HopgoodGanim LAWYERS

BLUE COAT

White Paper

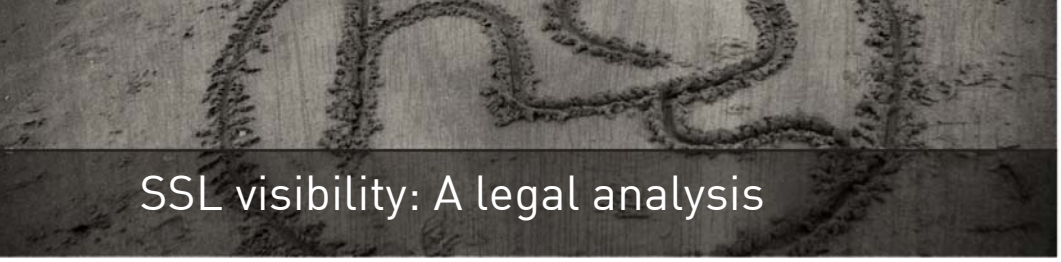
SSL visibility: A legal analysis

Hayden Delaney, Partner Technology and Intellectual Property, HopgoodGanim Lawyers

Sponsored by Blue Coat
https://www.bluecoat.com/solutions/managing-ssl-and-https-traffic

Hayden Delaney, Partner, Technology and Intellectual Property

h.delaney@hopgoodganim.com.au



SSL visibility: A legal analysis

HopgoodGanim LAWYERS

Abstract

Network encryption technologies have become a vital tool for ensuring many forms of online communication can be carried out privately and confidentially. Organisations such as banks, health care providers and other corporations rely on them to handle sensitive information.

The Secure Sockets Layer protocol, or **SSL**, publically released by Netscape in 1995 has arguably become the standard means of protecting online transactions. SSL, which in its manifestation for protecting web interactions is known as HTTPS, has been widely adopted to secure internet services ranging from large financial transactions to photo sharing on social media.[1]

Today, most enterprise and cloud-based applications use SSL and HTTPS to secure network traffic and transactions. This rate is growing over time. 2013 research estimates suggest that already 25-35% of traffic leaving enterprise networks is SSL-encrypted[2], and this number is only likely to grow.

SSL encryption - a false sense of security?

SSL by its nature enables secure communication over the public internet because the traffic appears unintelligible to any third party who might try to intercept it along the way. Typically only the intended recipient can decrypt the traffic. This has the unfortunate side effect of rendering many security tools - designed to find malware or other threats in network traffic - completely blind to threats that may be hiding in such SSL traffic.

So ironically, while SSL was created to enhance online security, a growing number of cyber criminals are using it to hide their activity. Cyber criminals can make use of encrypted channels for covert command and control communications for botnets. Many damaging Advanced Persistent Threats (APTs) find their entry points, or exfiltrate sensitive data, over SSL connections.

As a result, security professionals in many organisations are adopting sophisticated technology that enables them to see inside the contents of SSL communications, so as to inspect it for threats. While SSL visibility tools can increase network visibility and security, they also create additional risks – in particular, the potential for the organisation to gain visibility of information otherwise presumed to be private by employees or customers. Organisations planning to adopt such technology need to carefully consider a number of issues.

This paper addresses some of the key legal Australian issues which need to be considered when adopting SSL visibility tools within your organisation. The paper sets out recommendations on how these issues can be legally managed and addressed by implementing clear and transparent policies, contractual measures and technical controls. As the paper will argue, the legal solutions are ultimately grounded in the principles of openness, transparency and compliance.

Analysis

The use of SSL visibility tools for network security may raise some interesting legal issues. The issues arise from a combination of Australian laws that aim to protect individuals' privacy when using the internet and traditional forms of telecommunication, and others that arise from contract law. It should be noted that the scope of this paper is limited to Australian laws, its analysis is general in nature, and it should not be considered a substitute for independent legal advice.

[1] Technology experts may point out correctly that Secure Sockets Layer is actually an old standard, replaced by the newer Transport Layer Security or TLS. While technically correct, SSL remains the broadly accepted term, and its use here refers to both SSL and its descendants.
[2] NSS Labs, SSL Performance Problems, 2013 https://nsslabs.com/reports/ssl-performance-problems

HopgoodGanim LAWYERS

Interception issues

The Interception Act

The fundamental objective of the *Telecommunications (Interception and Access) Act 1979* is to protect the privacy of individuals communicating over Australian telecommunications systems. Broadly speaking, the act prohibits third parties from intercepting and accessing these communications. However, it also specifies circumstances in which it may be legal to do so.

