Submission to the

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Pirate Party Australia

Mozart Olbrycht-Palmer (mozart.palmer@pirateparty.org.au)

19 January 2015

Contents

1 Summary 2

2 Is data retention necessary? 2

3 How much data will be retained and for how long? 5

4 What data will be retained 7

5 Non-content data 9

6 Where and how data will be stored 10

7 Destination or address of communications 10

8 Location 11

9 Data retention plans 11

10 Review period 11

11 Access to stored data 12

12 Costs 14

13 Conclusion 14

1 Summary

The Pirate Party thanks the Parliamentary Joint Committee on Intelligence and Security ('PJCIS') for the opportunity to submit on such an important issue as the introduction of a mandatory data retention regime.

The Pirate Party opposes the introduction of a mandatory data retention regime on a number of grounds. It is the Party's view that the case for such a regime has not been sufficiently made out and considers that, if introduced, it would be an unreasonable and unnecessary intrusion upon the right to privacy. The Pirate Party is also concerned that storing such enormous amounts of personal data will lead to abuse, both by service providers and those agencies with access, as well as create a high-value target for state and non-state actors.

However, if Australia is to have a mandatory data retention regime, the proposed retention period is unjustified and inconsistent in light of evidence that very little of the retained data older than 12 months will be useful. The privacy protections regarding access to the retained data in the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 are insufficient, and would allow access to sensitive records with limited oversight and no requirement of judicial authorisation.

Further, interested parties have been given limited opportunity to assess the true impact that this regime would have because the data to be retained is discretionary and yet to be specified. In addition, the cost of implementing a mandatory data retention regime does not appear to have been modelled, and evidence suggests that it may be substantial.

2 Is data retention necessary?

Data retention is proposed ostensibly to assist in the prevention and detection of criminal activity, and the prosecution of those engaged in terrorism, drug trafficking, child exploitation, fraud and other crimes of a conspiratorial nature.[1]

This information can theoretically be used to monitor organised crime and criminal conspiracies, including terrorist cells and child exploitation rings, by revealing connections between suspects. Telephone numbers, IP addresses, and other identifying data can be used to match suspicious activity with individuals and organisational entities.

[1] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 2.

However, experience overseas has shown that mandatory data retention regimes do not seem to provide any significant benefit for the prevention, detection or prosecution of crime. The German Parliament's Research Service observed that the

> marginal increase in the clearance rate by 0.006 percent could raise doubts about whether the provisions in their current form would stand their ground under a proportionality review. *In any case, the relationship between ends and means is disproportionate.*[2]

Across the Atlantic, the US Government's Privacy and Civil Liberties Oversight Board concluded that

> the Section 215 [bulk telephony metadata] program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack. And we believe that in only one instance over the past seven years has the program arguably contributed to the identification of an unknown terrorism suspect. Even in that case, the suspect was not involved in planning a terrorist attack and there is reason to believe that the FBI may have discovered him without the contribution of the NSA's program.[3]

As a result of the above, it is clear greater investigation is needed to verify the claims of Australian law enforcement and intelligence agencies, as their claims appear to run contrary to the evidence available from the United States and Germany.

Furthermore, the Attorney-General's Department website gives an illustration of the adequacy of current laws:

---

[2]Arbeitskreis Vorratsdatenspeicherung, *Impossible to Ensure Legality of EU Communications Data Retention Directive Says German Parliament* (26 April 2011) Vorratsdatenspeicherung <http://www.vorratsdatenspeicherung.de/content/view/446/79/lang,en/>citing Ronald Derksen, 'Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta' ['Compatibility of the Data Retention Directive with the European Charter of Fundamental Rights'] (Preparation No WD 11–3000–18/11, Wissenschaftlichen Dienst des Bundestages [Research Service of the German Parliament], 2011) 20 <http://www.vorratsdatenspeicherung.de/images/rechtsgutachten_grundrechtecharta.pdf>.

[3]United States Privacy and Civil Liberties Oversight Board, *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* (2014) 11: <http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf>.

