A WORKING JOURNALIST'S PERSPECTIVE ON SECURITY

John Hilvert

As a journalist, frankly these are dark times. These are very dark times because we have a situation where it seems that national security has led to a conflation of a whole series of issues, in terms of control, in particular control of our telecommunications. Those of you who are in the game will probably be aware, the Attorney-General is currently circulating a discussion paper which proposes more direct day to day control of the operations of our telecommunication companies (Telcos) and our internet service providers (ISPs). In the past, that was available theoretically if triggered by a national emergency.

We do not know how that discussion paper will be received. But effectively it means day to day supervision of our Telcos and our ISPs is being sought in the name of national security. To what extent this will limit what our Telcos and our ISPs who are supposed to be at the vanguard of innovation can do, is of concern.

A typical example might be AARNet, a major internet provider. It is probably one of the fastest ways you can get telecommunications and operates a multi-gigabyte network and the way it does its communications is through software. It uses very advanced software and the problem with the requirement that the Attorney-General's department (AGs) or a delegate of that agency can access AARNet is that supervision effectively stops any change to that software for fear that it may, in some way, undermine national security.

In relation to the current legislation one of the first things you need to know is that as at August 13, which is a little over three weeks away, ISPs are expected to submit to the Attorney-General, their plans for complying with the mandatory data regime. This is made difficult because most of the details of what are actually required, are yet to be made available. So we have a situation where there is a mandatory order on all our Telcos and ISPs of which many are ignorant and most are uncertain. Now there are provisions for extensions of time to be granted. I expect these will be sought for the August 13 deadline, but it indicates some of the outrageous requirements that are going on at the moment.

Turning to my life as a journalist with this mandatory data regime, let me start by putting on my other hat, which was as the former communications manager at the Internet Industry Association (IIA). I left that role about five years ago and the Internet Industry Association is now represented by the Communications Alliance, which is doing an excellent job.

While I was with the IIA, I learned that in 2010 and earlier the Attorney-General's department was really keen to have access to metadata. That was under Labor, of course. And being good industry associations, we said 'yeah sure you can have our

metadata, but how do you want it, in your database? in a central database? or do you want us to keep it?'

The response was: 'I don't know'. About a year later, we heard from the department 'I don't think we can keep it centrally. Can you keep it yourself?'

We said 'Fine, but how much are you willing to pay us for the storage and security?' The officials went away again. In the end, I think they figured it sounded a bit too smelly to have a big database of everyone's internet data under government control. In the United States (US) such a proposal was tossed out. More or less the same response occurred in the United Kingdom (UK).

In the end, the current government finally said, 'Well okay, we'll pay for it but the ISPs have to look after it'.

That's more or less the current position. The current estimate for this massive database is something like half a billion dollars in public money to fund all those ISPs. I estimate there are about 50 ISPs in Australia, and maybe 80 per cent of users are accounted for by the top five. But ISP operations are all over the place. That is the big issue. As a tech journalist, I know that many ISPs have got, at most, maybe two security people looking after their operations. They need them to secure the privacy and integrity of their communications.

So our ISPs will now have to store and secure personal data in a way they have never done before. And the inevitable will happen, there will be a breach, there will be a massive breach. It may not be Telco, it may not be Telstra, it may not be iiNet, but it may be some local ISP that will get hacked. It will happen.

It is so easy to get hacked these days. You just have to see what is happening in America. There they have far more people looking after security. The Office of Personnel Management (OPM) in the US Department of Defense got hacked. So the odds are the Australian ISP database is going to be hacked and many journalists, are anticipating it. It is on our 'risk management matrix'.

Indeed I suspect the government is also anticipating it, because that will be the basis on which the government will say, 'Well look, we cannot really trust personal metadata, vital for national security, be left in the hands of these ISPs. They are mainly concerned with communication and profit. We'll take it on and we'll do it more efficiently'. I think that is the end game, and I predict it will occur in the next 6-12 months.

To finish off, I will discuss the journalist information warrant for enthusiasts interested in this area. The journalist information warrant was the basis upon which the Labor Opposition finally said yes, we need to follow this up. We will back mandatory data retention because journalists will be protected. If you search the legislation, the journalist information warrant is an entirely secret process. Journalists would also be forbidden from disclosing information about the new journalist information warrant — including the 'existence or non-existence' of such a warrant and any failed attempt by government to pursue a journalist's communication records. Doing so would be punishable by two years' imprisonment.The Prime Minister appoints a public interest

advocate to argue a position when an application for a journalist information warrant is sought, but the advocate will have no contact with the journalist or the media organisation. There is no trigger to determine when an advocate will be called. The grant of a warrant relies on 'snoops' officially noting that a journalist's data is about to be accessed without a warrant. The advocate will only be required where the authorising body knows or reasonably believes there is a journalist whose metadata is involved, and the purpose of the authorisation would be to identify another person known or reasonably believed to be a *'source*'.