Section 7 of the act provides that:

> *"A person must not:*
>
> *(a) intercept;*
>
> *(b) authorise, suffer or permit another person to intercept; or*
>
> *(c) do any act or thing that will enable him or her or another person to intercept,*
>
> *a communication passing over a telecommunications system."*

There are three parts of section 7 that are relevant to this discussion. These are "intercept or interception", "communication" and "passing over a telecommunications system".

The act broadly defines "communication" to include a conversation and a message, and any part of a conversation or message (in any form, including signals and encrypted data) carried over a telecommunications network that is within, or partly within, Australia.

It also provides that a "communication" is taken to start "passing over" the telecommunications system when it is sent by the person sending the communication and continues until it becomes accessible to the intended recipient. This is an expansive and broad definition and captures more than just the fixed infrastructure of the telecommunications system.

The act defines "telecommunications system" to include any equipment, line or other facility that is connected to such a network.

The Interception Act and SSL visibility tools

It is clear that any internet-based communication will constitute a "communication" within the meaning of the Interception Act. It is possible that an SSL communication, when encrypted, may not constitute a "communication" within the meaning of the Interception Act on the basis that it does not constitute a "message" or a "conversation". While this point is untested, we would argue that SSL visibility tools that only decrypt certain communications based on policy will help mitigate the risk of contravening the Interception Act.

An SSL communication will "pass over a telecommunications system" from the moment it is sent until it becomes accessible to the intended recipient. Once that communication "ceases to pass over the telecommunications system" it will cease to be subject to the law in section 7 of the Interception Act.

In the context of encrypted communications, we can say that once the communication is able to be decrypted by the intended recipient, it ceases to pass over the telecommunications system. It is the intervening period that needs to be considered and we can clearly see that SSL visibility tools do deal with communications prior to them being accessible to the intended recipient.

The key remaining question is whether an SSL visibility device configured to decrypt SSL communications passing over a network will constitute an "interception" within the meaning the Interceptions Act.

The concept of an "interception" is defined in section 6 of the Interception Act:

> *"... interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system* ***without the knowledge of the person making the communication****."*

SSL visibility tools are indeed capable of being used to listen or record communications without the knowledge of the person making the communication before that communication is accessible to the intended recipient. Therefore, such tools could be used in a way that contravenes section 7 of the Interception Act.

The key to using these tools lawfully is to ensure that there is knowledge and transparency as to their use, and the policies governing such use. If the interception occurs with the knowledge of the person making the communication, then there will be no "interception" within the meaning of the Interception Act.

Example – R v Catena [2012] WASC 144

This view was reinforced in a ruling the Supreme Court of Western Australia recently handed down in R v Catena which has come to be known in legal circles as the Catena Case.

The case concerned two Citigroup brokers that had been subject to an investigation for insider trading offences. Some of the key evidence against them included recordings of telephone conversations between them over their office phones. It was common practice at Citigroup to record all telephone conversations between brokers as part of its quality assurance and governance controls.

The brokers' lawyers disputed the admissibility of the recordings and argued that they were made in breach of the Interception Act.

However, the court found that as the brokers were aware that their calls would automatically be recorded due to clear Citigroup policies and documentation, there was no "interception" and thus no breach of the act. The evidence was admitted.

We would argue that SSL visibility tools are legally no different to Citigroup's phone recorders and, if their use was made clear and transparent, it would be hard for a Court to consider their use as a breach of interception laws.

Privacy issues

Privacy Act issues

The main aim of the *Privacy Act 1988* is to protect Australians' personal information from violations and abuses. The Act regulates the ways in which government agencies and private organisations (with an annual turnover exceeding $3 million) collect, use and disclose personal information within Australia.

Australia's privacy laws have recently been overhauled and since March 2014 so-called "APP entities" have been required to comply with a single set of 13 legally binding Australian Privacy Principles (APPs). The amendments have also, for the first time, given the federal privacy commissioner the ability to financially penalise companies (up to $1.7 million) for serious and repeated breaches of the act. The new Australian Privacy Principles radically impact the way APP entities handle personal information.

The Act broadly defines personal information as any information or opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether it is true or recorded in a material form.

SSL communications will in many instances contain personal information of some kind. As a result, information collected and handled using SSL visibility tools could be subject to the compliance requirements contained in the Privacy Act.

Openness and transparency

One of the fundamental objectives of the Privacy Act is to ensure that APP entities manage personal information in an open and transparent way. The aim of Australian Privacy Principle 1 is to build community trust and confidence as much as it is to enhance accountability for data handling practices.

The Privacy Act specifically requires:

- *reasonable steps be taken to implement practices, procedures and systems that will ensure the entity complies with the APPs – this is sometimes referred to as the "privacy by design" principle; and*

- *having a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information.*

In the context of organisations decrypting the SSL communication entering their networks, the needs of the Privacy Act appear to resonate with those of the Interception Act. Arguably it requires an APP entity to ensure such SSL collection is openly and transparently understood across its user base, and their existence and use to be disclosed in compliance documentation (such as the organisation's Privacy Policy).

