

8 October 2014

iiNet's response to Industry Consultation Paper – Telecommunications data retention - statement of requirements September 2014 (v 1.1)

As a company with over 950,000 customers, iiNet has been a strong advocate for the rights of consumers.

Over recent months, we've communicated with our customers on a range of high-profile topics, including mandatory data retention. We received a significant level of feedback from both our customers and other members of the public on this issue, with the majority supporting our opposition to mandatory data retention.

Blanket data retention is mass surveillance. It is not something that we currently do, and would add significant costs to the way we do business.

The basis of our objection to mandatory data retention includes:

- a lack of evidence suggesting changes to the current laws will prove more effective than existing laws, where we already cooperate with law enforcement agencies;
- a lack of justification as to why we should be monitoring our customers for two years on the chance this data may help an investigation;
- no explanation why the existing (and less than two-year-old) preservation notice regime is insufficient;
- ISPs are not 'agents of the state' but if we are compelled to take this role, the government should be responsible for the storage and security of this data; and
- an international trend away from blanket data retention by progressive governments, particularly in Europe.

In this response to the Attorney-General Department's Industry Consultation Paper, we first respond to the direct question concerning the practicability of retaining the set of telecommunications data that meets the requirements outlined in the paper.

We then elaborate on our continuing and significant concerns with the government's in-principle decision to impose a mandatory data retention regime on communications providers, announced on 5 August 2014.

TABLE OF CONTENTS

	Page No.
A. Practical concerns with the proposed data set.....	3
Uncertainty.....	3
“The proposed minimum standard includes no data that is not currently collected by some industry participants.”.....	3
Data formatting.....	5
Privacy.....	6
Retention period.....	7
Cost.....	8
Exemption regime.....	9
Access to communications data.....	10
B. The case for data retention has not been made.....	11
“Providers should be subject to data retention obligations for all services they provide to the public, whether directly or through contracts involving third parties.”.....	11
Not “just” like an envelope	12
Existing preservation notice regime.....	13
Overseas experience – is data retention the way the west is going?.....	14
UK - New Data Retention and Investigatory Powers Act.....	15
UN High Commissioner for Human Rights report on the right to privacy in the digital age ...	16
Contacts.....	17
References.....	18

A. Practical concerns with the proposed data set

iiNet is Australia's second largest DSL Internet Service Provider and the leading challenger in the telecommunications market. We maintain our own super-fast broadband network and support over 1.8 million broadband, telephony and Internet Protocol TV (IPTV) services nationwide.

iiNet welcomes this opportunity to provide comment on the Attorney-General Department's Industry Consultation Paper.

Uncertainty

"The proposed minimum standard includes no data that is not currently collected by some industry participants."

On 1 October 2014, the Attorney-General stated that the data retention laws will not "involve anything beyond what the telcos do at the moment."¹

However, the proposed data set out in this latest Consultation Paper includes categories of data that iiNet does not currently retain and has no business need to retain for the two-year retention period.

The Consultation Paper expressly states that data which falls within the defined data set will be required to be retained "even if this exceeds business needs" and that "the policy recognises that providers may need to modify some systems to ensure they meet the minimum standard".

Our systems are geared towards how our customers' services and settings are presently configured. In many instances we don't store how a customer used to have their service and settings configured as we provide the service in response to how our customer has requested it that particular day. For example, over time, a customer may change their DSLAM profile from "gamer" to "stable" or upgrade their customer premises equipment (CPE) from one brand to another. We have no business need to retain this historical information as it is not required to deliver the service today.

Nor is it helpful to refer to the proposed data set as "a **narrow** selection of telecommunications data" given its extensive scope. The data generated as a result of our customers using the Internet and mobile telephone networks is very different in nature and volume than traditional fixed-line, analogue phone records.

The proposed data set outlined in the Industry Consultation Paper includes:

- Subscriber name

- Additional authorised or registered users
- Address - residential, business, post office, billing & payment, service installation
- Account or service identifier - IP address, email address, phone number, international mobile subscriber identity, other network identifiers
- Any bundled services or additional accounts
- Date of birth
- Financial, charging, billing and payment information
- Account status or billing type – including whether account has been suspended for failure to pay and post/pre-paid status of the service
- Identification and verification data - may include passport number, Medicare number, other credit cards, rates statement
- Available bandwidth
- Upload/download volumes
- Records of successful, tariff communications - time, date, duration of communication
- Records of unsuccessful, untariffed communications - time, date where communications is incomplete (eg unanswered)
- Any identifier which uniquely describes the service at the time of the successful or attempted communication, including date & time marking.
- The source identifier for communications terminating on a provider's network or service (excluding URLs)
- The destination identifier for communications terminating on another provider's network or service (excluding URLs)
- Type of service - eg. ADSL, cable
- Type of application - eg. VOIP, instant messaging, email
- Additional features - call waiting, bandwidth allocation, upload/download allocations
- Physical and logical location of device - at start of call, at end of call

Category 2 of the proposed data set is described as follows:

Information necessary to trace and identify the source of a communication (including unsuccessful or untariffed communications).

