and Kasper Rasmussen, 'What's in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS' (Paper presented at the International Conference on Security and Privacy in Communication Systems, 2018)

[13] United States Government, *Pulse* <https://pulse.app.cloud.gov/https/domains/>

[14] United States Government, above n

[15] Office of the Australian Information Commissioner, 'APP 11 Guidance' (2019)

Additionally, federal government agencies must be governed in a way that is 'not inconsistent with the policies of the Australian Government'.[16] Relevantly, these include the Attorney-General's Department's Protective Security Policy Framework (PSPF) and the Australian Signals Directorate's Australian Government Information Security Manual.

The PSPF sets out four core requirements for Information Security, two of which are relevant here: namely the requirement to safeguard information from cyber-attacks, and the requirement to ensure robust ICT systems. In terms of the first of these requirements, federal agencies must, as a minimum, implement certain strategies to mitigate cyber-security incidents.[17]

In terms of the need to ensure robust ICT systems, government agencies must apply the Australian Government Information Security Manual's cyber security principles. These principles include those that are designed to reduce security risks through the implementation of security controls (the 'protect principles'). The protect principles require, among other things, that systems and applications are 'configured to reduce their attack surface' and 'administered in a secure … manner'. They also require measures to be taken to identify and mitigate security vulnerabilities and to ensure that information is 'encrypted at rest and in transit between different systems.' The use of HTTPS encryption for government services websites therefore appears to be a necessary, albeit insufficient, condition for demonstrating adherence to the principles. More specifically, guidelines issued by the Signal's Directorate in relation to web application development recommend that: 'All web application content is offered exclusively using HTTPS'.

Although our security audit revealed some concerning findings with the security of government websites, the Australian Government's recent launch of its 2020 Cybersecurity Strategy will hopefully drive continued improvements in the extent to which personal information is protected across all levels of government. There is some evidence that the forcing of HTTPS protocol by government websites has already improved since the audit reported here was undertaken.

The near ubiquity of modern Internet and communications media will continue to drive further adoption of e-government web platforms. However, it is probably also fair to say that the level of public trust in the security of information provided to such sites could be improved. Thus, the focus for the public sector must evolve from solving technical questions of how to deliver services online (which questions have, for the most part, already been resolved) into how to assure that these online services are the most effective, usable, and safe for citizens.

After all, as observed in a recent report prepared by the Australian Cyber Security Growth Network, '[t]he growing economic dependency on the digital domain has an intrinsic relationship with the trust users and consumers have in it and therefore the security, privacy and resilience of the infrastructure and data.'[18]

[16] *Public Governance, Performance and Accountability Act 2013*, s21.

[17] Australian Government Attorney-General's Department, 'Protective Security Policy Framework' (n.d.)

[18] Australian Government, Australian Cyber Security Growth Network, 'Australia's Digital Trust Report' July 2020, ii.