Collection

The Australian Privacy Principles call for transparency at both an organisational and individual level. APP 5 clearly obliges APP entities that collect personal information about an individual to take reasonable steps to notify them that it is taking place, approximately at the time when it is collected. However, the definition of collected could give organisations using SSL visibility tools some room to manoeuvre.

Under the Privacy Act, an APP entity "collects" personal information only if the entity collects the personal information for inclusion in a record or generally available publication. The term "record" is broadly defined and includes a document, in a database or an electronic or other device.

This requirement is collection-event specific. In the context of using SSL visibility tools, consideration needs to be given to:

- *when, or if, a collection occurs; and*

- *whether a collection notification statement under the APPs needs to be provided.*

An APP entity does not "collect" personal information where that information is obtained but not included in a record or generally available publication. An SSL communication will not be "collected" by the APP entity unless it is stored electronically (for example, saved into a database).

If an organisation configures the tools not to store personal information automatically – but merely temporarily flag or block certain communications based on policies – then it may be able to minimise the burden of complying with the Privacy Act.

Use and disclosure

The Australian Privacy Principles also prohibit APP entities from using or disclosing personal information for any purpose apart from that for which it was collected. IT security and network managers within APP entities should keep this principle front of mind when using SSL visibility tools. It would be best practice to ensure systems and rules are in place to ensure that the personal information they collect is only used for the purpose for which it was collected. In practice, that should be limited to ensuring network security and preventing data theft.

HopgoodGanim LAWYERS

Recommendations in the deployment of SSL visibility and inspection solutions

Legal and compliance considerations

Compliance with the requirements set forth by both the Inspection Act and the Privacy Act comes back to transparency and openness of how the organisation manages information. Disclosure of the use of SSL visibility tools, and clearly articulated policies for such data collection are very important.

Organisations can provide evidence that they have disclosed the use of SSL visibility tools to monitor their networks in a number of ways, including:

- express contractual acknowledgements and consents as to the use of such tools in employee and contractor agreements and, where appropriate, incorporating terms from policy documents;
- having published policy documents which clearly specify how and when such tools are used and how any data held in connection with the use of such tools will be held, used and disclosed;
- having access and process controls in place which ensure that a user is told (at least, on the first occasion in which they login to the network) of the fact that SSL visibility tools are used on the network. This notification should include information about the tools and web links to the organisation's policy documents; and
- having access and process controls in place which ensure that SSL communications are selectively intercepted and decrypted based on pre-defined criteria reflected in the organisation's policy documents.

Ideally, organisations should consider using all these means when reasonably possible. They provide strong evidence that the tools are used with the knowledge of all persons on the network. Having appropriate, accessible and clearly defined policy documents will ensure there is transparency around how the tools are used and could help avoid legal disputes.

Organisations may also consider including a specific section within the their privacy policy which explains how the tools are used, whether any information will be collected via the tools, how long the information will be held, what it will be used for and whether it will be disclosed to any third parties. Internal information access and process controls can be implemented to audit and track the manner in which staff across all its ranks is using collected information. Once an organisation no longer needs the information then it should destroy or de-identify it.

Technical considerations

It is up to each organisation to explore specific technology solutions most effective to inspect SSL traffic. Information system managers and IT security leaders are best placed to decide the technical architecture best suited for their networks.

However, there are some general considerations for successful deployment of such technologies:

- Ensure the volume of SSL-encrypted traffic within the organisation is well understood (along with consideration of the increasing volumes of SSL traffic across the internet) so that a chosen solution has the capacity to process the volume of information in accordance with policy.
- An effective solution will allow "policy based inspection", providing information security teams with the ability to implement policy at a granular level. This provides flexibility to choose which content their systems decrypt, and which they let pass through encrypted websites (for example, banking or health-related websites). This allows organisations to balance their need to combat security threats to their networks with appropriate protections for employee or customer privacy.

- Organisations should also consider applying rigorous access controls to SSL visibility tools and the data intercepted by them. That should apply even moving up the chain to the most highly privileged users. The tools should also have the capability to securely audit access to decrypted SSL data in order to ensure that all users are accountable.

- SSL visibility tools typically work through the decryption, inspection, then re-encryption of SSL traffic, and have the potential to adversely affect network performance. Organisations should ensure that their chosen technology solutions have the requisite performance to manage these complexities without negatively impacting their employees' or customers' experience.

For further information about SSL visibility tools or any aspect of data protection and privacy, please contact Hayden Delaney, Partner at h.delaney@hopgoodganim.com.au or via phone on 07 3024 0332.