Outside Scope

Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Meeting of Industry Forum

Monday 5th December 2011

11.00 a.m. – 5.00 p.m. *(1.00pm – Lunch, 3.30pm – Afternoon Tea)*

S47G(1)(a)

Facilitator – Catherine Smith

AGENDA

OUTSIDE SCOPE

Data Retention (Simon Lee)

OUTSIDE SCOPE

PAGES 1, 2, 11 & 12 OF THIS DOCUMENT HAVE BEEN REMOVED AS BEING OUTSIDE THE SCOPE OF THE REQUEST

Agenda Item 3 - Data Retention - Simon Lee - Power point presentation

- Models
  - Status Quo
  - Industry co-regulation / self regulation
  - mandatory
    - Decentralised industry
    - Centralised industry
    - Centralised government

S47F(1) - who is industry and how many other people will be included - is the organisation that makes code representative of industry.
Code route is difficult to enforce
- ACMA role to require parties to comply
- Breach after continued non-compliance

How long does industry code take to establish?

S45(1), S47G(1)(a), S47G(1)(b)

S47F(1) - CA has representations for industry players
ACMA satisfied of proper representation

IIA Code - Purely self regulatory - Voluntary code
Co-regulatory - comes to ACMA - registered with ACMA
Public interest tests and consultation requirements

S47F(1) - Use code approach to develop data sets - update over time
Other issues regarding timeframes - legislation

How certain do you want regime -

S47F(1) - complexity of industry makes development of codes more difficult
Correlation of all utility information

S47F(1) - only ever looked at DR from perspective of the consumer not the corporate clients.
Would it ever be used. - Computer banking systems - would it ever be used.

S47F(1) - volumes are an issue - would go directly to business source rather than telco.

S47F(1) - Differentiating between what is retained for business purposes and what is required to be retained. - Address major privacy concerns.

CS - think about some things in primary legislation and have some things in co-regulation code.

[redacted] - where do you start.

CS - would industry like to have the opportunity to develop a code first and then govt come in after if that is not successful.

[redacted] - industry would like the opportunity, but the industry make up is not necessarily going to fully supportive. How do you make all people in industry participate, and comply.

[redacted] - combination of bottom 4. Need cooperation between industry and government. Decentralised industry will not work - efficiencies to be gained.

[redacted] - do agencies need the opportunity to access information from a centralised storage point.

[redacted] - Centralised would be good, but the key issues are timeliness, data is available and is accurate. One stop shop - data normalised.

[redacted] - Timeliness becomes more and more important particularly with cybercrime. Centralisation will be key to this process.

[redacted] - Commercial reality - build systems and start retaining.

CS - Costs is a big factor - are there commercial opportunities for industry. Impacts on small providers.

[redacted] S33(a)(iii)

[redacted] - partnership with industry and government would be better.

- Privacy issues in one storage facility insurmountable - but can be overcome with additional security. - spoke and hub arrangement

[redacted] - think about analogies used and descriptors. Position whole debate on a grown up debate about what should be in this space. This is the issue - high level principles before dealing with the detail.

Who will be covered - C/CSPs and additional industry participants.

Who will be exempt??

Global providers will be requested information.

CS - determining case by case basis on exemptions - would not necessarily be for small end of town.

Exemption regime provides flexibility.

[redacted] - Classes of services blanket exemption would be useful.

S47F(1)

Any approach will need to be proportionate.

S33(a)(iii)

[redacted] - 6.2.f. - [redacted]

S47F(1)

6.1.e - [redacted] S33(a)(iii)

[redacted] - [redacted] S33(a)(iii)

S47F(1)

[redacted] could do web trace to find info - but does not need to own business purpose. Is this really necessary with the prepaid determination. Information may not be useful.

S47G(1)(a), S47G(1)(b)

Is it really required? -gives you something to start with.

1.2 - Current prepaid determination has data retention requirements in it, but inconsistent with the requirement under 1.2 - fixed network.

