iinet
connect better

Submission

SENATE STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

COMPREHENSIVE REVISION OF TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979

Sydney
29 July 2014

Contents

Introduction	3
Not ‘just’ metadata	3
Examples	5
Twitter	5
Websites	7
Facebook	8
Mobile telephone	9
Wearable devices	10
Routinely collecting data?	11
Implications for industry	12
A Standard System	13
Conclusion	14
References	15

Introduction

Thank you for your invitation to the iiNet Group to offer comments to this Committee. I am Stephen Dalby, iiNet's Chief Regulatory Officer. My colleagues are Leanne O'Donnell, iiNet Regulatory Manager and Roger Yerramsetti, iiNet Operations Manager.

We have previously provided a written submission[1] in which we elaborated on our concerns with the proposed mandatory data retention regime. Our conclusion in that submission was that proponents of such a scheme grossly underestimated the volume of data to be collected, and the consequential costs flowing to those companies forced to undertake the proposed surveillance of the Australian population.

On this occasion, we offer additional information on the poorly defined but freely used term – metadata.

Given that various public comments have indicated that the full set of metadata may not be required to be retained, we will illustrate our observations that stem from an apparent requirement for ISPs and carriers to not only collect metadata, but also to process the metadata to redact or remove the content from the metadata, which appears to be surplus to requirements.

It is important for us to note that contradictory and confusing comments from law enforcement agencies and government sources, regarding this subject, have led us to base our comments on a range of inputs, as well as interpretations and assumptions of those inputs. The documented descriptions of metadata, that have been provided, lead us to believe that a full set of metadata is preferred, however, public comments have also suggested that a much smaller sub-set is acceptable.

A definitive statement outlining the government's requirements would reduce the uncertainty and enable us to more meaningfully respond to any proposed data retention regime.

Not 'just' metadata

In an Internet protocol (or IP) online environment, metadata is pervasive and extensive. Metadata underlies all communications. It is fundamentally misleading to downplay the degree of intrusion of data retention regimes, such as those which operate at the European Directive level. A false assertion is that such regimes do not include the actual content of what our customers might be communicating. These inaccurate distinctions are dangerous and inappropriate.

It is misleading to assert such data is 'only' metadata or 'just' metadata. Metadata reveals even more about an individual than the content itself.

As I'll expand shortly, a post or a 'Tweet' on the social media platform Twitter is considered to be a very limited or concise form of messaging. A single Tweet is only allowed 140 characters, but it is important to understand that, as a piece of communication, a Tweet could contain 40 fields of metadata, comprised of thousands of characters.

This metadata can be used to extract more information that the content. In May this year, David Cole, a Professor in Law and Public Policy at Georgetown University Law Center reported[2] a number of points, including:

- NSA General Counsel Stewart Baker has said, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."
- General Michael Hayden, former director of the NSA and the CIA, called Baker's comment "absolutely correct," and frighteningly raised anxiety levels by asserting, "We kill people based on metadata."[3]
- [Conversely] the Privacy and Civil Liberties Oversight Board has found that there is little evidence that the metadata program has made us safer.[4]

Caspar Bowden, a specialist in EU Data Protection and European and US surveillance law has argued[5] that:

- retention is like having a CCTV camera installed "inside your head" that is, that it invades the subjective interior space of our thoughts and intentions, because these can be inferred from Internet and other metadata;
- It is incompatible with human rights, in any democracy, to indiscriminately and continuously collect communications data or metadata on the entire population. The essence of the freedom conferred by the right to private life is that official infringements must be justified and exceptional.

The EU Advocate General, Pedro Cruz Villalón, in his opinion[6] supporting the overturning of the EU Data rRetention Directive:

- Argued the retention of such data "may make it possible to create both a faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity."
- He also highlighted the risk that the retained data might be used illegally in ways that are "potentially detrimental to privacy or, more broadly, fraudulent or even malicious".
- He expressed concerns that data retained under the directive is not held by public authorities but by the providers themselves; and that it does not need to be physically stored in the EU but can be kept on servers anywhere in the world.

The complex, voluminous, often sensitive and private nature of data, sought under a mandatory data retention regime, exposes the hollowness of the claim that communications data or metadata is "just like the envelope without the contents". The difficulty with such an analogy is that it attempts to compare a piece of paper (the envelope) with a chain of events and links to myriad other data, meticulously described and recorded.