Case study 2: Telecommunications data foils mass casualty terrorist attack in Australia

In 2005, a combined Australian Security Intelligence Organisation (ASIO) and law enforcement operation (Operation Pendennis), prevented a mass casualty terrorist attack in Australia, including targeting of the Melbourne Cricket Ground, and resulted in the arrest and conviction of 13 men on terrorism charges, with sentences of up to 28 years in jail.

Telecommunications data was critical to the successful outcomes of the investigation and subsequent trial. Telecommunications data was used to identify a covert phone network that was being used as an attempt to hide illicit activities from ASIO and law enforcement agencies. Had this data not been available, ASIO and law enforcement agencies would likely not have understood the network of people that were involved in the planning of a terrorist attack in Australia.

Without access to this telecommunications data, ASIO would not have been equipped to provide advice to manage the risk and work with law enforcement partners to prevent a mass casualty terrorist attack in Australia. To obtain the same information via other means (subject to this information being available through other means) would have required much higher levels of intrusion into an individual's private life. The analysis of telecommunications data is a key component in the overwhelming majority of priority security investigations and consistently proves to be an invaluable intelligence capability, including helping eliminate individuals from security concern.[4]

Operation Pendennis was successful without a mandatory data retention regime. Using this as a case study to support a mandatory data retention regime is inappropriate as it demonstrates that in 2005 law enforcement and intelligence agencies had sufficient capabilities with regard to telecommunications data. Rather than being a case study in support of mandatory data retention, the Attorney-General's Department has presented a case demonstrating the efficacy of current laws.

The most recent confirmed and suspected terrorist incidents in western countries — those in Paris, Sydney, Montreal and Boston — were committed by assailants already known to authorities, and in some instances were acting alone. Thus, data retention would not have helped to pre-empt them. Resources should be directed towards current law enforcement efforts and targeted surveillance rather than placing an entire nation under suspicion

[4]Attorney-General's Department, *Case studies*, <http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Casestudies.aspx>.

and thereby diverting, diluting and distracting their efforts.

3 How much data will be retained and for how long?

An argument used to support a mandatory data retention regime is that unless service providers are required to retain information, they simply will not. The concern arises, therefore, from a perception that service providers will keep less information and for shorter periods of time as it becomes increasingly unnecessary and uneconomical to do so.[5]

However, what this argument fails to recognise is the reality that mandatory data retention may require the retention of information that has never in fact been kept by service providers. This means that rather than experiencing a decreased amount of data being available as a result of service providers storing less data, an unprecedented amount may be made available under a data retention regime that requires service providers to store more data than has been stored in the past.

While this may be desirable for certain law enforcement and intelligence agencies, it indicates the potential for a mandatory data retention scheme to be far more intrusive than claimed. If a service provider is required to store transient data incidental to the provision of the service, this may effectively involve creating records that the service provider has never needed to keep.

In effect this will be more akin to a data creation regime than a data retention regime in many cases.

This problem is raised by the proposed s 187A(1) that requires service providers to 'keep, or cause to be kept' the records specified. The regulations will specify the data required to be retained, but this does not appear to require any reference to currently retained data or common industry practice.

Similarly, two years may be a longer period than records have been kept in the past. An increase in the type of data and the period of time for which they are stored would be a dramatic intrusion upon privacy.

The following table, created from data published by the European Commis-

[5] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 2, 5.

sion,[6] shows the data retention periods across the European Union:

6 months (all data)	Cyprus, Lithuania, Luxembourg, Romania
12 months (all data)	Belgium, Bulgaria, Denmark, Estonia, Finland, France, Greece, Netherlands, Portugal, Spain, United Kingdom
12 months (telephony data) 6 months (Internet data)	Malta, Slovakia
12 months 6 months (unsuccessful calls)	Hungary
14 months (telephony data) 8 months (Internet data)	Slovenia
18 months (all data)	Latvia
24 months (all data)	Poland
24 months (telephony data) 12 months (Internet data)	Ireland, Italy

The two-year retention period proposed in the Data Retention Bill is generally inconsistent with past European Union practice, where the most common period was 12 months or less.