Differentiation between retention and collection. Needs to be looked at and consistent, not duplicative.

Subscriber information - is this information more generally held by industry for business or other legislative requirements which means that it may not have to be legislated in a data set.

[redacted] generally keeps consumer stuff for two years for possible TIO investigations.

S45(1), S47G(1)(a), S47G(1)(b)

Is there stuff that we keep that you want us to keep longer or is .

3 pronged approach - keeping information for longer

consistent approach to the retention of data

S47F(1)

[redacted] - Are agencies going backwards because they are seeking information that is no longer kept and not looking to see what information is actually available now.

Look to see what other information is available on networks that may do the job rather than thinking only one type of data is useful.

S47F(1)

[redacted] - important that we see all stakeholders as trying. Is there disparity between capability of different agencies. Efficiency gains for agencies that are lagging behind.

NITAC providing assistance to small agencies.

[ ] - appears that certain agencies are ahead of other agencies and there does not appear to be shared. CS - matter for government to determine assistance and costs.

[ ] - imposing requirements on C/CSPs which does not actually have visibility of information.

[ ] - goes towards a level playing field for the market segments (3 tiers).

[ ] - standard default data set - use tiered system to differentiate.
OPT in system to negotiate an alternative if appropriate.

[ ] - What approach do we take - can different segments adopt different approaches.

[ ] - what seeing in marketplace is getting squeezed out of the application service layer. Apple launched application that will displace other carriers SMS business.
[ ] - Already happened in Dutch market - no SMS in Dutch market - using bypass product.
[ ] S47G(1)(a)

[ ] - got to reduce costs to maintain competitiveness.

Timeframe

- depend on costs
- ability for industry to remove data from system - processes will need to be put in place.

- [ ] - up to two year period need to have a destruction requirement if has no business or tax purpose.
- [ ] - need to implement business processes to ensure destruction processes.
- [ ] - visibility of whether data is being queried or not. Every time you ask a query you leave a footprint - potentially identifies targets. Very difficult to eliminate risk from business - have to extract all information and keep a separate data base. The security required predicates the type of storage requirement / model.
- [ ] - Would someone have an audit role - security of LELU is important.
- [ ] - Destruction clauses would be good

Lunch Break - 1:00pm

Back - 1:30pm

- Standardisation specifications - any comments

[ ] - indicates that it is better to standardise at the industry end rather than the agency end. Is this a valid assumption.

S45(1), S47G(1)(a), S47G(1)(b)

[redacted] have standard technology for data storage. Lowest cost option is not necessarily at industry end.

[redacted] industry has various networks and data storage processes - difficult for agencies.

[redacted] - [redacted]

S37(2)(b), S45(1), S47G(1)(a), S47G(1)(b)

[redacted] - want to move towards electronic request and delivery.

[redacted] - looking at ETSI so it would be cheaper in longer term to get built in by vendors.

[redacted] - We source equipment from US, EU and China.

[redacted] look to distinguish between TI, CAD and subscriber information.

[redacted] - Vendors are better able to work with standards rather than develop separately.

Not going to get an ETSI dump from [redacted] Best to hope for is normalised information.

S45(1), S47G(1)(a), S47G(1)(b)

Do not presupposed - if you end up with centralised model - then data quality becomes self answering.

[redacted] - Inevitably some data will be lost or not useable / un recoverable. Is regime based on risk management or gold plated.

CS - Risk based is immediate though, but need to take away and think about it.

[redacted] - web trace is difficult - single feed into single system - has previously been lost.

CS - Various risk factors can probably be identified.

[redacted] - Significant costs associated with legacy systems.

LM - We need to look at all of these costs and discuss with agencies.

