iiNet Limited
ACN 068 628 937

iiNet Limited
502 Hay Street
Subiaco, WA 6008

Support: 13 22 58
Sales: 13 19 17
Fax: 1300 785 632
Web: iinet.net.au

The way in which western nations are going?

Australia's Attorney-General Brandis confirmed in a press conference on 5 August 2014 that an *"in-principle"* decision has been made that data retention laws would be introduced to parliament sometime later this year.

Last month, the Attorney-General in stating that the question of data retention *"is under active consideration by the government, asserted: this is very much the way in which western nations are going."*[i]

This generalisation deserves some close scrutiny, as there are important contra-indications. Several western nations have taken a different view to data retention, for example -

Country	Status of Data Retention Regime
Austria	Ruled Unconstitutional
Bulgaria	Ruled Unconstitutional
Cyprus	Ruled Unconstitutional
Czech Republic	Ruled Unconstitutional
Germany	Ruled Unconstitutional
Romania	Ruled Unconstitutional
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	Ceased following judgment of European Court of Justice. Records deleted.
UK	Under Challenge

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"*.[ii] 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%.[iiiiv]

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

Under Denmark's data retention regime, which commenced in 2007, telcos are 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' data[vi].

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 timestamps[vii].

In 2013, a report[viii] 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 police[ix]. 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."*[x]

Critically, UK representatives before the CJEU in July 2013 conceded there was no *"scientific data"* to underpin the claimed need for data retention[xi]. As the authors of a study on the EU Data Retention Directive highlight in respect to the *"evidence"* which has been presented to justify the Directive, it is sufficient to note that the plural of anecdote is not *"data"*[xii].

EU Data Retention Directive

On Friday 8 August, Andrew Colvin, AFP Deputy Commission stated:

> *"And the challenge to that directive, because it's an important point, is on the basis of the* ***oversight mechanisms*** *that didn't exist in the EU …"* (my emphasis)

The court's concerns that the Directive *"does not provide sufficient safeguards…to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data*[xiii]*"* was just one reason leading to the court's decision to strike down the Directive as a disproportionate interference with fundamental rights[xiv]. In 2010, the European Data Protection Supervisor had called the Directive: *"without doubt the most privacy-invasive instrument ever adopted by the EU in terms of scale and the number of people it affects.*[xv]*"* In fact, the legitimacy of the legitimacy of the EU's Data Retention Directive has been questioned since legislation was first proposed in 2002.[xvi]

In April 2014, in the landmark judgment (by CJEU) the EU Data Retention Directive[xvii] was declared invalid. This means that there is currently no EU law mandating the retention of communications data[xviii]. *That the data retention scheme effectively introduced blanket surveillance and treated everyone's data the same was seen as especially problematic:*

> *"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.*[xix]*"*

In practice the CJEU ruling means that any legislation requiring retention of communications data by a Member State of the EU must now comply within the framework set out in the judgment[xx], which includes:

- 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).[xxi]

Following the CJEU ruling:

- In April, four **Swedish** telcos 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.[xxii]
- 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 immediately[xxiii]. The publicly stated reason for this was not the CJEU ruling, but the technical difficulties of using this retained data in police investigations (as discussed above).[xxiv]
- 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.[xxv] Both the Slovenian and **Romanian** Constitutional Courts also ruled blanket data retention to be unconstitutional in July this year.[xxvi].

Digital Rights **Ireland** 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".*[xxvii]

New Data Retention and Investigatory Powers Act - UK

David Irvine, Director-General of ASIO pointed to the data retention law (DRIP)[xxviii] recently passed in the **UK** when discussing the government's moves on this front in a press conference on Friday 8 August 2014.

However, this "emergency" legislation ignored the critical part of the CJEU ruling - that blanket data retention severely interferes with the fundamental rights to respect for private life and to the protection of personal data.[xxixxxx]

In this context, this new legislation is being challenged both in the national courts and at the European Commission level[xxxi]. Two British MPS are launching a legal challenge to the new legislation. It is reported, 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)[xxxii].

An alternative – Targeted preservation notices

Australia

Largely absent from recent discussions on data retention is that changes made to the *Telecommunications (Interception and Access) Act* in 2012[xxxiii] provided new and significant powers to law enforcement and national security agencies following Australia's signing of the Council of Europe Convention on Cybercrime. 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 Act[xxxiv].

'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.