If the dubious case for mandatory data retention is accepted, it remains questionable as to whether two years is necessary. According to the European Commission's 2011 evaluation report of the Data Retention Directive:

> Quantitative evidence provided … so far by Member States regarding the age of retained data suggests that around ninety percent of the data are six months old or less and around seventy percent three months old or less when the (initial) request for access is

[6] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (Report from the Commission to the Council and the European Parliament, European Commission, 2011) 14 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF>.

made by law enforcement authorities ….[7]

In 2008, information provided by nine Member States of the European Union (Cyprus, the Czech Republic, Denmark, Estonia, Ireland, Latvia, Mlta, Spain, and the United Kingdom) indicated 'around ninety percent of the data accessed by competent authorities that year were six months old or less and around seventy percent three months old or less when the (initial) request for access was made.'[8] Less than 2% of the telecommunications data accessed was more than 12 months old, while just 12% was 6–12 months old.[9]

The Pirate Party contends that a two-year data retention period is unreasonable and unjustified. The effects of the demonstrable intrusion upon privacy created by a mandatory data retention must be limited as much as possible. Given 98% of telecommunications data accessed in Europe was under 12 months old, and 86% was under 6 months old, the Pirate Party considers that if the PJCIS accepts there is a case for instituting a mandatory data retention regime it should recommend the retention period be reduced to 6 months.

4 What data will be retained

The legislation provides very few limits on what can be retained, and fairly broad guidance for what the regulations can prescribe.

The proposed s 187A(1) provides that the data to be retained will be included in the regulations. This raises two concerns: firstly, that it is unclear whether these will be based on the existing types of data currently retained by service providers, and, secondly, that there is an immediate problem with critiquing this legislation in terms of its appropriateness and impact on human rights. The first of these issues has been substantially addressed above.

The second issue — the lack of detail regarding what will be retained — is particularly worrying as it hampers analysis of the impact of the legislation. The legislation is therefore incomplete, giving the public and the PJCIS insufficient information to make meaningful and informed recommendations and criticisms.

The proposed s 187A(2) uses the phrase 'The kinds of information prescribed for the purposes of paragraph (1)(a) must relate to one or more of the following matters' as though it is intended to be a limiting safeguard. The reality is that the list of matters to which the retained data must relate is

[7] Ibid 15.
[8] Ibid 22.
[9] Ibid.

exceptionally broad. It allows for retention of data that relates to characteristics of subscribers, accounts and devices, the origins and destinations of communications, when, where and for how long a communication occurred and the type of communication. There is little conceivable information that could not be the subject of the regulations.

The proposed s 187A(4) contains sparse restrictions. It does not require service providers to keep the content or 'address' of certain communications, communications that they are required to delete, and location information not used for providing the service. Between the proposed ss 187A(1), 187A(2) and 187A(4) there is enormous flexibility and scope for what can be retained, with minimal exclusions.

The statement of compatibility with human rights claims that 'The purpose of the Bill is to require service providers to retain a strictly defined subset of telecommunications data produced in the course of providing telecommunications services.'[10] This may well be the purpose, but it is inadequately and improperly conveyed in the legislation. The data to be retained is anything but strictly defined: apart from vague limits, the Minister has discretion over what will be retained and is yet to publish the regulations specifying what will be held.

These concerns have been addressed by the Senate Standing Committee for the Scrutiny of Bills, which stated that 'the bill does not itself contain a clear definition of the specific types of data that are covered by the data retention scheme' and did 'not consider paragraph 187A(1)(a) to be an appropriate delegation of legislative power.'[11] In the Committee's view 'it seems appropriate for Parliament (not the executive) to take responsibility for ensuring that the scheme is adequately responsive to technological change in the telecommunications industry.'[12]

The Parliamentary Joint Committee on Human Rights ('PJCHR') was 'concerned that the types of data to be collected remain unspecified until such time as the relevant regulation is made' and recommended 'that, to avoid the arbitrary interference with the right to privacy that would result from reliance on regulations, the bill be amended to define the types of data that are to be retained.'[13]

A further consideration is the amount of irrelevant data that will be retained. While this may have some bearing on the cost, the greater consideration is the size of the 'data haystack' that will be created. Increasing numbers of devices

[10] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 5.