In practical terms this category requires a material extension of our existing retention periods and in some instances even the creation of data such as:

- Email and webmail access logs – including identifiers associated with emails sent and received (3.5 million non-spam emails per day)
- CPE and device identifiers such as MAC address and type
- connection history and bandwidth traffic consumption

iiNet has no business need to retain IP logs after routing. We do not use them for billing purposes. This specific category of data would also require us to start retaining WiFi access logs.

The apparent requirement to capture the location when a communication or session starts and when a communication or session ends is of concern. iiNet should not be required to create and retain records about our customers' use of our services that would not otherwise be created for our business needs.

In the attempt to be technology neutral, many of the obligations in the data set are vaguely defined. All items in the proposed data set start with “information necessary to” and while there are explanatory statements to try to give clarity as to what must be retained, uncertainty remains. Category 1 also includes “supplementary information”. Providers should not have to make judgment calls as to what is supplementary information and more generally as to what data falls within the defined data set.

Other areas of uncertainty include the use of ambiguous terms such as “internet identifiers” and “network identifiers”. The Industry Consultation Paper states that the retention obligation is limited to the provider who has direct access to the data – but often no one provider has access to significant portions of the proposed dataset. So who collates and manages relationships between the then disparate data sets? Data models would have to be built which would provide a way to link and contextualise data, which itself would have to be managed at significant cost, and would add complexity, driving out timelines and decreasing the agility of the industry as a whole.

The identification of the communication end point is also another area of uncertainty as the end point is often not the device we see the connection from – any number of devices can be behind that device (the same is true of either mobile or DSL), and creating the connection.

The proposed data set includes a requirement to identify when a device is active or inactive – this status can change several times a day, and would require active monitoring. It is also limited to the connection point i.e. DSL or 3/4G modem. This specific retention obligation alone in itself would create significant amounts of data. It is not at all clear what is the value for law enforcement agencies of knowing whether a device is offline or not.

The Industry Consultation Paper states:

- they considered individual data sets (as adopted overseas)
- but they propose to make the primary legislation ‘technologically neutral’
- and to provide ‘guidance material over time’. (Note - not by regulations, or even ministerial determination.)

Detail provided by way of guidance material, which have no legal standing, is not good governance. In short, iiNet is very concerned that this Industry Consultation Paper is suggesting that the Parliament make vague and uncertain laws.

Data formatting

From the Consultation Paper:

Data retention does not require the centralising of data to a single point on each provider’s network, the formatting of data in accordance with any technical standard, or the development of request management systems to interface with agencies.

iiNet is concerned that law enforcement agencies will ask the government to require data is kept in an ‘agreed’ format, and there will be little opportunity for industry to ensure that this ‘agreed’ format does not present an excessive technical and financial burden.

The Consultation Paper states that providers won't be required to develop request management systems "to interface with agencies". Yet there is no recognition of the significant work and associated costs to ensure the retained data can be:

- efficiently queried by the communications provider upon request, and
- provided in a form to the requesting agency that can be understood.

iiNet has not been provided with any information concerning the capability of the relevant agencies to analyse the broad range of categories of data which are proposed to be retained.

Privacy

iiNet is committed to providing excellent service. Respecting and protecting our customers' personal information plays an important role in this commitment.

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) in concluding its discussion on the topic of data retention noted²:

A mandatory data retention regime raises fundamental privacy issues, and is arguably a significant extension of the power of the state over the citizen. No such regime should be enacted unless those privacy and civil liberties concerns are sufficiently addressed.

The Industry Consultation Paper and the government's public comments on data retention have not sufficiently addressed the very real privacy concerns with such a regime.

Category 1 of the proposed data set requires the retention of information necessary not just to identify the subscriber, but also refers to a range of 'supplementary information'. This 'supplementary information' extends to personal information such as billing and payment history, and current and historical contact information. The examples set out under this category also include: "any metrics that describe the use of the account, service or device, such as the available bandwidth, upload volumes and/or download volumes". What relevance this subset of the category of data might have for law enforcement has also not been made clear.