In the case of Twitter, this may include who wrote the tweet, their biography, their location, when it was written, how many other tweets have been written on that user's account, where the author was when the tweet was posted, what time it was, who it was sent to, where the author is based and, surprisingly, in the case of Twitter, the 140 characters of content in the tweet, as well.

Using faulty analogies to explain complex issues, with the frequent use of the word 'just', is risky and misleading. As the ACLU explained in their report[7] on metadata and privacy a URL is both metadata (a delivery instruction) and is also content:

- requesting a web page essentially means sending a message saying "please send me back the page found at this URL."
- a single URL reveals exactly which page was sought, and thus exactly what content was received.

The data generated as a result of our customers using the Internet and telephone networks is certainly different in nature and volume than traditional fixed-line, analogue phone records.

This data can reveal even more about an individual than the content itself:

Examples

TWITTER

An article in the Wall Street Journal described 150 points of data available from one tweet[8], once it is deconstructed from its metadata. This was based on the work of then Twitter engineer Raffi Krikorian in 2010.

While only 140 characters are permitted in a Tweet; there are many individual pieces of metadata attached to it, including the content of the tweet.

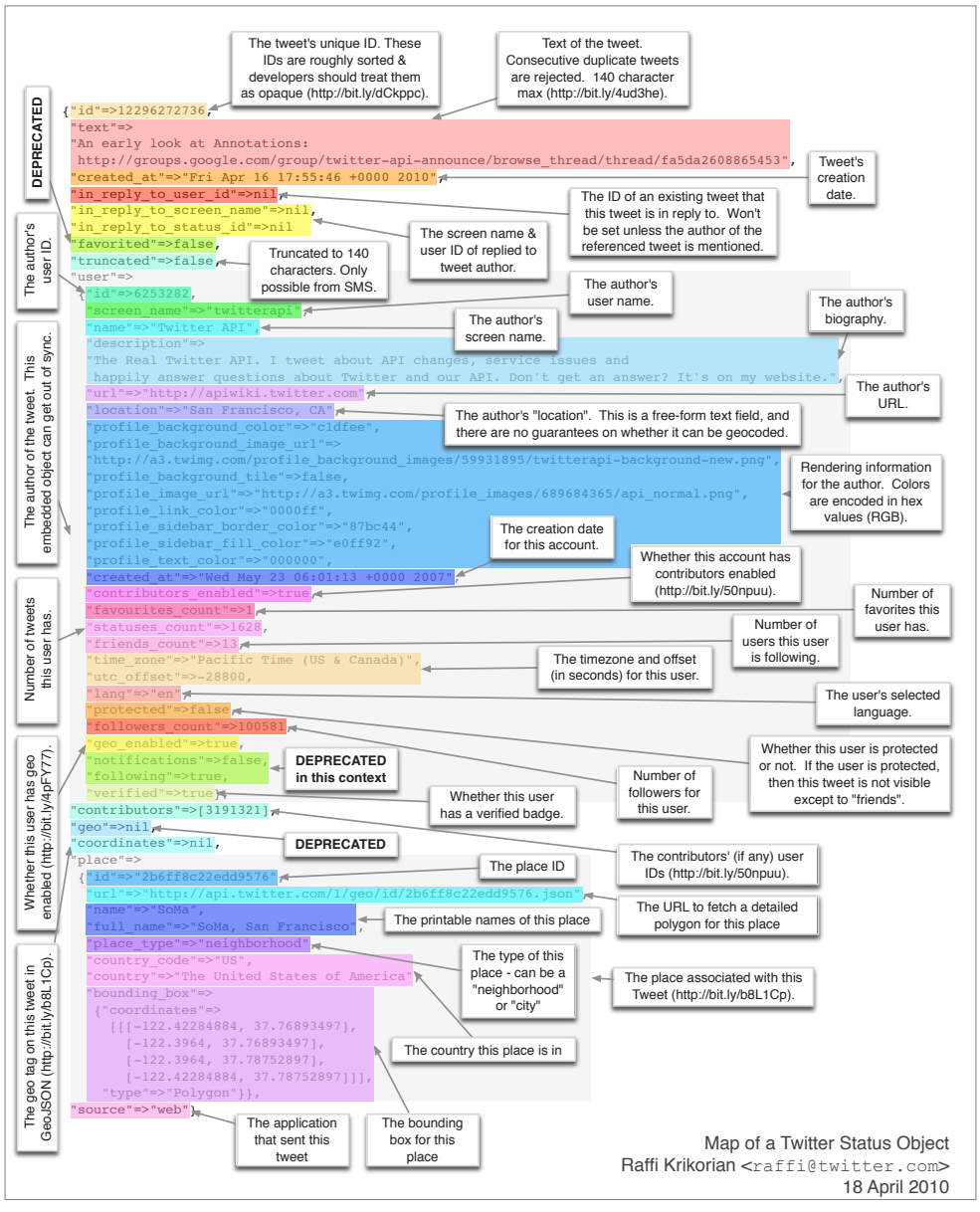

Figure 1 Raffi Krikorian's deconstructed Tweet.

In Figure 2 below we reprint a more recent illustration of Tweet metadata produced by Twitter user @USGuardian, of the Guardian News. This clearly shows the inclusion of the Tweet's content in the metadata.

If redacted Metadata (i.e. minus content) is required by new legislation, significant processing will be necessary for us to provide metadata without content.