[11] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Alert Digest No. 16 of 2014*, 26 November 2014, 3.

[12] Ibid.

[13] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report of the 44th Parliament* (2014) 14.

are being equipped with the capacity to connect to the Internet for various reasons, and, while some might argue that a large haystack is desirable,[14] the usefulness and efficiency of wading through retained data generated by Internet-capable refrigerators, robot vacuum cleaners, automatic orchid hydration systems, children's game consoles and various hobbyist devices among others is questionable. Already concerns have been raised that the sheer volume of data being stored is overwhelming law enforcement and intelligence agencies, hampering their ability to adequately detect and prevent terrorist attacks such as those in Paris and Boston.[15]

5 Non-content data

The Bill's explanatory memorandum states that 'telecommunications data is less privacy intrusive than content'.[16]

However, the PJCHR stated: 'Communications data can reveal quite personal information about an individual, even without the content of the data being made available, revealing who a person is in contact with, how often and where. This in turn may reveal the person's political opinions, sexual habits, religion or medical concerns.'[17]

The claim made in the explanatory memorandum that 'Access to telecommunications data also infringes less on personal privacy compared to other covert investigative methods as it does not include the content or substance of the communication'[18] is therefore significantly misleading.

In literal terms, telecommunications data can reveal who (the individuals involved), where (the location), when (the date and time), why (the subject of the communication) and how (the devices) — the only thing missing is what (the contents).[19] Even then, as the PJCHR suggests, the content of a communication can be extrapolated to a degree from the other aspects.

[14]See eg John Yoo, 'The Legality of the National Security Agency's Bulk Data Surveillance Programs' (2014) 37 *Harvard Journal of Law and Public Policy* 901, 907–908.

[15]'Authoritarians Use Paris Terror Attack As Excuse for Power Grab' on *WashingtonsBlog* (16 January 2015) <http://www.washingtonsblog.com/2015/01/authoritarians-use-paris-terror-attack-excuse-power-grab.html>.

[16]Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 3.

[17]Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report of the 44th Parliament* (2014) 13.

[18]Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth) 5.

[19]This is partially acknowledged by the Attorney-General's Department: see eg Attorney-General's Department, *Data retention*, <http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/default.aspx>.

6 Where and how data will be stored

In order to remain competitive, service providers are likely to consider outsourcing the collection, management, storage and security of personal and private data to cheaper overseas locations. Currently some of the leading outsourcing destinations are India, China, the Philippines, Argentina, Bulgaria, Malaysia, Pakistan and Egypt. Questions arise as to where the data will be stored and whether it can be stored in a secure manner. Would, for example, the Government allow storage of telecommunications data in the countries named? Has the Government considered that local storage could increase the costs for consumers, while overseas storage may reduce the security of personal data?

Merely storing such a tempting honey pot of personal data in Australia carries security risks. According to a 2013 article in *The Australian*:

> Chinese hackers have stolen the top-secret floor plans of Australia's newly-built spy headquarters … . Documents detailing the ASIO building's communication cable layouts, server locations and security systems had all been illegally accessed … . 'The plans were traced to a server in China.' [T]he theft meant China could bug the building.[20]

If ASIO cannot ensure the security of its own information, what guarantee do Australians have about the security of their personal and private data?

7 Destination or address of communications

The proposed s 187A(2)(c) requires that the destination of a communication be retained, while s 187A(4)(b) purports to exclude 'addresses on the Internet'. The Pirate Party is not convinced that this is an appropriate way to achieve the aims of the legislation: how are 'destination' and 'address' delineated? While it is apparent that the proposed legislation is attempting to distinguish interpersonal communications from web browsing, this ought to be expressed clearly. Contrary to the note in the legislation, the difference between 'destination' and 'address' is not immediately apparent and merits further consultation with technical experts.

[20] Mitchell Nadin, 'ASIO secret floor plans "stolen by Chinese hackers"', *The Australian* (online), 28 May 2013 <http://www.theaustralian.com.au/national-affairs/foreign-affairs/asio-secret-floor-plans-stolen-by-chinese-hackers/story-fn59nm2j-1226651733841>.