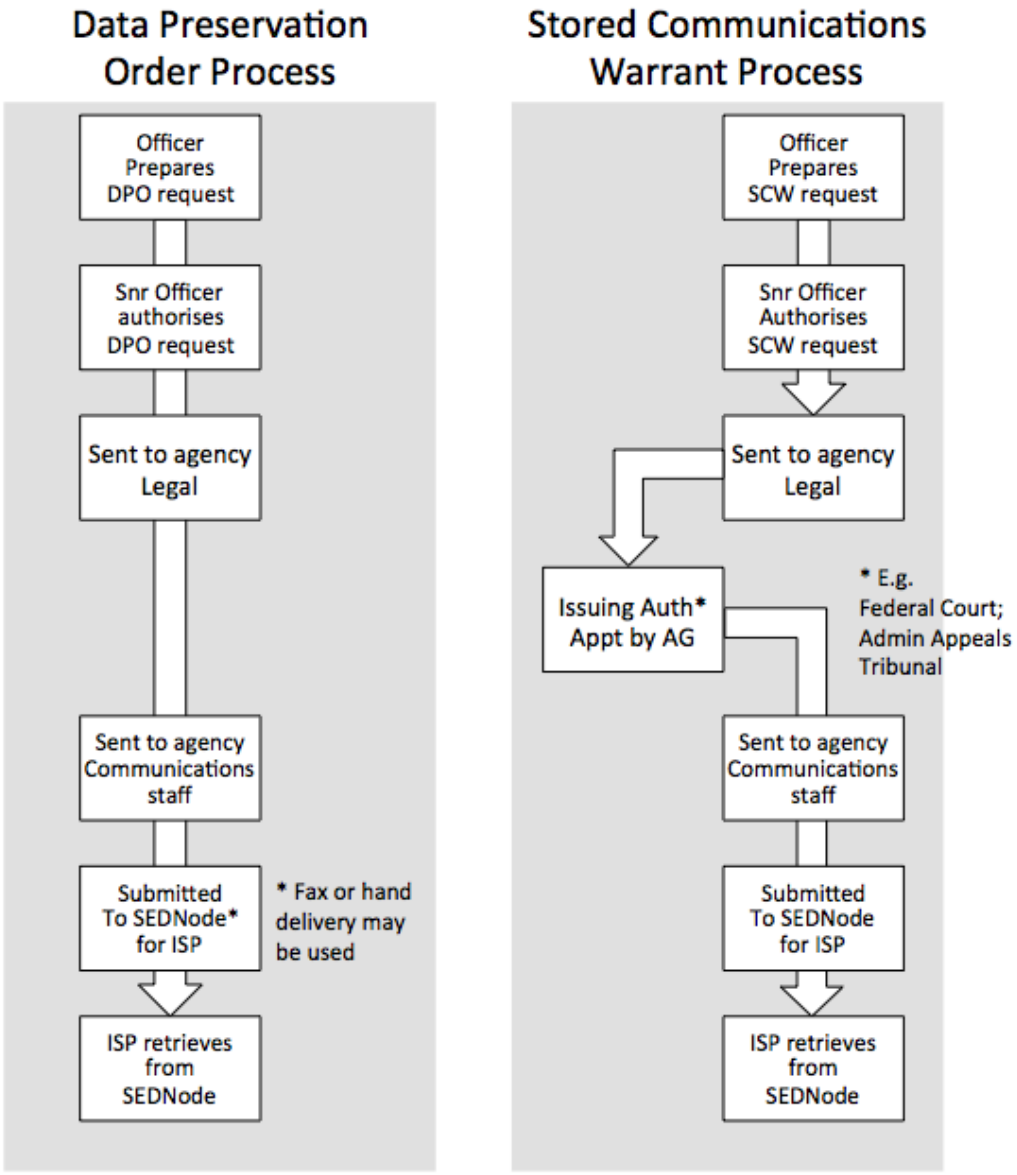
These targeted preservation notices apply to stored communications, defined in the TIA Act to mean:

stored communication *means a communication that:*

a) is not passing over a telecommunications system; and
b) is held on equipment that is operated by, and is in the possession of, a carrier; and
c) *cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.*

Law enforcement agencies will only be able to access the information retained pursuant to a preservation notice under a warrant. We have set out in the following pages a visual representation of how these existing laws operate from a practical perspective. Targeted preservation notices used together with stored communications warrants provide an alternative framework to mass data retention that is designed to ensure that any retention and access to private data is necessary and legitimate.