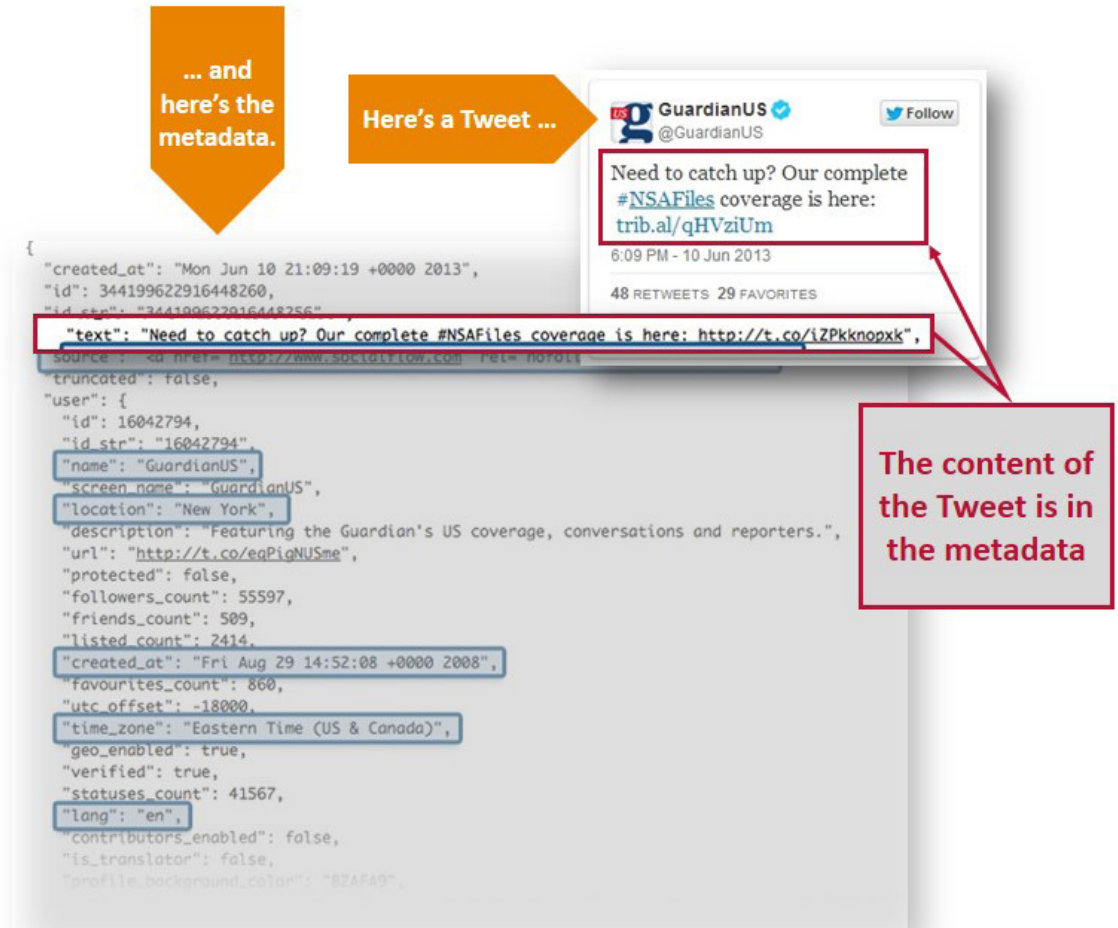

Figure 2 Tweet metadata with content

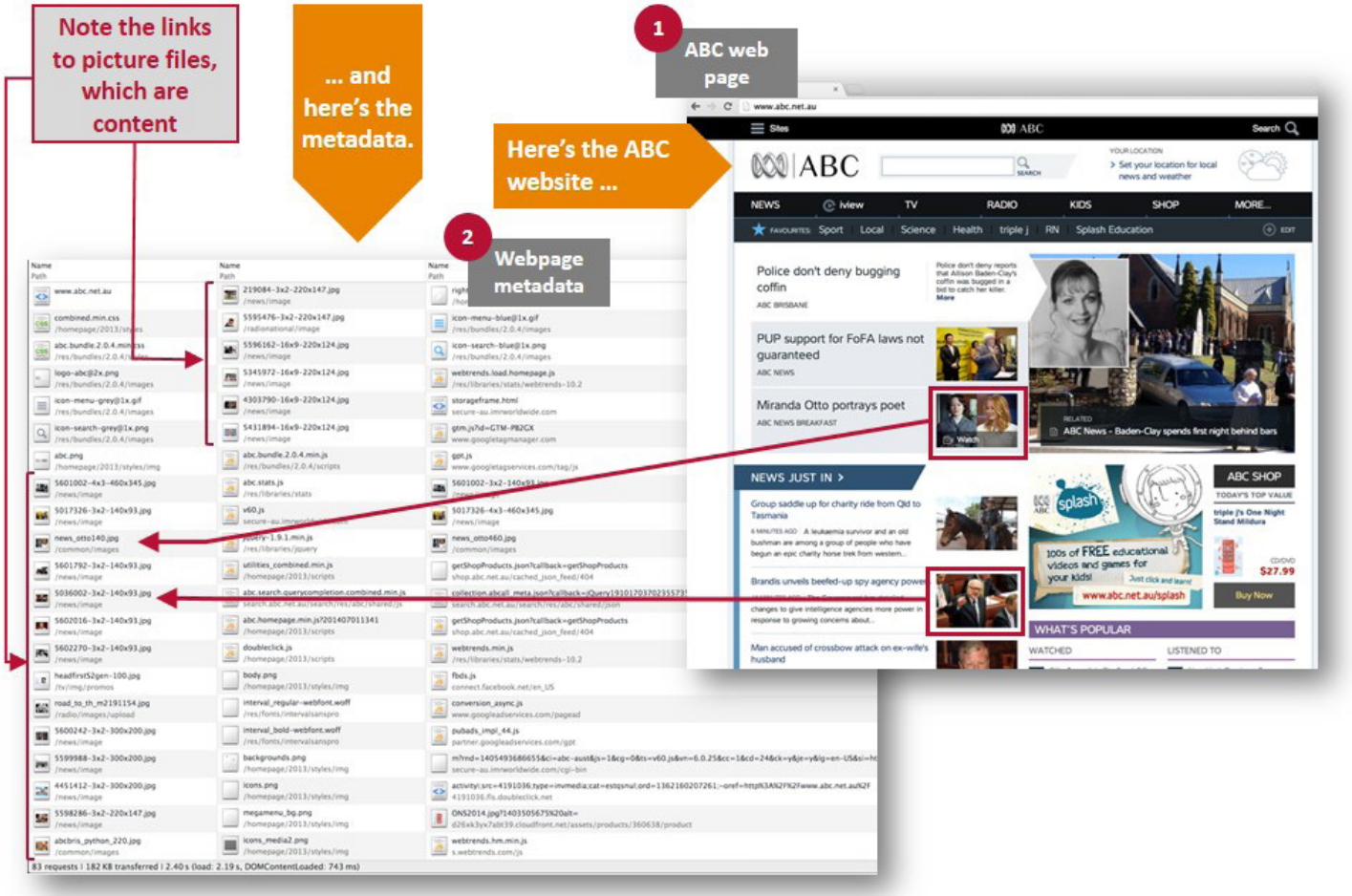

Figure 3 - ABC Homepage and metadata 16 June 2014

FACEBOOK

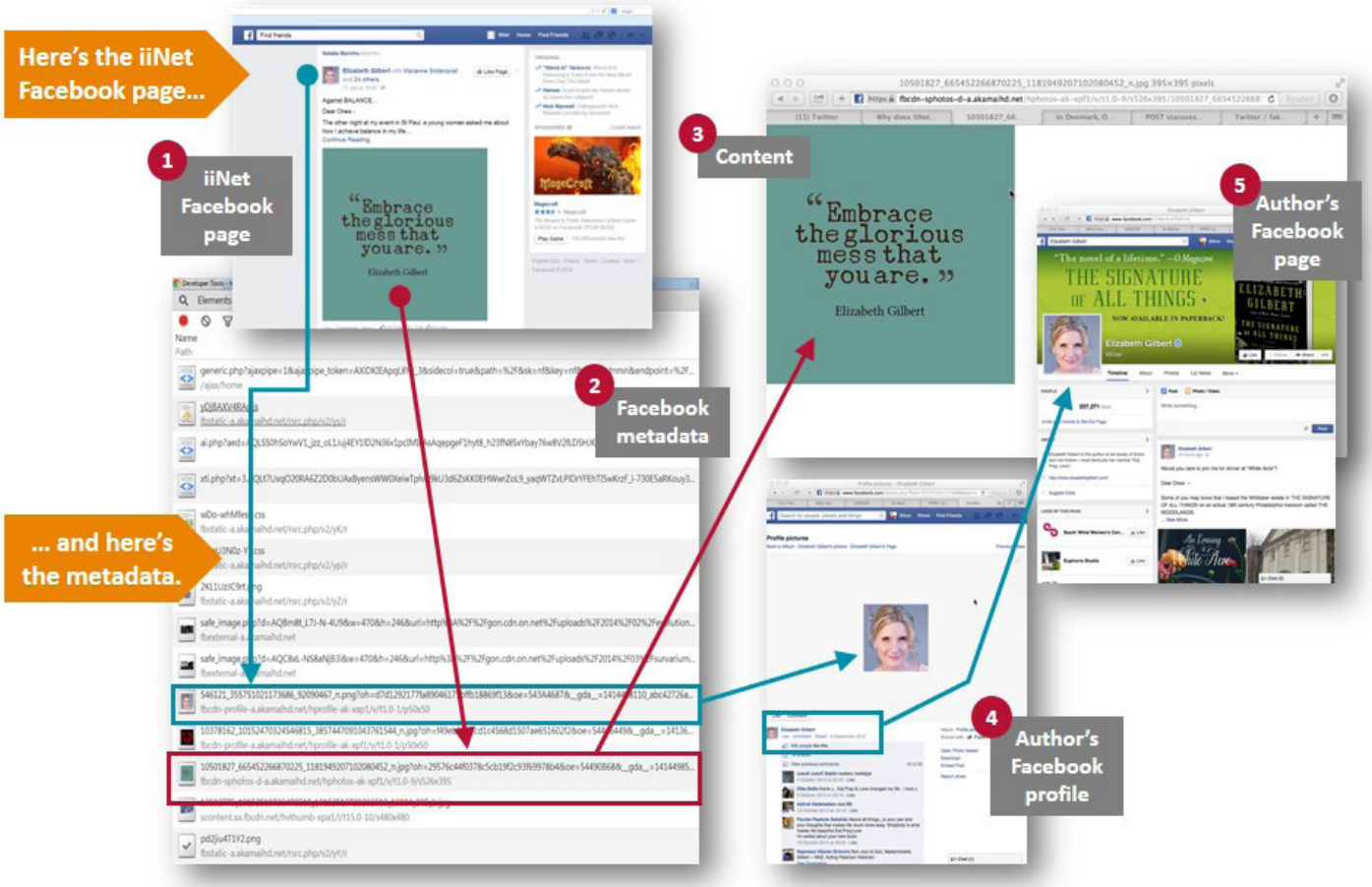

Figure 4 Facebook page and metadata

MOBILE TELEPHONE

Green party politician Malte Spitz had German telecommunications giant Deutsche Telekom hand over six months of his phone data that he then made **available to publisher, 'ZEIT ONLINE'**

Spitz's geo-location data was combined with information relating to his life as a politician, such as Twitter feeds, blog entries and websites, all of which is all freely available on the Internet.

Figure 5 Mash up using mobile metadata

WEARABLE DEVICES

Data from a range of “wearable” personal devices, home automation and monitoring systems will also generate metadata.

