ISPs and the balance between personal privacy & public law enforcement

Andrew Stone, University of Sydney

Andrew Stone BA (Hons), LLB (Hons), University of Sydney. Andrew graduated from the University of Sydney in 2003.

1 Does privacy exist? If so, how may privacy be defined?

In order to determine whether Australian law strikes an appropriate balance between privacy interests and national security and law enforcement, it is first necessary to consider whether privacy exists, and if so, how privacy is defined.

Some commentators have suggested privacy is a fantasy.[1] It appears Padraic McGuiness intended to suggest privacy does not exist when he stated: "when people all lived in villages, everyone else had a pretty good idea of everyone else's business."[2] However, contained in the statement of McGuiness' is an implicit acknowledgement that privacy exists. His metaphorical 'villagers' did not know the full 'extent' of information relating to everyone else's business; they knew a lower extent – in McGuiness' words: merely a 'pretty good idea.' The gap between knowing the 'full extent', and holding a 'pretty good idea' demonstrates the villagers (either consciously or unconsciously), did not communicate the full extent of information about themselves to others. This demonstrates that privacy exists.

Having determined that privacy exists, privacy can be defined as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[3]

2 How Important is privacy?

Privacy is important, but so are competing policy issues, like law enforcement. Many privacy fundamentalists appear to believe that personal privacy is more important than public law enforcement,[4] and if privacy is compromised, then law enforcement will override privacy to the extent that, in theory, one's entire existence can be reduced to the numbers on a barcode contained in a file.[5] Such a belief is based upon the assumption that at some future time, the online world will be the only world, and within that electronic world, super efficient digital law enforcement will completely overwhelm the more abstract notion of personal privacy. These assumptions are flawed because the physical world will remain. *The Matrix* has great special effects, but the idea that machines and centralised law enforcement authorities will be the ruin of society has been around since the Luddites of the Industrial Revolution, yet humanity is still going strong.

In order to ameliorate particular problems associated with government use of personal information identified by privacy fundamentalists,[6] an appropriate balance of privacy and law enforcement objectives is required.

An appropriate balance to privacy and law enforcement in the online environment is one that engenders trust rather than security. Nissenbaum argues trust in the online environment is not achieved through an 'us versus them' approach.[7] Applying that general approach, this paper argues that trust is achieved through rigorous evaluation of both policy objectives by independent adjudicators.

3 Does Australian law strike a balance between personal privacy interests and public law enforcement?

ISPs may be faced with a conflict between the privacy of their subscribers, and the objectives of law enforcement agencies in a number of contexts in the course of business dealings with subscribers. The following examples indicate that Australian law strikes a balance in some, but by no means in all such contexts.

3.1 Appropriate balance:

a) Interception Warrants under the *Telecommunications (Interception) Act 1979*

Interception warrants for law enforcement purposes under the *Telecommunications (Interception) Act 1979* are examples of an appropriate balance in Australian law. Interception warrants are legal authorisations for law enforcement agencies to intercept:

> "communications passing over a telecommunications system, including listening to or recording by any means a communication passing over that telecommunications system without the knowledge of the person making the communication."[8]

The person seeking to intercept must apply for a warrant from an arbiter who may be either an eligible judge, or a nominated member of the Administrative Appeals Tribunal.[9] Where the relevant suspected offence is a Class 2 offence (an offence punishable by imprisonment for at least seven years and meeting certain other requirements) the relevant arbiter must consider the privacy of persons whose communications are intercepted.[10] This administrative process engenders trust because it requires objective consideration of both law enforcement and privacy policy interests.

As risk to life[11] or national security[12] rises, so the formalities required in relation to the procurement of a warrant diminish.[13] This does not undermine trust because the

conventional objective process is the norm. The merits in terms of trust of the normative process are enhanced through principles such as those enunciated in *Taciak*, where Sackville J held in obiter that a restrictive approach to the construction of legislation authorising the use of information for specific purposes should be applied.[14]

Where the relevant suspected offence is a Class 1 offence (for example – suspected murder or kidnapping),[15] there is no explicit requirement for the relevant arbiter to consider the privacy of the individual whose communications are being intercepted.[16] This is in clear distinction to the requirement for an arbiter to consider an individual's privacy in relation to a suspected Class 2 offence.

(b) Telecommunications Industry Ombudsman Scheme

This scheme in an excellent example of an authority that engenders trust. The Telecommunications Ombudsman Scheme is a cost free alternative dispute resolution scheme which investigates complaints received from consumers in relation to a telephone or internet service. As Magnusson notes, its independence from both government and industry is its fundamental strength.[17] This objectivity is the key to building trust.