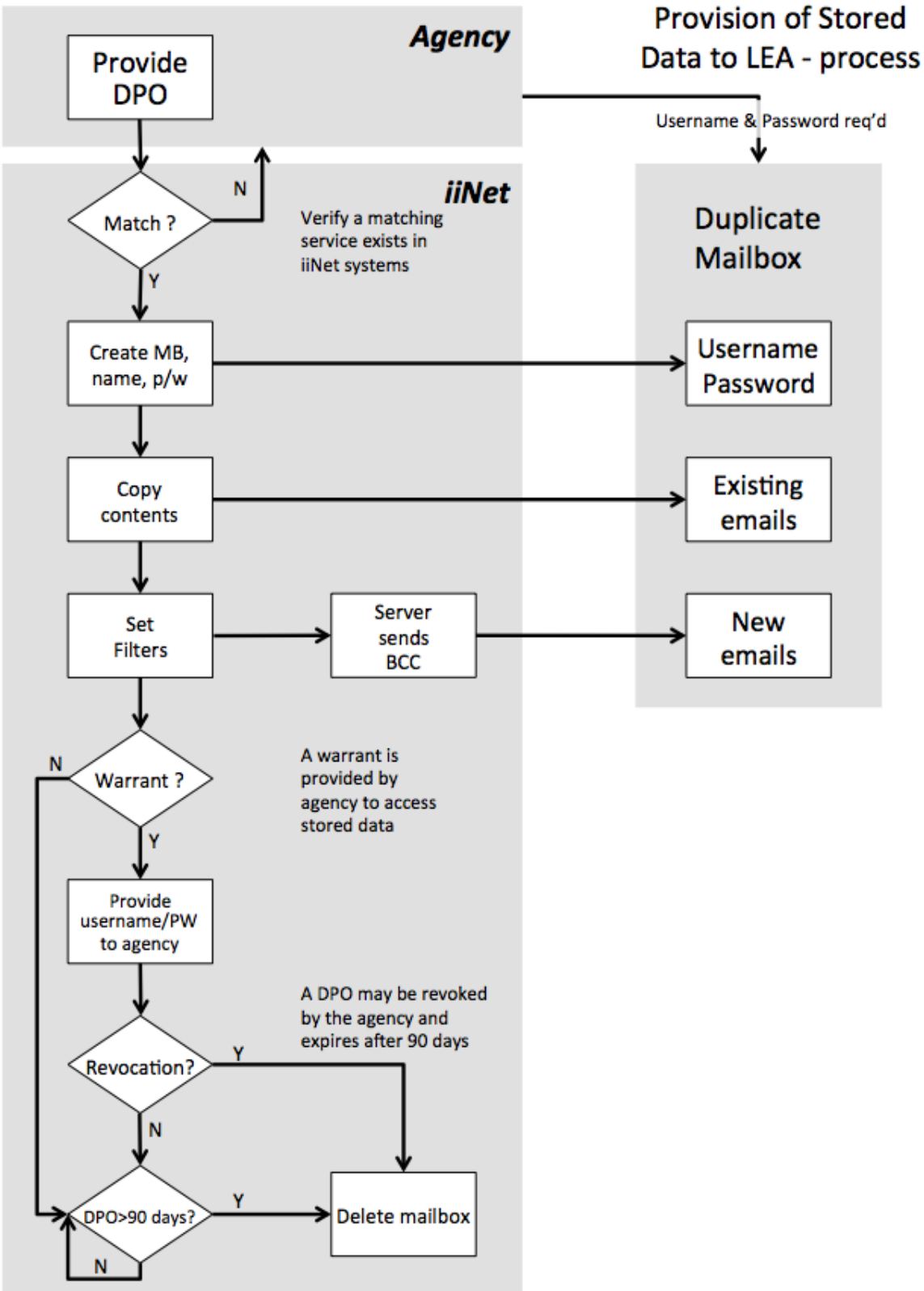
Overview of Data Preservation Order and Stored Communications Warrant processes.