Wearable devices measure and record biometric data such as sleep patterns, pulse, temperature, activity levels, distance travelled, altitude, GPS coordinates as well as calls made or received and photographs taken, much of which will be incorporated into metadata as content or as links to the content[9].

Figure 6 ‘Wearable’ devices generate metadata

ROUTINELY COLLECTING DATA?

In its submission[10] to this Inquiry, the Attorney General's Department asserted:

> Service providers routinely engage in telecommunications data retention for their business purposes.

This assertion is overstated. Carriers only collect appropriate data for their businesses. There is a world of difference between the data collected in order to bill a customer for their Internet usage, versus the collection of a mass of data generated by a customer during their sessions on-line. The data generated by telecommunications traffic massively outweighs the data required for ISPs and carriers to run their businesses.

This suggestion from the Attorney General's Department could be likened to saying, "You are going to the shops to get a litre of milk anyway, and so it's no big deal to bring me the whole supermarket".

iiNet has no use for surveillance data, so there is no commercial driver to collect a massive volume of data, indexed to individuals, that we'll never use. In the event that a specific data preservation order is received from law enforcement agencies, special steps are required to retain the information specified in that notice.

We note that other reports emphasise the word 'telephone' in comments attributed to government sources. If the requests for metadata are to be restricted to telephony traffic, this limited approach conflicts with previous confidential documents provided to industry by the Attorney General's Department, which have clearly spelled out a much broader data set to be collected.

This broader data set has been described as consistent with that adopted in the European Data Retention Directive and is the data necessary to trace and identify the source and destination of communications (including unsuccessful or un-tariffed communications) on fixed network and mobile network telephony as well as Internet access, Internet email and Internet telephony.

It is further described as necessary for agencies to have access to the data to "reveal the daily habits of targets to enable targeted surveillance." We were also told that the additional data collection results from "... the use of new technologies, such as Voice over Internet Protocol (VoIP) and encryption, increases among agency targets."

The inconsistent and contradictory messaging from government sources is confusing and unhelpful.

The communications industry and broader community does not know whether the government is only looking for the data already collected 'routinely' by telephone companies, or is actually seeking the full set of data as set out in their briefing paper.

Is it the metadata such as that described by the European Directive or is it a smaller, sub-set of metadata, which has had the content, processed and redacted?

Additionally, the Privacy Act[11] prohibits the collection of data beyond that which is required for the service provider to conduct their business[12]. iiNet has worked hard to ensure that it is compliant with this obligation which I can broadly paraphrase as - "If you don't need it, don't keep it."

Browsing data, posts to RSVP, Twitter, Instagram, Facebook, Weibo or Google+, purchases from iTunes, Netflix, Amazon, eBay, Alibaba, searches via bing, Google, YouTube, Baidu or Yahoo, transactions for on-line banking, ticket purchases, hotels or PayPal are not routinely retained by iiNet for our business purposes. These are private and irrelevant to the provision of our service.

If we don't need the data at all, then it logically follows that we don't keep it in the first place, as it only creates unnecessary overhead. We don't build storage capacity for data we don't keep. The company has a formal data retention policy, which operates in line with my comments here.

Assumptions have been made about how our business operates; which leads to erroneous conclusions. Recent public assertions[13] have been made, for example, that "The ISP (as they do with their billing system) will be able to match the specific time and date stamp and IP address with a customer account." These sorts of assertions are misleading, as iiNet, and probably most Australian ISPs, do nothing of the sort. This demonstrates the danger of making comments in the absence of facts, and the consequential risk of creating a false impression. Suggesting that "It's no 'big deal' because carriers are already doing it", when carriers are not 'doing it' is misleading.

That careless approach is unacceptable for public policy development. Indeed, in a recent policy background paper[14], the Department of Communications highlighted that:

> The design of regulatory interventions requires an in-depth understanding of markets, supply chains and revenue flows, technical developments, expected regulatory costs and consumer and end-user expectations.

IMPLICATIONS FOR INDUSTRY

Mandatory data retention regimes turn commercial companies, like iiNet, into unwilling agents of the state. As the Office of the Victorian Privacy Commissioner submitted, the proposal for a two-year data retention scheme:

> "...is characteristic of a police state. It is premised on the assumption that all citizens should be monitored. Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life."[15]

Law enforcement agencies already have the power to undertake targeted requests for data, for example, by issuing an "ongoing data preservation notice".

iiNet does not agree that it should accept the role proposed by those calling for an onerous data retention regime. If we are ultimately compelled by law to collect such data, the government must be responsible for its storage and protection.