- How long to build systems and implement
- [redacted] - commercial planning windows - long cycles of planning well advanced for 12/13 budget, mandatory regulatory function - build something - 4 releases a year - (IT interface) upfront planning is 12 months and 6 months for build.
- Mobile and fixed telephony - would not have to do much, but if anything needs changing would need to have some lead time.
- IP would be much more different.
- 12-18 months to be fully compliant.
- [redacted] identified that they do not keep unsuccessful calls and they would have to build a system to retain data and manage.

S45(1), S47G(1)(a), S47G(1)(b)

- [redacted] - Is there an option to keep some data for a shorter period of time - can require more money and process and complexity.
- Maybe have a minimum retention period and then a different time frame for which information may be kept for a period of time.

- What other legislation is in place or business requirements that are duplicative for data retention.
- [redacted] - what industry retains will depend on business law requirements which may be different for different services or plans.
- PS - Pre-paid determination - should carve out be contained in data retention regime or pre-paid determination.
- DR is a requirement to retain, not what to collect.

[redacted] - how do you get consistency across identity attribute information. Need to think how these work together.

[redacted] - credit card information - Payment Card Industry Standards compliance - information security around credit card data.

Data set 1.1C need to be consistent with other laws and prepaid determination.

IPND Review - Is it worth attacking from this end. Can there be something that we can do here.

[redacted] - Costs may be too high for agencies in the long run. Capex costs are not generally recovered, but

IPND-e is a big cost subsidiser. Cost recovery formula and push back to agencies needs to be looked at carefully.

[redacted] - IPND already provides a centralised model for doing things - should keep in mind.

- Impact on networks, staffing, security.

Responses requested in relation to consultation material by 6 January 2012.

Privacy Forum 6 September 2011

Morning Session – Industry

Summary of discussion

ALL DELETIONS ON THIS PAGE ARE MADE UNDER SECTIONS 45(1), 47F(1), 47G(1)(a) & 47G(1)(b)

Speaker	
SO	Sabeena Oberoi (DBCDE)
CD	Chris Drew (DBCDE)
LS	Leife Shallcross (OAIC)
JP	Joanne Pickering (OAIC)
AS	Ahmad Shah (PM&C)
CB	Catherine Bridges (AGD)
PH	Piet Hooker (AGD)
SL	Simon Lee (AGD)
SW	Stuart Woodley (AGD)

Comment

The TIA Act was intended to protect privacy but because of the holes in it, it can be said that it's against privacy.

PIA's are now more standard and are more interactive. While a range of structures are available, the best privacy impact assessments involve conversations with the general public.

What is privacy?

Privacy is not:

- citizens wanting to keep everything secret or confidential, nor it is about having something to hide. Rather, privacy is about human dignity.

Privacy is:

- control: deciding what to reveal and when to reveal.
- creepiness factor: much concern about big brother, too much information and intrusive powers.

Privacy Forum 6 September 2011

Morning Session – Industry

Summary of discussion

Concerns about this motivate people to think about privacy. Privacy law deals with function enhancement/function creep very badly.

- risk and who bears it – focus is risk allocation rather than risk management as the ordinary citizen is now being asked to shoulder the risk in the online world Responses include the EFT Act which takes a deliberate move to shift some risk back to industry.

Global interest in privacy is increasing: massing changes in technology, how we communicate, the amount of data flowing around and the increase in our electronic footprint as well as awareness of how data is being created and used (eg location data).

Challenge to facilitate reasonable use and privacy of personal information – people are seeking greater protection:

- behavioural targeting in advertising – advertisers receiving a negative reaction so industry self-modifying some of its behaviour
- -data breach notification
- exploration of the 'right to be forgotten'
- EU – consent needed to place cookies (statement of need)

cf EU – data retention requirements.

- all jurisdictions have reasonable law enforcement access regimes.

www.zeit.de/datenshultz/malte-spitz-data-retention

One view is that privacy and security are a zero-sum game (trade off)

Cf Book to read - Daniel Solove - "Nothing to Hide the False Tradeoff Between Privacy and Security"

TIA Act Approach - long in the tooth, framework and assumptions creaky.