Notes:

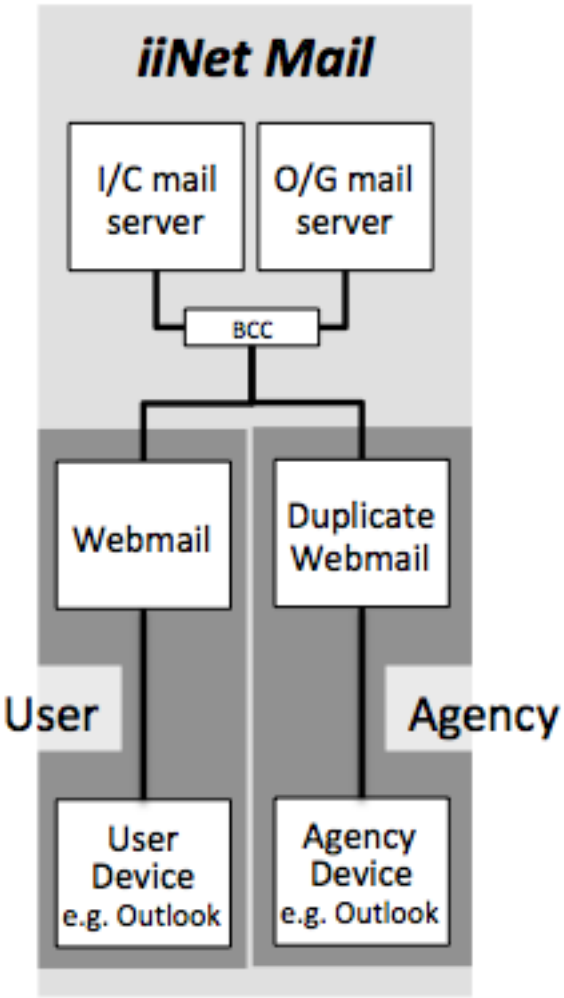
- *Treat as a guide only. Not validated with agencies. Based on iiNet observations.*
- *SEDNode = Secure Electronics Disclosure Node (Operated by Attorney Gen Department)*

Provision of stored data (emails) to Law enforcement agency



DPO = Data Preservation Order
MB = Mailbox; P/W = Password
I/C = incoming
O/G = Outgoing

Interim email arrangements



References

[i] "Data retention is 'the way western nations are going': Brandis", 16 July 2014, available at: http://www.zdnet.com/au/data-retention-is-the-way-western-nations-are-going-brandis-7000031658/

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

[iii] "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/

[iv] "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/?wpmp_tp=1

[v] 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

[vi] "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

[vii] "Denmark: Government postpones data retention evaluation", 13 February 2013, available at: http://edri.org/edrigramnumber11-3dk-postpones-data-retention-evaluation/

[viii] Report is available at: http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf

[ix] "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/

[x] "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

[xi] 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

[xii] 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

[xiii] CJEU Judgment available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN (see in particular paragraphs 55 – 69)

[xiv] Will Australia learn from the EU's mistakes on data retention?, 9 August, available at: http://ohrh.law.ox.ac.uk/will-australia-learn-from-the-eus-mistakes-on-data-retention/

[xv] speech given at the conference 'Taking on the Data Retention Directive', 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

[xvi] 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

[xvii] Text of the Directive is available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

[xviii] The Data Retention Directive Never Existed', Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2467244

[xix] CJEU Judgment available at: http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN

[xx] See xiv p8

[xxi] The Court of Justice declares the Data Retention Directive to be invalid, Press Release of the Court of Justice of the European Union, available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

[xxii] "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/

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

[xxiv] "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/

[xxv] Boehm & Cole study.

[xxvi] 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

[xxvii] "Data retention held unconstitutional in Slovenia", 12 July 2014, available at http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/

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

[xxix] "The DRIP myth list", 14 July 2014, available at: https://www.openrightsgroup.org/blog/2014/the-drip-myth-list

[xxx] "Does the UK's new data retention bill violate the EU Charter of Fundamental Rights?", 10 July 2014, available at: http://eulawanalysis.blogspot.co.uk/2014/04/the-data-retention-judgment-cjeu.html

[xxxi] 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

[xxxii] "MPs to seek judicial review of emergency data law", 22 July 2014, available at: http://www.bbc.co.uk/news/uk-politics-28417886

[xxxiii] See Chapter 3 of the TIA Act and commentary from law firms, available at: http://www.allens.com.au/pubs/tmt/fotmt27nov12.htm

http://www.minterellison.com/publications/new-data-preservation-laws-address-cybercrime-concerns-pu201209/

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