The Office of the Australian Information Commissioner (OAIC) has spent considerable time and resources since November 2012 educating businesses and the broader community about the new Australian Privacy Principles³ (APPs). For example, iiNet participated as a partner with OAIC in this year's Privacy Awareness Week⁴.

Relevant to the issue of data retention, APP 3.2 provides:

If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities .

APP 11.2 also established requirements for APP entities to destroy or de-identify personal information where it is no longer needed.

So on the one hand, we have one government agency highlighting the need for businesses like iiNet to respect and protect our customer's personal information and on the other, government and law enforcement agencies calling for mandatory data retention of all our customers.

Last month, the Privacy Commissioner also highlighted his concerns relating to mandatory data retention⁵:

there is the potential for the retention of large amounts of data to contain or reveal a great deal of information about people's private lives, and that this data could be considered 'personal information' under the Privacy Act.

The retention of large amounts of personal information for an extended period of time increases the risk of a data breach. Organisations holding this information need to comply with all their obligations under the Privacy Act, including the requirements to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure.

Key to this debate will be ensuring the ongoing privacy interests of Australians. It will also be important to consider whether a data retention scheme is effective, proportional, the least privacy invasive option and consistent with community expectations. Any scheme should also be transparent, accountable and have appropriate independent oversight.

iiNet shares these concerns. In particular, the retention of a vast set of personal information would likely prove to be an appealing target for hackers all around the world – creating a risk of identity theft in the event of a data breach⁶.

Retention period

The PJCIS report on potential reforms to national security noted that the Committee was asked to consider:

Applying **tailored** data retention periods for **up to 2years for parts** of a data set, with specific timeframes taking into account agency priorities and privacy and cost impacts.⁷ (our emphasis)

The Consultation Paper departs from this tailored approach. The Consultation Paper only refers to a blanket two-year retention period that applies across **all** the categories of data to be retained.

There is no discussion of the possibility of tailored retention periods or why the maximum two-year period and not the minimum six-month period set out in the EU Data Retention Directive was chosen.

There has been no attempt to provide coherent evidence as to why this particular retention period of two years should apply uniformly across all the categories of data set out in the proposal.

This failure to tailor retention periods to what is "strictly necessary" was one flaw highlighted by the CJEU in its decision⁸ striking down the EU Data Retention Directive:

Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned" (para 64)

"it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary" (para 65).

A standard two-year retention period is not necessary or proportionate. It would force significant extra expense on communications providers who have no business need to retain the complete proposed data set for that significant period of time.

In 2010, the European Data Protection Supervisor called the EU Data Retention Directive: *“without doubt the most privacy-invasive instrument ever adopted by the EU in terms of scale and the number of people it affects.”*⁹

The legitimacy of the EU’s Data Retention Directive has in fact been questioned since legislation was first proposed in 2002.¹⁰

In April 2014, in a landmark judgment the EU Data Retention Directive¹¹ was declared invalid by the Court of Justice of the European Union (CJEU)¹². It was especially problematic that the Directive effectively introduced blanket surveillance and treated everyone’s data the same:

“the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.”¹³

In practice, the CJEU ruling means that any legislation requiring retention of communications data by a Member State of the EU should now comply within the framework set out in the judgment¹⁴. This framework includes the following principles:

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and /or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);
- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);
- ensure retention periods are limited to that which is ‘strictly necessary’ (paragraph 64);
- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61).¹⁵

These principles are very much relevant to the current discussion in Australia. It is therefore very disappointing that none of these principles appear to have been acknowledged, let alone adhered to in either the proposed data set or the explanatory statements set out in this latest Industry Consultation Paper.

Cost

It is very hard to measure exactly what a mandatory data retention scheme will cost, even with the information provided in this paper about the proposed data set.

The government does not propose to mandate particular security standards, according to this latest Consultation Paper. However, retaining the proposed data set for two years involves significant security risk, and significant costs associated cost to manage this risk.

Current security and integrity controls on data retained for legal reasons such as financial data, has evolved over many years and these applications are significantly different to applications which retain general logging information. Put simply, financial applications are designed significantly differently to a logging platform or other database driven applications. If iiNet was compelled to introduce the same level of functionality to preserve the integrity of the full retained data set it would incur significant cost including audit costs.

No guidance has been provided on other practical issues such as whether communications providers will be free to seek the lowest cost solutions. For example, will offshore cloud storage be acceptable

or will the data be required to be stored in Australia? As set out in **Appendix A**, there are many other unanswered questions about how any scheme will work in practice.