8 Location

The proposed s 187A(4)(e) states that a service provider is not required under s 187A to store:

> information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

This paragraph is unclear as to the circumstances in which a service provider will be required to store information relating to the location of a device. The clumsy wording seems to have the intent of not requiring the retention of location data unless it is required for the provision of the service, according to the explanatory memorandum.[21] However, the Pirate Party considers this to be poor legislative drafting and recommends that this paragraph be revised.

9 Data retention plans

The requirement that data retention plans be kept confidential may make it difficult to tell how intrusive they actually are. A data retention plan could, it seems, go further than the legislation alone, in which case it is possible for it to be much more intrusive upon privacy. This is obviously concerning, and the Pirate Party does not believe there is sufficient justification for the confidentiality requirement.

10 Review period

The Pirate Party recommends that the review period in s 187N(1) be reduced to be 12 months after the implementation of the mandatory data retention regime, and every 12 months thereafter for at least five years. Given the domestic and international concerns raised regarding the appropriateness and efficacy of such a regime, it is appropriate to continuously monitor the successful use of the regime and any concerns relating to its abuse. Therefore it would be useful for the PJCIS to review the operation of the legislation annually for at least five years after implementation.

[21] Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 45.

11 Access to stored data

Access by the public

It is unclear whether provision will be made for subscribers and users to inspect or otherwise gain access to the retained data they and people using their accounts have generated. Under the *Privacy Act 1988* companies have a general obligation to allow individuals to inspect and correct personal data that they hold.[22] However, journalist Ben Grubb was (and appears to remain) engaged in a dispute with Telstra over a request for their personal telecommunications data.[23] This issue ought to be resolved, and preferably individuals would be permitted to inspect the records held.

Access by law enforcement and intelligence agencies

The European Union's Data Retention Directive was implemented in different ways across the EU's constituent countries. Although some countries (such as Hungary, Malta and the UK) had fairly minimal access restrictions for law enforcement and intelligence agencies, this was by no means the case for all countries. Most countries required judicial authorisation (or, in some countries, authorisation by a public prosecutor), and some countries — chiefly Denmark, Greece and Portugal — imposed strict conditions.[24]

In Denmark applications had to meet 'strict criteria on suspicion, necessity and proportionality', in Greece investigation by other means must have been 'impossible or extremely difficult', and in Portugal the condition was that access must have been 'crucial to uncover the truth or that evidence would be, in any other manner, impossible or very difficult to obtain.'[25] In Finland, subscriber data could be accessed without a warrant, but any further retained data required judicial authorisation.[26]

The Pirate Party requests that the PJCIS recommends the addition of provisions requiring strict regulation of access to retained data that includes:

- a requirement of a warrant or similar form of judicial authorisation, and
- robust criteria relating to suspicion, necessity and proportionality.

[22] *Privacy Act 1988* (Cth) sch 1 cl 6.

[23] Ben Grubb, 'Spies can access my metadata, so why can't I? My 15-month legal battle with Telstra', *The Sydney Morning Herald* (online), 10 October 2014 <http://www.smh.com.au/digital-life/consumer-security/spies-can-access-my-metadata-so-why-cant-i-my-15month-legal-battle-with-telstra-20141010-1146qo.html>.

[24] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (Report from the Commission to the Council and the European Parliament, European Commission, 2011) 10–12.

[25] Ibid 10, 12.

[26] Ibid 12.

The proposed s 110A(3) is concerning due to the discretionary power it confers to expand the number of agencies that are able to access the retained data. The Pirate Party considers this discretion to be far too broad, and believes that the power should instead be held by Parliament.

Access by private parties

A frequently asked questions (FAQ) page on the Attorney-General's Department's website includes:

> **Will data retention be used for copyright enforcement?**
>
> The *Telecommunications (Interception and Access) Act 1979* only allows access for limited purposes, such as criminal law enforcement matters. Breach of copyright is generally a civil law wrong. The proposed data retention regime does not change this in any way.[27]

This is somewhat disingenuous. It is conceivable, if not certain, that private parties would be able to subpoena service providers and gain access to records. The Attorney-General's Department did not actually answer the question it had asked itself: there is no guarantee that data retention will not be used for civil matters, and it probably will. This suggests that the flow-on consequences of the mandatory data retention regime have not seriously been considered, and would go beyond the intent of the proposed legislation.