We won't volunteer to monitor and collect data on inoffensive Australian citizens but, if we are compelled to do so, the government must accept and store this data. The Office of the Victorian Privacy Commissioner also submitted[16] to a previous inquiry:

> Retaining the data would create a massive security risk if an ISP suffers a breach of security, including a significant risk of identity theft. The immense amount of data would also create an incentive for hackers to view ISPs as a target.

Law enforcement is the responsibility of governments. They carry the costs of such work, on behalf of the population. It is inappropriate to impose costs and obligations on unwilling commercial entities in order to create an intrusive police state.

A regime obsessed with surveillance of the general population, and the compilation of digital dossiers on every citizen, including children and the innocent, is incongruous in Australia. In the event that a police state is established, we accept we will have no option. In the meantime, we find it 'off brand' for iiNet and in conflict with our corporate values.

We believe that the community, and our industry, views these vague proposals with a great deal of uncertainty. Descriptions of metadata have ranged from 'just' routine data already collected for the purposes of telephone billing obligations, through to the full suite of the

data covered by the European Directive, covering all telephony platforms and Internet protocol communications. Despite the obvious facts, some have suggested that the metadata required will be bereft of content – implying, therefore, that what is required is actually processed metadata, with all content redacted.

The telecommunications industry may find itself coerced, into not only the onerous requirement to collect, store and protect massive quantities of unwanted data, but will also have imposed upon it the obligation to process petabytes of data per day to remove content or links to content.

A STANDARD SYSTEM

We believe that a standard system to facilitate targeted, necessary and proportionate[17] requests for data access and limited retention available to Australian law enforcement agencies.

We do not agree that a comprehensive collection of all metadata on every man, woman and child in Australia is either necessary or proportionate.

Chapter 4 of the TIA Act contains a general prohibition on the disclosure of telecommunications data. It also includes a regime of authorisations that permits certain enforcement agencies to access and disclose telecommunications data without needing to obtain a warrant.

The number of requests (which are increasing) made under this Part of the Act, that is over 330,000 disclosures in the 2012-2013 period are set out in the AGD's annual TIA Act Report[18]. That entities such as the RSPCA and local councils are permitted to fall within the scope of 'enforcement agencies', under this Part of the TIA Act, does not appear to meet the necessary and proportionate test.

iiNet agrees with arguments that requests for telecommunications data should require a warrant. In Canada, a recent Supreme Court decision[20] bars internet service providers from disclosing communications data such as the names, addresses and phone numbers of their customers to law enforcement officials voluntarily in response to a simple request — something ISPs have been doing hundreds of thousands of times a year.

At the very least, requests for access to telecommunications data (and section 313 notices under the Telecommunications Act) should be:

- provided to companies in a standard manner
- accompanied by sufficient information to confirm that it is appropriately authorised by a senior representative of the relevant agency
- subject to independent oversight
- restricted to a narrower range of law enforcement, anti-corruption and national security agencies that have a demonstrated investigative need for access to that range of information.

CONCLUSION

As I have attempted to demonstrate, it is disingenuous to claim that any proposed mandatory data retention regime concerns 'just' metadata when the detailed description of metadata, provided by the Attorney General's Department, is taken into account. Such an amorphous adjective attempts to provides some sort of solace and allay concerns, regarding Australian's right to privacy. Not only is the metadata sensitive and voluminous, it is, in many cases, content.

In order to redact the normally generated metadata down to a subset, which meets the stated requirement for 'metadata without content', a significant amount of processing will need to be carried out on the metadata, prior to its retention. This will create additional costs. Clearly this specialized data processing is not a role suited to access providers. It is inappropriate to require parties that don't need the data and don't want the data, to be held accountable for collecting, processing and storing the data.