The categories of costs include:

- upfront capex costs
- ongoing maintenance and investment such as hardware replacement (each 18-24 months) for storage of retained data
- costs of capturing the data (and in some cases creating data that hadn't been previously created);
- storing data with appropriate security and evidentiary integrity;
- retaining the data in such a way that it is readable/understandable by the agencies;
- secure destruction of data after the retention period has lapsed;
- handling requests for access from law enforcement agencies;
- dealing with our customers' concerns and queries about the retention of their personal information.

There has been no suggestion by the government that it would reimburse or even contribute to the substantial costs incurred by providers in complying with a mandatory data retention regime. In these circumstances, consumers will ultimately bear these costs.

This position on costs is a departure from the recommendation in the PJCIS report in which it was stated that if the government was persuaded to introduce a mandatory data retention regime *"the costs incurred by providers should be reimbursed by the Government"*.

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

iiNet is also concerned that the significant costs of a data retention regime could also result in a less internationally competitive communications sector.

Exemption regime

The Industry Consultation Paper suggests that the data retention obligations may include appropriate exemptions for services that are of limited or no relevance to law enforcement or national security, such as IPTV services.

The exemption regime of the nature outlined in this paper does not provide the necessary transparency or certainty for industry or consumers. It could, for example, result in a situation where a well-resourced provider could get an exemption for IPTV services and another industry member may not.

If the government does proceed with a data retention scheme, it should follow the framework outlined in the CJEU's judgment, which includes adhering to the following:

- only retaining data that would contribute to the prevention, detection or prosecution of serious offences
- distinguishing between the usefulness of different categories of data and tailor retention periods to the objective pursued;
- addressing the consequences of the scheme for lawyers and journalists who expect confidentiality for much of their communications.

Access to communications data

The Consultation Paper does not propose any changes to the increasingly contentious regime for accessing communications data.

iiNet agrees with the PJCS's recommendation that the Attorney-General's Department should review the threshold for access to communications data. Such a review should reduce the number of agencies able to access communications data, for example, by using gravity of conduct which may be investigated as the threshold on which access is allowed.

Analysis of the publicly available figures has revealed that:

No less than 40 government agencies made 293,501 warrantless requests for metadata from internet service providers in the 2011-12 financial year. Just 56,898 of those requests were made by the Federal Police, which has the primary criminal law-enforcement role. The RSPCA, Wyndham City Council, the Tax Practitioners Board and even the Victorian Taxi Directorate also have been allowed to access individual telecommunications data for a 'law-enforcement purpose'.¹⁶The CJEU also provided guidance on this question of access to data collected under mass surveillance regimes in its landmark judgment striking down the Data Retention Directive. In its decision the Court accepted that data retention constitutes a *prima facie* interference with fundamental rights, not least because so-called 'metadata' "may allow very precise conclusions to be drawn concerning ... private lives"¹⁷. If access to this sensitive data is granted, the Court said such access must be subject to prior review "carried out by a court or by an independent administrative body."

Ideally requests to ISPs such as iiNet for access to communications data would be accompanied by a warrant.

B. The case for data retention has not been made

“Providers should be subject to data retention obligations for all services they provide to the public, whether directly or through contracts involving third parties.”

iiNet continues to be very uncomfortable with the notion that commercial businesses may be forced into a role as unwilling agents of the state to collect, store and safeguard very large databases for which the companies themselves have no use – a role very different from that which those companies were originally established.

As the Office of the Victorian Privacy Commissioner submitted to the PJCS 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.¹⁸”

There has been no compelling evidence put forward that demonstrates that these new laws will be any more effective than the existing laws.

UK representatives before the CJEU in July 2013 conceded there was no “*scientific data*” to underpin the claimed need for data retention¹⁹. As the authors of a study on the EU Data Retention Directive highlight in respect to the “*evidence*” which had been presented to justify the Directive, it is sufficient to note that the plural of anecdote is not “*data*”²⁰. Last year the Privacy and Civil Liberties Oversight Board found²¹ that there is little evidence that the metadata program has made the US safer.

Dr Bendall, the former Victorian Privacy Commissioner, for example has expressed scepticism as to whether data retention would aid law enforcement and national security agencies due to the incentive this would provide to anonymise communications.²²

The proposed data set and lengthy retention period is also not necessary or proportionate²³. What is being proposed is not a targeted approach but wholesale collection and storage of data of all our customers. To quote Paul Bernal, commenting in the European context,

“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.²⁴”

Not “just” like an envelope ...

To date, informed discussion concerning data retention has been hampered by the use of faulty analogies to explain complex issues and the frequent use of the words “just” or “only”.