- Contains a seriousness threshold and considered, documented provisions including privacy, independent scrutiny and accountability

The challenge is to modernise the framework to allow vital access for law enforcement agencies AND to have community trust (which must be given not demanded).

Role of a PIA –

"Tells the story" of a project from a privacy perspective and helps to manage privacy risk s and impacts.

A PIA is not a compliance assessment against the 10 information privacy principles but an analytical tool that helps to identify privacy risks, foresee problems and bring forward solutions"

Several steps are involved:

Ist step – information gathering and mapping information flows (disclosure and gathering with different principles)

2nd step - analysis against law and other risks

3rd step - stakeholder consultation including PUBLIC (bring public into your confidence) and internal

4th step – written conclusions, usually recommendations that facilitate internal thinking and are sometimes published.

Informing our views (how the task will be done):

Privacy Forum 6 September 2011

Morning Session – Industry

Summary of discussion

4A Framework, analysis against privacy principles, overseas experience and stakeholder views to inform conclusions
AGD view about the PIA process:
PIA document has a formal role, taken into account at the most senior levels. Privacy is important at the start of the process - first principles reform requires extensive consideration of privacy and an independent consultancy ensures privacy interests are factored in from the start.
First consideration: What are your processes for managing requests, how do you make the Act work?
What are your business impacts, what is the cost of accountability?

SW

S47F(1)

QUESTION 1

Current practices for assisting agencies and managing data

Telecommunications data is likely to be the most interesting area, how do companies manage data?

Outside Scope

S37(2)(b)

S47F(1)

MATERIAL OUTSIDE SCOPE OF REQUEST

S37(2)(b)

Distinction between what the network holds itself - then overlay of data retention requirements that might require additional information – beyond what the organisation NEEDS to collect.
Swapping fundamental architecture in telecommunications. Used to collect a lot of information as that was the way they billed.

THE FOLLOWING PAGE HAS BEEN REMOVED AS BEING OUTSIDE THE SCOPE OF THE REQUEST

Privacy Forum 6 September 2011

Morning Session – Industry

Summary of discussion

S47F(1)

Are there existing privacy issues with the current regime? Data retention - concern about data aggregation.
Given the value that companies for business purposes are placing on 'big data' - there is clearly going to be value for law enforcement too.
Identity becomes a great issue.
We have all these protections about how we deal with the information/hand it over etc - but then have no idea what the law enforcement agencies do with the information.

QUESTION 2

S47F(1)

MATERIAL OUTSIDE SCOPE OF REQUEST

Privacy Forum 6 September 2011

Morning Session – Industry

Summary of discussion

S47F(1)	What information does your system need to collect in the future? Possible privacy principle: law is structured on the basis that no carrier will be asked to retain data beyond its normal business practices.
QUESTION 3	Oversight and Accountability
S47F(1)	MATERIAL OUTSIDE SCOPE OF REQUEST
	S37(2)(b)
SO	
Next Steps	
SW	Haven't made concrete plans for further discussions/meetings like this, can do one on one.
	Would like more discussions about the privacy impacts of identification of customers/targets and around jurisdiction (following input from AGD on the policy directions)

Attendees:

S38(1)	
Kathryn Bellgard	AFP
Chris Cheah	ACMA
Chris Drew	DBCDE
Sabeena Oberoi	DBCDE
Damian Mahoney	DBCDE
S47F(1)	S47G(1)(a), S47G(1)(b)
Catherine Smith	AGD – Facilitator
Wendy Kelly	AGD
Stuart Woodley	AGD
Lionel Markey	AGD
Simon Lee	AGD
Jillian Cook	AGD
Andrew Newman-Martin	AGD
Sarah Bury	AGD
Megan Chalmers	AGD

The meeting opened at approximately 9.40am.

Catherine Smith welcomed participants and outlined the purpose of the Industry Forum.