(c) Decryption requirements under the *Telecommunications Act 1997*

The encryption and decryption of electronic data is an important issue in the context of the internet. Currently, Australian law does not restrict the use of cryptography on telecommunication networks. Part 15 of the *Telecommunications Act 1997* simply imposes a duty upon ISPs to: "maintain an interception capability which is compatible with international standards."[18] ISPs and law enforcement agencies may reasonably query: does this duty to maintain an interception capability "compatible with international standards" mean that an ISP must maintain a capability to decrypt communications passing over the network for the benefit of law enforcement agencies in Australia? The UK legislation will be relevant in this context.

Under UK law, individuals holding a decryption key will be required to disclose the decryption key to law enforcement agencies seeking disclosure of the decrypted data if disclosure is: "proportionate to what is being sought to be achieved by its imposition".[19] On its face, this drafting appears to leave open an interpretation whereby the law enforcement objectives which prompted the disclosure application must be balanced by, or "in proportion to", the privacy costs imposed upon a person whose data is being decrypted. If this interpretation of the UK Act is valid, then the UK approach offers an appropriately balanced and objective model, on which basis the approach may be useful to apply in the Australian context.

3.2 Imbalance

(a) Risk to privacy interests through section 282 of the *Telecommunications Act 1997*

Disclosure by an ISP of information[20] under the *Telecommunications Act* is an example of an imbalanced approach to privacy and law enforcement in the online environment. The disclosure of the contents or substance of a wide range of communications listed in Division 2 of Part 13 of the Act is not prohibited under section 282 of the Act if the disclosure is 'reasonably necessary' for the enforcement of, amongst other things, the criminal law.[21]

The process for determining what is 'reasonably necessary' is not objective. For this reason it does not engender trust, thus it cannot be defined as a balanced approach. ISPs can either make a unilateral evaluation,[22] or they can rely on certification by the requesting agency,[23] in relation to whether the disclosure is "reasonably necessary" under section 282.

(1) Unilateral evaluation:

In 2000-2001, telecommunication companies passed on information 524,253 times.[24]

Even if it is assumed that just a fraction of these telecommunication companies were ISPs, it is unimaginable that ISPs would make a unilateral evaluation in every case. Many ISPs do not consider themselves as the gatekeepers of the online environment, on which view unilateral evaluation would be acceptable to ISPs. ISPs may be considered 'common carriers'.[25] As such, ISPs would feel no duty to make a unilateral evaluation. Even where the ISP did make a unilateral evaluation, there is no guarantee they would adopt an objective approach. So, the extent to which trust through objectivity is engendered through section 282 depends upon largely upon the certification scheme.

(2) Certification scheme:

The current certification scheme under the *Telecommunications Act* is an imbalanced approach to privacy and law enforcement because it lacks objectivity. All that is required for disclosure is for an authorised officer[26] of an agency to certify that the disclosure is 'reasonably necessary' for enforcement of the relevant law.[27] This effectively subjective definition of 'reasonably necessary' creates the imbalance. The definition does not integrate privacy policy objectives. The certification scheme is essentially a process of rubber-stamping to facilitate law enforcement objectives alone.

(b) Risk to law enforcement interests – *Telecommunications (Interception) Act 1979*

Interceptions which are "passing over a telecommunications system" may be intercepted under the *Telecommunications (Interception) Act*.[28] The definition of "passing over" in this context is considered to be ambiguous.[29] Without clarification, this ambiguity appears to preclude the interception of an email message at rest on the computers of the addressee's ISP. However, an alternative interpretation is open under which such an email can be considered to be "passing over a telecommunications system", despite its lack of motion.

In order to clarify the ambiguity which exists in relation to this section, it is profitable to recall the distinction drawn by US lawyer Lawrence Lessig between the internet and the telephone system. The internet's design is end-to-end. In other words, intelligence in the network is kept at the ends, where the end is the end-user, not the computers within the network.[30] Lessig analogises the internet's end-to-end design with a motorway:

> "as long as the car is properly inspected and the driver properly licensed, whether and when to use the highway is no business of the highway."[31]

It is possible to extend Lessig's analogy in order to establish that an email at rest on the computers of the addressee's ISP is "passing over a telecommunications system." It is arguable that a car stopped on a motorway, for example at a toll booth, is still "passing over" the motorway despite its temporary stop, because it is absurd to suggest that a car stopped at a tollbooth has passed over the motorway and has thus completed the journey on it. "Passing" in this context means the process of transit from end to end rather than motion.