Here are just a few examples that explain why analogies or claims of “just” or “only” metadata are misleading in this context:

- In May this year, David Cole²⁵, a Professor in Law and Public Policy at Georgetown University Law Center highlighted that 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 asserted: “We kill people based on metadata.”²⁶

Caspar Bowden, a specialist in EU Data Protection and European and US surveillance law has argued²⁷ that:

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 2013 opinion²⁸ supporting the overturning of the EU Data Retention 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.”
- 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”.
- 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.

Ryan Gallagher in August this year reported²⁹ on the role of metadata in the CIA’s “extraordinary rendition” program, which involved kidnapping terror suspects and taking them to secret “black site” jails. Gallagher noted that in June 2013, President Obama tried to dismiss concerns about metadata collection in the United States by claiming that “nobody is listening to your telephone calls.” However, as Gallagher noted:

... clearly, the government doesn't need to be listening to your calls to deem you a threat. That metadata has been the deciding factor in targeting people for extraordinary rendition is a profound illustration of that — and it shows that metadata collection has real-world ramifications: it is not just some benign activity.

During the height of the extraordinary rendition program, for instance, some of the people targeted were victims of what was called “erroneous rendition.” In other words, the CIA would kidnap the wrong person.

The significant implications for all Australians of a mandatory data retention scheme should not be downplayed by resorting to misleading analogies or rhetoric of “just” or “only” metadata that has dominated much of the public discussion.

Existing preservation notice regime

Largely absent from the discussions on data retention to date is that changes made to the *Telecommunications (Interception and Access) Act* in 2012³⁰ have already given new and significant powers to law enforcement and national security agencies. These amendments provide certain law enforcement agencies the power to undertake targeted requests for data, for example, by issuing an “ongoing data preservation notice”. As explained in the Act:

This Part establishes a system of preserving certain [stored communications](#) that are held by a [carrier](#). The purpose of the preservation is to prevent the [communications](#) from being destroyed before they can be [accessed](#) under certain [warrants](#) issued under this Act³¹.

‘Enforcement agencies’ and ‘interception agencies’, including the AFP and state police, are authorised to issue data preservation notices if they consider:

- there are reasonable grounds for suspecting there are or may be stored communications that might assist in connection with the investigation of a ‘serious contravention’, and
- the stored communications relate to the person covered by the notice.

Law enforcement agencies will only be able to access the information retained pursuant to a preservation notice under a warrant.

Targeted preservation notices used together with stored communications warrants provide an alternative framework to mass data retention. iiNet believes this is an approach which better takes into consideration privacy and civil liberties concerns while being more likely to ensure that any retention and access to our customer’s personal information is necessary and legitimate.

De facto widening of section 313 obligations

Section 313 of the *Telecommunications Act 1997* places obligations on carriers and carriage service providers to “do (their) best to prevent telecommunications networks and facilities from being used in ... the commission of offences” and to give Commonwealth, State and Territory authorities “such help as is reasonably necessary” for purposes including enforcing the criminal law.

The extent of the obligations of carriers and services providers under section 313 is already vague and uncertain. Under the proposed data retention laws these obligations would remain vague and uncertain, though would likely be widened, given that carriers and service providers would hold additional information so arguably become more able to “do their best” or provide “help”.

It is unsatisfactory that the proposed data retention obligations do not in parallel clarify and appropriately define and limit the obligations of carriers and service providers under section 313.

Overseas experience – is data retention the way the west is going?

In July this year, the Attorney-General asserted that mandatory data retention is “*very much the way in which western nations are going.*”³²

This generalisation deserves some close scrutiny, as there are significant contra-indications.

Quite a number of western nations have taken a different view to data retention than that contemplated by the Australian government. For example –

Country	Status of Telecommunications Data Retention Regime
Austria	Ruled Unconstitutional
Bulgaria	Ruled Unconstitutional
Cyprus	Ruled Unconstitutional
Czech Republic	Ruled Unconstitutional
Germany	Ruled Unconstitutional. No mandatory data retention
Romania	Ruled Unconstitutional (twice)
Slovenia	Ruled Unconstitutional
Denmark	Session logging ceased following judgment of European Court of Justice
Slovakia	Ceased following judgment of European Court of Justice. Records deleted.
Sweden	Under Challenge, judgment pending
UK	Under Challenge
Ireland	Under Challenge
Switzerland ³³	Under Challenge
Norway	No mandatory data retention regime

Digital Rights **Ireland** who were one of the parties to the CJEU challenge to the EU Data Retention Directive have highlighted that:

“It is unprecedented in Europe for a law to be struck down so widely. Data retention has been rejected unanimously by every supreme court or constitutional court to consider it – [at last count](#) being held unconstitutional in **Austria, Bulgaria, Cyprus, the Czech Republic, Germany, Romania, and Slovenia** as well as by the European Court of Justice”.³⁴

Germany has been without data retention measures since 2010, following a decision of the German Constitutional Court. The Court emphasized that the collected data could be used to establish “*meaningful personality profiles of virtually all citizens and track their movements*”.³⁵ The following year, a German parliament study concluded data retention in Germany had led to an increase in the crime clearance rate of 0.006%.³⁶³⁷

In **Norway**, data retention legislation is yet to be adopted, despite it being a member of the European Economic Area³⁸.