There is no monitoring or reporting mechanism for the number of times a journalist information warrant will be sought, granted or denied. We know from the Australian Federal Police (AFP) that they had at least 13 attempts to access journalist information last year. That figure is for the Australian Federal Police alone. There is no monitoring or reporting mechanism for the number and type of metadata utilised under the authorisation, nor the number of journalist relationships that may be examined and possibly compromised.

The definition of 'professional journalist', the term used in the Act, is much narrower than under Commonwealth shield laws. These laws were enacted because there was a realisation that journalists had an ethical requirement to protect their sources. If a journalist said 'I am duty bound to protect a source', the shield law process would be activated and the issue of whether the shield should apply would be considered by a judge. There is a discretion whether the journalist information would be made available to the court.

But the definition of a 'professional journalist' for the purposes of grant of a warrant appears to be narrower than that covered by the present shield laws. It may mean a freelance journalist, of which I am now one, may miss out on that protection. It could mean bloggers miss out and it could mean journalists writing a book rather than an item for publication in the news media could also miss out.

Finally, and most disturbingly, there is no testing of whether a journalist warrant has been actually granted to require information or metadata from an ISP. According to guidelines supplied to ISPs by the Attorney-General's department, if an ISP receives a request for information or for metadata, the ISP will have to take the agency at its word that it has obtained a warrant to access the metadata of a journalist. The ISP will not be able to see the warrant to verify the grant before handing over the data.

The actual answer to the frequently asked question in the guideline (FAQ) is interesting. It says, *'The data retention obligations do not alter the powers relevant to making requests. Service providers should expect that the kind of request they receive will change only to the extent that once the data retention regime is fully implemented requested data within the prescribed data may be 2 or more years old*'. That is it.

In other words, there will be no testing. The checks that the Attorney-General' department s and the government are relying on are *post hoc* checks. As far as I am aware, there are no actual checks. What I would have been very comforted to have seen is for a scheme in which a proportion, maybe, 1 in 1000, accesses to metadata without a warrant were subject to an Ombudsman overview. I do not know if that is

possible, but that would be something that might have given me some comfort. In fact, the checks that I can see would be provided a long time after the event.

I am very unhappy as a journalist to see what is happening with these laws. Basically the system relies on trust. Do we trust our government to follow through in an appropriate way? I leave that as an open question.

Q What's the point of enacting some sort of privacy right of the type that's just been described when in every other area of information law such as defamation, suppression orders, etc, the internet is proving that the existing laws are very difficult to make work. How would you make Facebook, Google or some other multinational corporation respect our privacy laws in practice?

JH Many of the software companies that we know of are deliberately fixing it that the user has the control of access to their information and their own encryption keys. Those companies stressed they don't hold encryption keys, 'If a user loses them they lose them, they can't come back to us,' has been a common response. That's quite vital, because they need to have the confidence for people to use their services and the only way they can do that is by taking it up to the Government.

Q A question European Union regulators have been looking at is the right to be forgotten. The holding of data by any particular agency or corporation is time limited, so there is effectively a time code against any data retained and as soon as that time code reaches zero then the data must be deleted. I wonder if any of the panel had any knowledge about that kind of thing aimed at organisations such as Google, Facebook and so on.

JH I understand Google actually will signify whether or not the Act has been used in some way and I think that was one of the consequences of that action. Google's doing it as part of their transparency requirements, so you'll often find Google will indicate how often it's been asked to respond to Government access to the records and the like. I think it's an interesting earlier attempt to recognise some personal rights. You'll find that the transparency and accountability requirements of these mega software companies require them to account for any changes at all and some of that is designed to show that they are as open and transparent as possible, notwithstanding some harms that may have been caused to some of the people.

Q I'm all in favour of a statutory right to privacy and all of that sort of thing, but aren't we really confronted with the problems that most people are prepared to surrender privacy. They take out Coles and Woolworths cards which record all of their purchases so that the retailers can get back at them and know exactly what they've been doing, they go into quizzes which find out their personal details and there's no 'oh, we will protect your privacy when you enter this little competition'. You've got an odd chance that you might win something but we really would love to have all of this information. You have millions of people throwing away their privacy and this is in addition to Facebook, etc. So what are you going to do, do you want to force people not

to do that? Do you want to force the people who are collecting this information to not use it? We are in a commercial situation in which for one reason or another a great majority of people surrender their privacy.

JH It's about informed consent really. If I volunteer information in response to a survey, a typical thing might be with the website Trip Adviser which asks me, how was my last trip to Budapest. That's informed consent but if I see that being used outside the terms of my review, I will be very unhappy. My colleague Roger Clarke former chair with the Australian Privacy Foundation has actually been tracking surveys of privacy awareness. Contrary to our beliefs from social media, there is a *heightened* concern rather than a lower end concern about our privacy awareness. It's more nuanced and as long as there is some informed consent, I think it's understood.