If this analogy were applied, then a communication is "passing over a telecommunication system" when resting at the addressee's ISP, prior to receipt and reading by the addressee. This means it can be intercepted pursuant to section 7(1)(a) of the *Telecommunications (Interception) Act.*

4 Conclusion

Both personal privacy and public law enforcement objectives are vitally important to an open society. An approach by policymakers which engenders public trust through objectivity and a balanced approach in relation to both priorities is most likely to facilitate ongoing public acceptance of online technologies.

This paper identified that a balanced approach currently exists in Australian law in relation to interception warrants under the *Telecommunications (Interception) Act 1979* generally, and a balanced approach exists under the Telecommunications Industry Ombudsman Scheme. In relation to decryption requirements under the *Telecommunications Act 1997*, international standards are relevant. To the extent that UK decryption requirements may be considered an international standard for the purposes of the *Telecommunications Act 1997*, then because the UK approach to decryption balances personal privacy and law enforcement objectives, the Australian law in relation to decryption will be similarly balanced.

However, the paper demonstrated that a balanced approach does not exist in some areas of Australian law. Privacy objectives are not integrated under section 282 of the *Telecommunications Act 1997*. Additionally, law enforcement objectives may be compromised under the *Telecommunications (Interception) Act 1979* where an email communication is at rest on the computers of the addressee's ISP.

These areas of law indicate that a better balance between the two policy objectives of personal privacy, and public law enforcement could be achieved in Australian law.

---

1 Eg Scott McNealy CEO Sun Microsystems at a product showing in 1999: "You already have zero privacy: get over it". Quoted in Rosen, J "The Eroded Self", *The New York Times* April 20 2000 p46.

2 McGuiness, P, *The Age* 27/5/95. Similarly Scott McNealy's comment at a 1999 product showing: "You already have zero privacy: get over it" carries with it the implication that privacy does not exist.

3 Westin, A, *Privacy and Freedom* (1967) 7.

4 See for example, Cohen, J, *Information Rights and Intellectual Freedom* in Ethics and the Internet Anton Vedder (ed) Intersentia, Antwerp 2001.

5 Rosen, J, "The Eroded Self", *New York Times* April 30, 2000. See also Kang, J "Information Privacy in Cyberspace Transactions" 50 Stan.L. Rev. 1193 at 1198.

6 Singleton, S, "Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector", *Cato Policy Analysis* No. 295, January 22 1998 p.20.

7 Nissenbaum, H, "Securing Trust Online: Wisdom or Oxymoron?" 81 B.U.L. Rev. 635.

8 *Telecommunications (Interception) Act 1979* (Cth) s6(1).

9 *Telecommunications (Interception) Act 1979* ss 6D, 39-40.

10 *Telecommunications (Interception) Act* ss45-46.

11 *Telecommunications (Interception) Act* ss7(2)(c).

12 *Telecommunications (Interception) Act* s9.

13 *Telecommunications (Interception) Act* s7(4)-(8), s10.

14 *Taciak v Commissioner of Australian Federal Police* 131 ALR 319 per Sackville J.

15 *Telecommunications (Interception) Act* s5.

16 *Telecommunications (Interception) Act* s45-45A.

17 Magnusson, R, "Australia's Changing Telecommunications Environment" (1999) 27 *Federal Law Review* 33 p.67.

18 For a discussion of different types of encryption and decryption infrastructure, see Magnusson, ibid at p.60-65.

19 *Regulation of Investigatory Powers Act* 2000 (UK) Part III Section 49 (2)(c).

20 *Telecommunications Act 1997* (Cth) s276(1).

21 *Telecommunications Act* s282.

22 *Telecommunications Act* s282(1) & (2).

23 *Telecommunications Act* s282(3).

24 Answer to Question on Notice No. 150, House of Representatives Hansard, 19 March 2002. Quoted in Yeng, T, "An ISP's responsibility for co-operating with government agencies in Australia" (2002) 5 (2) *Internet Law Bulletin* p.13.

25 Huston, G, "The ISP – the uncommon carrier" *ISP Column*, January 2002.

26 *Telecommunications Act* s282(10).

27 *Telecommuniations Act* s282 (3), (4), (5).

28 *Telecommunications (Interception) Act* s7(1).

29 Magnusson, op cit at p.57.

30 Lessig, L, *The Future of Ideas* Random House, New York 2001, p.34.

31 Ibid, p.39.