Under **Denmark’s** data retention regime, which commenced in 2007, communications providers were required to retain and store all their customers’ telephone and internet data for a period of one year. The telco industry bears the cost of this storage and retention of their subscribers’ data³⁹.

The Danish law contains a requirement for session logging. The following information must be retained: source and destination IP address, source and destination port number, transmission protocol (like TCP and UDP) and timestamps⁴⁰. In 2013, a report⁴¹ produced by the Danish Ministry of Justice, highlighted that five years of extensive Internet surveillance have proven to be of almost no use to the police⁴². The report mentions only two cases in which session logging proved useful to the police — and both were cases of financial crimes. Torben Olander reported: “... *the police and security services are drowning in a tsunami of user data that they cannot sort and therefore cannot use.*”⁴³

Following the CJEU ruling in April this year (discussed above):

- four **Swedish** communications providers deleted their retained data. Since May 2012, they had been required to store subscriber and location data for mobile, internet services, email, and internet telephony for six months. The Swedish telecommunications regulator decided it wouldn't take action against them, despite the continued existence of the Swedish data retention law.⁴⁴
- The **Danish** parliament asked the government to consider the implications of this decision for Denmark’s own data retention regime. In June 2014, it was reported that the special session logging requirements in the Danish law will, be lifted immediately⁴⁵. The publicly stated reason for this was not the CJEU ruling, but the technical difficulties of using this retained data in police investigations (as outlined above).⁴⁶
- The Constitutional Court in **Slovakia** suspended the relevant provisions of the Slovak data retention law and included an order to delete already retained data immediately.⁴⁷ Both the Slovenian and **Romanian** Constitutional Courts also ruled blanket data retention to be unconstitutional in July this year.⁴⁸

UK - New Data Retention and Investigatory Powers Act

Australian politicians and representatives from law enforcement agencies have repeatedly pointed to the data retention law (known as DRIP)⁴⁹ recently passed in the UK.

The UK was the first EU government to change its law on data retention following the Court of Justice of the European Union's judgment in April (which found that blanket data retention severely interferes with the fundamental rights to respect for private life and to the protection of personal data).

What the Australian politicians and law enforcement officials invariably fail to mention is that in passing this “emergency” legislation the UK is “consciously acting in defiance of the CJEU ruling⁵⁰”. Nor have they been open in acknowledging that this new data retention legislation in the UK is being challenged both in the national courts and at the European Commission level⁵¹. Two British MPs are launching a legal challenge to the new legislation. They argue that DRIP is incompatible with Article 8 of the European Convention on Human Rights (which covers respect for private and family life) as well as Articles 7 and 8 of the EU Charter of Fundamental Rights (respect for private and family life and the protection of personal data)⁵².

UN High Commissioner for Human Rights report on the right to privacy in the digital age

In July 2014, the UN High Commissioner for Human Rights released her report on the right to privacy in the digital age⁵³. Relevantly, the report stated⁵⁴:

Mandatory third-party data retention is neither necessary or proportionate

- It has been suggested that the interception or collection of data about a communication, as opposed to the content of the communication, does not on its own constitute an interference with privacy. From the perspective of the right to privacy, this distinction is not persuasive. The aggregation of information commonly referred to as “metadata” may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. (para 19)
- It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. (para 20)
- Governments frequently justify digital communications surveillance programmes on the grounds of national security, including the risks posed by terrorism. Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a “legitimate aim” for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose. (para 25)
- Concerns about whether access to and use of data are tailored to specific legitimate aims also raise questions about the increasing reliance of governments on private sector actors to retain data ‘just in case’ it is needed for government purposes. Mandatory third-party data retention – a recurring feature of surveillance regimes in many states, where governments require telephone companies and Internet service providers to store metadata about their customers’ communications and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate. (para 26)

iiNet urges the government and policy makers to take into consideration this overseas experience, together with the range of other matters set out in this response, when considering this proposal to introduce mandatory data retention.

It is also critically important that there is appropriate time provided for meaningful and informed public consultation and scrutiny of these proposals. We trust that this contribution contributes to a robust public discussion.

