Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Previous submission

In April 2002 the Office of the Federal Privacy Commissioner (the Office) made a submission to the Senate Legal and Constitutional Legislation Committee (the Committee) Inquiry into a number of anti-terrorism Bills. In that submission the Office considered proposed amendments to the *Telecommunications (Interception) Act 1979* (the Interception Act), in particular in relation to stored communications such emails, voicemails, SMS and MMS messages. (The submission is available on the Office's website at http://www.privacy.gov.au/publications/secleg.pdf.)

The Office remains of the position, expressed in that submission, that all forms of telecommunication should, where practicable, be afforded an equivalent level of privacy protection, being that currently afforded to 'live' voice communications such as telephone calls.

The legislation and proposed amendments

The primary objective of the Interception Act is to protect the privacy of individuals who use the Australian telecommunications system. The Interception Act does this by making it an offence to intercept communications passing over the telecommunications system, while balancing this with Australia's law enforcement and national security interests. The Interception Act specifies the circumstances in which it is permissible for law enforcement agencies and the Australian Security Intelligence Organisation (ASIO) to intercept communications under the authority of a warrant, subject to reporting and accountability mechanisms.

The Explanatory Memorandum to the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (the Bill) explains that the practical effect of the Bill is that "it will no longer be necessary to obtain a telecommunications interception warrant, or rely on another exception to the prohibition against interception, in order to intercept a stored communication." This change only has effect for a period of 12 months.

Effect of emerging technology on personal communications

Evolving technologies have led to a substantial increase in the use of stored communications, such as voicemail, email, SMS messaging and MMS messaging. Increasingly, these media are an integral and ordinary part of our personal communication with others, illustrating that such stored communications are little different in how they are used and accepted by individuals, than traditional voice telecommunications, or related technologies such as instant messaging or Voice over Internet Protocol (VoIP).

Increasingly, individuals rely on stored communications for private or intimate conversations, in the same way they would a telephone conversation. As a consequence, reading someone's stored communications is as intrusive as intercepting a voice telecommunication and should be subject to an equivalent level of privacy protection.

Private nature of personal communications

In general, people expect their private conversations, including those via telecommunications systems, to be free from intrusion by state and commercial interests. This expectation is limited where there are prevailing interests of national security and law enforcement relating to serious criminal offences.

Strong justification is needed for the interception of private conversations. The Interception Act recognises that there are circumstances where it is appropriate to allow law enforcement or security organisations to intercept telecommunications. It limits these circumstances, for example to the investigation of relatively serious crimes (e.g. class 1 or class 2 offences). The Interception Act provides a regulatory scheme that ensures any interception of private telecommunications is:

proportional to the seriousness of the law enforcement or security issues involved; limited to only that amount of privacy invasion required; and subject to specific accountability and oversight mechanisms, including a reporting scheme.

All private conversations conducted over the telecommunications system, whether by telephone, internet chat, email, SMS, or other telecommunication means, should, where practicable, be afforded an equivalent level of privacy protection. If stored communications are to be removed from the protections of the Interception Act, however, it appears that a significantly broader range of uses and disclosures of their content would be permitted.

The provisions of this Bill appear to mark a reduction in personal privacy in the context of telecommunications.

Effect of the Bill on private communications

There appear to be two notable privacy risks presented by the provisions of the Bill. First, if the protections of the Interception Act are removed for stored communications, then they will receive the lesser protection of the *Telecommunications Act 1997* (Telecommunications Act). Under the disclosure provisions of the Telecommunications Act (e.g. Division 3 of Part 13), it appears that access to the contents of stored communications would be permitted by law enforcement agencies, a range of Commonwealth agencies, and possibly others, in relation to the investigation of a broad range of illegal activity, fraud and the protection of public revenue. Similarly, ISPs and their employees would have a broad capacity to disclose the contents of stored communications in the performance of their duties. In addition to permitting disclosures for specified purposes, this Division of the Telecommunications Act includes general provisions such as s. 280(1)(b), which appears to permit disclosures by telecommunications carriers and carriage service providers, such as ISPs, that are "required or authorised by law".

The Office has not been able to conduct a thorough analysis of the full scope of the protections for stored communications provided by the Telecommunications Act. The examples of permitted disclosures listed above, however, indicate that a much broader range of uses and disclosures of the content of stored communications will be permitted than is presently the case under the Interception Act (e.g. disclosure to Commonwealth agencies acting to protect the public revenue, or to law enforcement agencies investigating minor offences).

Secondly, by establishing a different regime for the protection of stored communications in contrast to 'live' telecommunications, this Bill also raises the risk that individuals may lose confidence in the privacy and confidentiality of modern forms of telecommunication.

Considered overall, the provisions of the Bill appear to represent a shift in the balance between the private nature of personal communications and the ease with which law enforcement bodies and some government agencies can intercept such communications.

Email monitoring and network security

The Office notes the concerns raised by the Australian Federal Police (AFP), in its submission to the Committee's Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2004 (the February Bill), regarding e-security and corporate governance.

The Office agrees that it is appropriate for owners and operators to be able to protect their computer networks against malicious software, such as viruses, and to undertake content monitoring under certain conditions.

If there is continued legal uncertainty about whether such activities may contravene the Interception Act, this could be resolved by amending the legislation to ensure that while protection is maintained for personal telecommunications generally, e-security and corporate governance measures are permitted.

Conclusions

In the view of the Office, stored communications should generally be afforded no lesser protection than is presently the case; the same level of protection, for example, as intended by the February Bill, subject to the e-security and corporate governance issues noted above.

In the event that the current Bill is passed in its present form, the Office would strongly support a review of the Interception Act as foreshadowed by the Attorney-General in his second reading speech. This provides the opportunity to comprehensively review the provisions of the Interception Act, including the impact of the current Bill, and to consult widely on its application.