To quote Paul Bernal,[21] commenting in the European debate,

> "Most importantly, [data retention] still works on the assumption that there is no problem with collecting data, and that the only place for controls or targeting is at the accessing stage.
>
> This is a fundamentally flawed assumption – morally, legally and practically.
>
> At the moral level, it treats us all as suspects.
>
> Legally it has been challenged and beaten many times – consistently in the European Court of Human Rights, in cases from as far back as Leander in 1987, and now in the ECJ in the declaration of invalidity of the Data Retention Directive.
>
> Practically, it means that data gathered is vulnerable in many ways – from the all too evident risks of function creep ... to vulnerability, to leaking, hacking, human error, human malice and so forth.
>
> Moreover, it is the gathering of data that creates the chilling effect – impacting upon our freedom of speech, of assembly and association and so forth. This isn't just about privacy. (My emphasis)"

Relevantly, the regime in the TIA Act that currently provides for permitted access to telecommunications data expressly does not permit the disclosure of:

(a) information that is the **contents or substance of a communication**; or

(b) a document to the extent that the document **contains the contents or substance of a communication**. (Section 172)

Perpetuating the perception that there is a meaningful distinction between metadata and content is misleading. Inventing a fake difference by saying that - we don't want to know where you live, we just want your address - may temporarily placate some, but these word games are unlikely to stand the test of time.

REFERENCES

[1] iiNet's submission to **the Inquiry into a Comprehensive revision of Telecommunidcations (Interception and Access) Act 1979**, April 2014, available online: **http://www.iinet.net.au/about/mediacentre/papers-and-presentations/010414-iinet-submission-comprehensive-revision-of-the-tia-act.pdf**

[2] We kill people based on metadata, David Cole, New York Review of Books, 10 May 2014, available online: **http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/**

[3] The Snowden leaks and the public, Alan Rusbridger, New York Review of Books, 21 November 2013, available online: **http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/**

[4] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Privacy and Civil Liberties Oversight Board, 23 January 2014, available online: **http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf**

[5] Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament, Caspar Bowden, 7 February 2014, available online: **http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf**

[6] According to the Advocate General, Mr Cruz Villalón, the Data Retention Directive is incompatible with the Charter of Fundamental Rights, Advocate General's Opinion in Joined Cases C-293/12 Digital Rights Ireland and C0594/12 Seitlinger and Others, 12 December 2013, available online: **http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf**

[7] Metadata piecing together a privacy solution, A report by ACLU of California, February 2014, available online: **https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202%2021%2014%20cover%20%2B%20inside%20for%20web%20%283%29.pdf**

[8] In a Single Tweet, as Many Pieces of Metadata as There Are Characters, WSJ, 6 June 2014, available online: **http://blogs.wsj.com/digits/2014/06/06/in-a-single-tweet-as-many-pieces-of-metadata-as-there-are-characters/?mod=e2tw**

[9] Top New Fitness and Wellness Gadgets for 2014, CIO, 6 February 2014,

http://www.cio.com/article/2368845/healthcare/139268-Top-New-Fitness-and-Wellness-Gadgets-for-2014.html

[10] Attorney-General Department's submission to **the Inquiry into a Comprehensive revision of Telecommunidcations (Interception and Access) Act 1979**, April 2014, page 30 available online: **http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Submissions**

[11] Australian Privacy Principles, OAIC. Available online: **http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles**

[12] See Australian Privacy Principle 11.2

[13] Village Roadshow defends 'three strikes' policy against piracy, says iiNet is "scaremongering", CNET, 25 June 2014, available online:

http://www.cnet.com/au/news/village-roadshow-defends-three-strikes-for-piracy/

[14] Policy Background Paper No. 2: Regulating Harms in the Australian Communications Sector, Department of Communications, May 2014, p 20

http://www.communications.gov.au/__data/assets/pdf_file/0008/231884/Dept-policy-background-paper_2_May-14.pdf

[15] Office of the Victorian Privacy Commissioner's submission to the PJCIS Inquiry into potential reforms of national security legislation, 20 August 2012, available online:

http://www.privacy.vic.gov.au/privacy/web2.nsf/files/inquiry-into-potential-reforms-of-the-national-security-legislation/$file/submission_08_12.pdf

[16] see 15.

[17] International Principles on the Application of Human Rights to Communications Surveillance, May 2014, available online:

https://en.necessaryandproportionate.org/text

[18] **Telecommunications (Interception and Access) Act 1979**
Annual Report 2012-13, Attorney-General's Department, available online:

http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Documents/TSLB-GAPSTIAActAnnualReport2012-13.pdf

[20] R. v. Spencer, 2014 SCC 43 Available online:

http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

[21] DRIP: a shabby process for a shady law, Paul Bernal, 12 July 2014. Available online:

http://paulbernal.wordpress.com/2014/07/12/drip-a-shabby-process-for-a-shady-law/