Contacts

Stephen Dalby
Chief Regulatory Officer
iiNet Limited
e: sdalby@staff.iinet.net.au
ph: 08 9213 1371

Leanne O'Donnell
Regulatory Manager
iiNet Limited
e: lodonnell@staff.iinet.net.au
ph: 03 9811 0042

References

-
- ¹ Response to a question after the Attorney-General's National Press Club Address on 1 October 2014.
- ² Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, 24 June 2013, p 190, available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm
- ³ Australian Privacy Principles, OAIC, available at: <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles>
- ⁴ Privacy Awareness Week 2014, iiNet Blog, 6 May 2014, available at: <http://blog.iinet.net.au/privacy-awareness-week-2014/>
- ⁵ Australian Government's data retention proposal — statement, Australian Privacy Commissioner, OAIC, 8 August 2014, available at: <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/australian-governments-data-retention-proposal/australian-government-s-data-retention-proposal>
-
- ⁶ Office of the Victorian Privacy Commissioner's submission to the PJCS 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](http://www.privacy.vic.gov.au/privacy/web2.nsf/files/inquiry-into-potential-reforms-of-the-national-security-legislation/$file/submission_08_12.pdf)
- ⁷ Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, 24 June 2013, p 139, available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm
- ⁸ Judgment of the ECJ in Digital Rights Ireland data retention challenge, 8 April 2014, available at: <http://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge>
- ⁹ Speech given at the conference 'Taking on the Data Retention Directive', 3 December 2010, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf
- ¹⁰ See the history of the various challenges to the EU Data Retention Directive and its implementation by EU Member States in The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy Available at: <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf>
- ¹¹ Text of the EU Data Retention Directive is available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>
- ¹² Judith Rauhofer & Daithi Mac Singh, 'The Data Retention Directive Never Existed', 16 April 2014, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467244
- ¹³ Decision of the Court of Justice of the European Union in Joined Cases C-293/12 (Digital Rights Ireland) and C-594/12 (Kärntner Landesregierung), 8 April 2014, : <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN>
- ¹⁴ See CJEU Judgment
- ¹⁵ The Court of Justice declares the Data Retention Directive to be invalid, Press Release of the Court of Justice of the European Union, 8 April 2014, available at: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>
- ¹⁶ Ross Coulthart, Australia's Real Surveillance Scandal, The Global Mail, 13 December 2013, available at: <http://www.theglobalmail.org/feature/australias-real-surveillance-scandal/777/>

¹⁷ Fiona De Londras, CJEU strikes down data retention directive, Human Rights in Ireland, 8 April 2014, available at: <http://humanrights.ie/civil-liberties/cjeu-strikes-down-data-retention-directive/>

¹⁸ Submission 109 to Inquiry into Potential Reforms of Australia's National Security Legislation, available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjicis/nsl2012/su bs.htm

¹⁹ EU data retention might not be proportional to risks, 9 July 2013, available at: <http://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170>

²¹ 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 at: <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf>

²² Report of the Inquiry into Potential Reforms of Australia's National Security Legislation, 24 June 2013, p 179, available at: http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjicis/nsl2012/re port.htm

²³ International Principles on the Application of Human Rights to Communications Surveillance, May 2014, available at: <https://en.necessaryandproportionate.org/text>

²⁴ DRIP: a shabby process for a shady law, Paul Bernal, 12 July 2014. Available at: <http://paulbernal.wordpress.com/2014/07/12/drip-a-shabby-process-for-a-shady-law/>

²⁵ We kill people based on metadata, David Cole, New York Review of Books, 10 May 2014, available at: <http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/>

²⁶ 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/>

²⁷ Privacy and Security Inquiry: Submission to the Intelligence And Security Committee of Parliament, Caspar Bowden, 7 February 2014, available at: http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf

²⁸ 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 at: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf>

²⁹ Ryan J Gallagher, Extraordinary rendition and the secret role of metadata, Notes R J Gallagher, 28 August 2014, available at: <http://notes.rjgallagher.co.uk/2014/08/extraordinary-rendition-metadata-cia-erroneous.html>

³⁰ See Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* and commentary from law firms such as: <http://www.allens.com.au/pubs/tmt/fotmt27nov12.htm> & <http://www.minterellison.com/publications/new-data-preservation-laws-address-cybercrime-concerns-pu201209/>

³¹ See section 107G, available at: http://www.austlii.edu.au/au/legis/cth/consol_act/taaa1979410/s107g.html

³² Josh Taylor, "Data retention is 'the way western nations are going': Brandis", ZDNet, 16 July 2014, available at: <http://www.zdnet.com/au/data-retention-is-the-way-western-nations-are-going-brandis-7000031658/>