MATERIAL OUTSIDE SCOPE OF REQUEST

This is the second meeting of the industry forum. The last meeting consisted of

Outside Scope

and data retention. As no specific feedback was received following that meeting, it is presumed attendees were satisfied with its direction.

MATERIAL OUTSIDE SCOPE OF REQUEST

PAGES 2-10, 14 & 15 OF THIS DOCUMENT HAVE BEEN REMOVED AS BEING OUTSIDE THE SCOPE OF THE REQUEST

MATERIAL OUTSIDE SCOPE OF REQUEST

Simon Lee spoke to the subject of data retention, saying it had been a topic for consideration at the last meeting and he would be providing an update on actions since then.

Consulted with industry through 2009-10, looking at mandatory regime where carriers and CSPs hold their own data in their own systems for up to 2 years. Looking at datasets for standard telephony and IP communications; made decision to roll into TI reform package as a whole

Recommendations from Senate Committee:

Cost benefit analysis of data retention to justify business case from agency perspective of benefits of data retention

Financial impact on industry, compared to impact on agencies' investigations

Know that any data retention scheme would be sufficiently secure against hackers

Consult with wider range of stakeholders

Examples taken on board and considered holistically within policy.

Data retention—keystone for agencies' abilities in the future in relation to TI.

Mandatory decentralized data retention model:

-status quo

-industry self-regulation model

-developing previous data retention model

-centralised repository run by industry

-centralised repository run by government

-costs: to store, maintain, and how

S47F(1) , in relation to security: who is looking at data, guarantee of data integrity. Two different systems, two different sets of costs. Can't make determination of costs without knowing how data has to be treated.

S47F(1) : additional costs for new data set for purposes of complying with TI; be aware of this.

S47F(1) : data sets. Read dataset next to ETSI standard—very little difference. But, current draft has national requirements: carriers grade [natting]? [not sure if this was an acronym?]

S47F(1) : do we capture IP origin address on packets in this model for datasets (increase costs)

S47F(1) : not a requirement.

S47F(1) : if they haven't got it (the data), don't have to create it.

S47F(1) : industry not required to create anything if they haven't already done so.

S47F(1) : in relation to IP address and costs?

S37(2)(b), S45(1), S47F(1), S47G(1)(a), S47G(1)(b)

Discussion among S47F(1) and S47F(1) in relation to creation of data and IP addresses.

S37(2)(b), S45(1), S47F(1), S47G(1)(a), S47G(1)(b)

S47F(1): when product offering changes, will these datasets still be relevant then? So, if something new is created now, a dataset, when the product offering changes, will this still be relevant—comes back to cost of creating datasets now. From a business perspective, budget and costs. Is industry up for compensation from government for capturing information (creating dataset) today that may not be relevant in the future? His point: if customer A has a variety of products, will probably keep the data about his services, but the likelihood of requiring the datasets with his IP addresses...what happens in 4 years, when data no longer needed? They build in capacity/ability now to accommodate this capacity, what happens if/when data no longer needed? S47G(1)(a), S47G(1)(b) S47G(1)(a), S47G(1)(b)

Catherine Smith: government cannot give any guarantees now. The reality is that government puts forward policies which industry may or may not agree with. AGD is ensuring that all relevant arguments/views are put forward to the government. The reality is, [they—industry?] have been reminded by law enforcement of the benefits to society of these particular policies (child safety, protection, etc).

S47F(1): concerns in relation to issue of relevance of data being retained, the cost to industry of retaining this potentially obsolete data, and for how long?

S47F(1): in a converged society, IP address is the most useless identifier, because it will change as you roam. Should be MAP address or something else.

S47F(1): dichotomy in relation to the importance of telecommunications data, yet he has been to LEAs and they spend very little time on telco evidence. He is asking AGD—impress upon agencies the importance of this, especially if industry is being asked to bear the cost of complying with TI.

Simon Lee: another survey of what data is currently being retained for comparison purposes.