Abuse of retained data

There have been reports of several questionable uses and transmissions of data in the past. In 2012 it was reported that Telstra had sent data it had collected from its subscribers overseas, including information that may have been able to identify some users.[28] The centralised collection and storage of subscriber data creates a demonstrably high-value target for state and non-state actors who wish to use or sell the retained data for nefarious purposes.[29] Communications providers themselves are not immune from questionable data use practices, as was demonstrated when T-Mobile admitted selling personal details to a third party.[30] This suggests that strict

[27] Attorney-General's Department, *Data retention*, <http://www.ag.gov.au/NationalSecurity/DataRetention/Pages/Frequentlyaskedquestions.aspx#RetentionCopyright>.

[28] Ben Grubb, 'Telstra accused of Next G web "stalking"', *The Sydney Morning Herald* (online), 5 July 2012 <http://www.smh.com.au/digital-life/mobiles/telstra-accused-of-next-g-web-stalking-20120705-21ivs.html>.

[29] Joel Falconer, 'Anonymous hacks Australian ISP AAPT to demonstrate data retention problems', *The Next Web* (online), 26 July 2012 <http://thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/>.

[30] Barry Collins, 'T-Mobile admits selling customers' mobile records', *PC Pro* (online), 17 November 2009 <http://www.pcpro.co.uk/news/353377/t-mobile-admits-selling-customers-mobile-records>.

requirements regarding the security and use of retained data are necessary, and must be in place *before* a data retention regime is even considered.

12 Costs

There is significant concern surrounding the financing of a data retention regime that needs to be considered. A study conducted prior to the widespread implementation of the European Union's Data Retention Directive estimated that setting up a system to retain data for 500,000 subscribers would cost €375,240 for the first year, and then €9,870 per month in operational costs, while a data retrieval system would cost €131,190 with operational costs of €28,960 per month.[31] In a UK Home Office impact assessment it was estimated that the cost of retaining IP addresses alone would be £26.6 million over the 10 years from 2014.[32]

13 Conclusion

Data retention and its use for mass surveillance is anathema to the basis of Australia's legal system: the presumption of innocence. Degrading the presumption of innocence not only diminishes the basis for gathering evidence, it also undermines the effect of that presumption throughout the entire legal system.

If the public consciously recognises that there is a debased presumption of innocence, the very effectiveness of our legal system will have been undermined.

Criminals (or potential criminals) have already mitigated any such surveillance through the use of encrypted, proxy and anonomysing services, thereby severely reducing the efficacy of data retention. Some criminals will be caught at the lower end of the scale, but they would have likely been caught anyway. Including everyone with a phone or Internet connection in a database of suspicion does not enhance civil and political relationships and responsibilities.

[31] European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)' (Report from the Commission to the Council and the European Parliament, European Commission, 2011) 26 citing Wilfried Gansterer and Michael Ilger, 'Data Retention — The EU Directive 2006/24/EC from a Technological Perspective', Wien: Verlag Medien und Recht, 2008.

[32] Home Office (United Kingdom), 'Counter Terrorism and Security Bill — Internet Protocol Address Resolution' (Impact Assessment, 28 October 2014) 2.

Ultimately this harms the bond of trust between the state and its citizens, leading to a suspicious, less-stable and defensive electorate. In *Smith v City of Artesia* the New Mexico Court of Appeal recognised that:

> Privacy is inherently personal. The right to privacy recognises the sovereignty of the individual.[33]

Indiscriminate data retention treats the individual as a suspect by putting them under what is effectively constant and permanent surveillance. Although tenuously touted as a necessity for preventing, detecting and prosecuting crime, the reality is that it intrudes upon the privacy of all subscribers, almost all of which will undoubtedly be innocent. Such intrusions into privacy must be proportionate: placing an entire nation under surveillance is hardly a proportionate response for such limited gains.

tl;dr:

[33] *Smith v City of Artesia*, 772 P 2d 373, 376 (NM Ct App, 1989).