³³ Successful first step in challenging Swiss Data Retention, 2 July 2014, available at: <http://sustainability.oriented.systems/challenging-swiss-data-retention/>

³⁴ “Data retention held unconstitutional in Slovenia”, 12 July 2014, available at <http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/>

³⁵ Study by Professors Boehm & Cole "Data Retention after the Judgement of the CJEU", released in July 2014, available at: http://www.ianalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf

³⁶ “Impossible to Ensure Legality of EU Communications Data Retention Directive Says German Parliament”, 26 April 2011, available at: <http://www.vorratsdatenspeicherung.de/content/view/446/79/lang,en/>

³⁷ “Crikey Clarifier: data retention — what it is and why it’s bad”, 21 April 2014, available at: http://www.crikey.com.au/2014/07/21/crikey-clarifier-data-retention-what-it-is-and-why-its-bad/?wpmc_tp=1

³⁸ The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy Available at: <http://secile.eu/wp-content/uploads/2013/11/Data-Retention-Directive-in-Europe-A-Case-Study.pdf>

³⁹ “In Denmark, Online Tracking of Citizens is an Unwieldy Failure”, 22 May 2013, available at: <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy>

⁴⁰ “Denmark: Government postpones data retention evaluation”, 13 February 2013, available at: <http://edri.org/edriamnumber11-3dk-postpones-data-retention-evaluation/>

⁴¹ Report is available at: <http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf>

⁴² “Draconian data retention doesn’t work Danish police say”, 30 May 2013, available at: <http://freedomwatch.ipa.org.au/draconian-data-retention-doesnt-work-danish-police-say/>

⁴³ “In Denmark, Online Tracking of Citizens is an Unwieldy Failure”, 22 May 2013, available at: <http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy>

⁴⁴ “Four of Sweden's telcos stop storing customer data after EU retention directive overthrown”, 11 April 2014, available at: <http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/>

⁴⁵ Google Translate version of press release from Danish Ministry of Justice repealing rules on session logging, 2 June 2014: <http://bit.ly/Ve43u2>

⁴⁶ “Denmark: Data retention is here to stay despite the CJEU ruling”, 4 June 2014, available at: <http://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/>

⁴⁷ See Boehm & Cole study.

⁴⁸ Press release from the Slovenian Information Commissioner, 11 July 2014, available at: [https://www.ip-rs.si/index.php?id=272&tx_ttnews\[tt_news\]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461](https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461)

⁴⁹ *Data Retention and Investigatory Powers Act 2014* available at: <http://www.legislation.gov.uk/ukpga/2014/27/contents/enacted/data.htm>

⁵⁰ Mass surveillance of communications in the EU: CJEU judgment and DRIPA 2014/RIPA 2000 in the UK, Statewatch, August 2014, available at: <http://www.statewatch.org/analyses/no-252-mand-ret-dripa-ripa.pdf>

⁵¹ DRIP: the Commission acknowledges Access’ complaint, 6 August 2014, available at: <https://www.accessnow.org/blog/2014/08/06/drip-the-commission-acknowledges-access-complaint>

⁵² “MPs to seek judicial review of emergency data law”, 22 July 2014, available at: <http://www.bbc.co.uk/news/uk-politics-28417886>

⁵³ UNHRC: Joint statement on privacy in the digital age, 12 September 2014, IFEX, available at: https://www.ifex.org/international/2014/09/12/privacy_digital_age/

⁵⁴ Right to Privacy in the digital age, Office of the United Nations Human Rights Commissioner, 30 June 2014, available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Appendix A

Unanswered operational questions

The consultation paper focuses on providing information to industry on the proposed data set.

No certainty has been provided on how the regime might operate in practice. A meaningful exercise on estimating the costs that might flow from such a regime cannot be undertaken by industry participants without this information.

The questions⁵⁴ that remain unanswered include:

- How is the new system, if created, to be reconciled with Privacy Act requirements? For example, will there be a carve-out so that customers cannot ask for access to their 2 years of the retained communications data?
- What controls/limitations will there be over which agencies can request access to the retained data?
- What is the mechanism for ensuring that retained data can be used only for national security purposes and/or enforcement of serious criminal laws?
- How will any data retention regime interact with the existing preservation notice regime in the TIA Act?
- What requirements will be put in place in relation to disposal of data by both industry and agencies?

-
- What oversight mechanisms will be in place for any data retention regime? For example, will ISPs and/or agencies be required to report to AGD in relation to requests for data retained under the data retention regime?
 - Will there be review periods built into the regime? For example, what controls will there be over the way requested data sets might be asked to be amended as new technology emerges and other technology becomes less important?