Catherine Smith concluded discussion of this topic by saying data retention was the most controversial area of reform.

MATERIAL OUTSIDE SCOPE OF REQUEST

MATERIAL OUTSIDE SCOPE OF REQUEST

Catherine Smith wrapped up the day:

MATERIAL OUTSIDE SCOPE OF REQUEST

Outside Scope

- Data retention is the 'elephant in the room'. Need to work more on this, have intense discussions just about data retention. Must discuss more in-house and with industry as well. The value of any proposal must be considered. Important task? Future-proofing. No point in developing something that will be obsolete in a few years.
- S33(a)(iii)

MATERIAL OUTSIDE SCOPE OF REQUEST

Catherine Smith proposed the next meeting be held in early December, in Melbourne. They are looking at an ICC, and details will be arranged and advised shortly.

At the next meeting, each provider is requested to provide a recap of what it considers to be the pressing issues in relation to TI reform.

Catherine thanked everyone for their participation and the meeting closed at approximately 3.16pm.

11/10923.

11 # 887770.doc

Outside Scope

Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Meeting of Industry Forum

Friday 21 October2011

9:30am – 3:15pm

Robert Garran Offices, Barton, ACT

Facilitator – Catherine Smith

AGENDA

9:30 – 9:45	
9:45 – 10:00	
10:00 - 10:45	
10:45 – 11:15	
11:15 – 12:00	MATERIAL OUTSIDE SCOPE OF REQUEST
12:00 – 12:45	
12:45 – 13:30	
13:30 – 15:00	Data Retention (Simon Lee);
15:00 – 15:15	Outside Scope

Outside Scope

Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Policy directions meeting

Wednesday 7 September 2011

9.00am–4.30pm

Boulevard Hotel, William Street, Sydney

Chair: Catherine Smith, Attorney-General's Department

AGENDA

9.00am	MATERIAL OUTSIDE SCOPE OF REQUEST
9.15-9.45am	
9.45-10.15am	
10.15-10.45am	
10.45-11.30am	
11.30am-12.30pm	
12.30-1.00pm	
1.00-2.00pm	
2.00-2.30pm	
2.30-3.00pm	Data retention (Simon Lee)
3.00-3.15pm	MATERIAL OUTSIDE SCOPE OF REQUEST
3.15-3.45pm	
3.45-4.15pm	
4.15-4.30pm	
4.30pm	

11/18969-01 11 # 709486 00C

Privacy Workshop

6 September 2011

Boardroom

Bayview Boulevard Sydney

50 William Street

02 93837222

Agenda

Time	*Topic*	*Facilitator*
10.00 am	• Introductions	S47F(1)
10.10 am	MATERIAL OUTSIDE SCOPE OF REQUEST	
10.30am		
11.00 am		
	o data retention and storage	
11.30 am	MATERIAL OUTSIDE SCOPE OF REQUEST	
12.00 pm		
12.00		

Outside Scope

Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Thursday 25 August 2011

1.30–3.00pm

Robert Garran Offices, 3-5 National Circuit, Barton

AGENDA

1.
2.
3.

MATERIAL OUTSIDE SCOPE OF REQUEST

d. Data retention (Simon)

4.
5.
6.

OUTSIDE SCOPE

11/10923. 11 #6168740DOC

Outside Scope

Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Meeting of Industry Forum

Friday 5th August

9:30am – 3:30pm

Robert Garran Offices, Barton, ACT

Facilitator – Jamie Lowe, Assistant Secretary, Attorney-General's Department

---

AGENDA

9:30 – 9:45

9:45 – 10:45

10:45 - 11:00

11:00 – 12:45

MATERIAL OUTSIDE SCOPE OF REQUEST

5. Data retention (Wendy Kelly to lead)

12:45 – 13:30

13:30 – 15:15

15:15 – 15:30

MATERIAL OUTSIDE SCOPE OF REQUEST