Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

Review of the Integrated Public Number Database – April 2015 Report

Submission to the Department of Communications

June 2015

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public Inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably part of, a submission.

Introduction

This submission by the Australian Privacy Foundation (the APF) responds to the May 2015 report by the Department of Communications on the *Review of the Integrated Public Number Database* (the Report).

It follows two submissions that were made by the APF as part of the Review, in December 2011 and in July 2014 (the latter jointly with the Australian Communications Consumer Action Network (ACCAN) - both available online at https://www.privacy.org.au/Papers/indexPolicies.html#TelecommsIPND .

Overall Response

The APF welcomes recognition by the Department in the Report of the significance of privacy protection, consistent with findings by a range of authoritative independent inquiries and studies such as those by the Australian Law Reform Commission (ALRC), NSW Law Reform Commission, Victorian Law Reform Commission, Office of the Australian Information Commissioner (OAIC) and Australian Communications & Media Authority (ACMA).

That work demonstrates that –

- privacy is of concern to Australians, including people in demographics that are sometimes inaccurately characterised as indifferent to the privacy of themselves and third parties
- respect by business and government organisations for privacy fosters trust and engagement by consumers with those organisations
- Australian law at the Commonwealth and state/territory levels is failing to keep pace with emerging technologies such as the Cloud and practices such as the accelerating shift away from the POTS network
- there are substantive problems regarding regulatory incapacity on the part of particular agencies
- there is an expectation on the part of consumers that government entities such as ACMA and the Department will develop policy on a proactive rather than reactive basis.

Data supplied in the report and in other publications by the Department and ACMA demonstrates that Australians are embracing new communication technologies and services, evident for example in ACMA's estimate that 27 percent of the adult population relies on a mobile rather than fixed-line home phone. Overseas figures suggest that the shift from the fixed-line to mobile devices (including emerging multifunction devices rather than merely traditional mobile handsets) will continue.

The data further demonstrates that Australians from a wide range of demographics in metropolitan, regional and rural locations are actively choosing to protect their privacy by going ex-directory and by registering under the Do Not Call regime in order to minimise interference from unwanted callers. It is clear that many Australians consider that exemptions for calls by researchers are overly permissive and should be substantially reduced. That disquiet about exemptions is consistent with recognition that researchers have numerous opportunities to contact research subjects and that a more respectful approach to data collection is likely to result in robust data.

On that basis the APF strongly encourages adoption of global best practice both n privacy protection and in regulation and risk management in relation to the IPND. In particular the Department should resist assertions from vested interests that it is necessary to weaken privacy

protections relating to the IPND and thereby privilege those interests. Any such weakening would be contrary to the findings of inquiries noted above. It is also contrary to the intent of a range of legislation that includes the *Do Not Call Register Act 2006* (Cth) and the *Privacy Act 1988* (Cth). It would also be inconsistent with developments overseas, notably the strengthening of the European Union data protection and consumer protection frameworks that are a global benchmark for fostering economic development with due respect for privacy.

The Report notes the Department's consideration of industry compliance obligations and the management of the IPND database, currently undertaken by Telstra as a consequence of its privileged position prior to 1997. The APF urges the Department to heed recent competition policy reports, in particular that by the Harper Review, and adopt a pro-competition stance in regarding the IPND. That stance requires a preparedness on the part of the Department to critique claims by Telstra and claims by commercial researchers that feature in the Report.

The APF notes acknowledgement in the Report that

> 'there is little information about how Telstra determines access charges and handles its various roles as carrier, publisher of the White Pages® and IPND manager. There is also little or no current incentive for Telstra to update and refine the IPND over time, and some industry stakeholders have argued that the cost of interfacing with the IPND's legacy systems is significant.'

Privacy and competition policy objects are congruent. The APF encourages the Department to move without delay to separate IPND management from Telstra. Responsibility for the IPND should ultimately lie with the government, with any management contract awarded on the basis of a competitive tender rather than as a matter of legacy/incumbency. Telstra should be considered ineligible to tender because of its unavoidable conflicts of interest.

Management of a number of telecommunication databases (including the Australian Do Not Call and dot.au domain space registers) is undertaken competitively. Introduction of competition would also provide an opportunity to address concerns voiced by industry in the Report regarding cost and compatibility.

In moving towards competition the Department should embrace best practice, with a discernable and enforceable commitment to –

- transparency regarding policy-making and operation of the IPND
- progressing a pro-competitive arrangement for management of the IPND or equivalent
- consumer autonomy, consistent with other legislative regimes and featuring opt out from disclosure of non-critical uses
- robust reporting of data breaches.

Limited conception of privacy

We note that one of three 'high level strategic considerations' which informed the review was

> 'To protect the privacy of individuals through appropriate safeguards on use and disclosure' (Executive Summary)

While this is welcome, it unfortunately betrays a limited, but all too common, perception of privacy as being only about use and disclosure (and associated security). Given the acknowledged significance of the ALRC's 2008 Privacy Report as a source document, and given submissions made by ourselves and others, we would have expected much greater recognition of other statutory privacy principles and the underlying objective of privacy law to minimise intrusion into the affairs of individuals.

Greater recognition of this wider perspective would have led to greater attention to aspects of collection of personal information for the IPND, including questioning of the necessity and proportionality of collection in the first place, before issues of use and disclosure even arise. The limited conception of privacy is illustrated by the structure of the Report which has a separate section about 'Security and Privacy' when there are many privacy issues addressed in other sections.

There needs to be clear recognition of the fact that the IPND is a mandated breach of privacy principles – a compulsory collection and sharing of personal information which individuals would have some choices about under the normal operation of privacy principles. Recognition of this fact 'up-front' would provide a sounder basis for carefully questioning all claims for additions to, and use of IPND data.

Quality and Accuracy

The APF supports Recommendation 1 relating to data quality and accuracy, but also calls for some specific measures which the Report discusses (p.18) but on which it does not take a firm position. For instance:

- The IPND should be routinely 'washed' against the ACMA 'NUMB' database – we cannot see why there should be significant costs in an automated comparison, and in any case the cost should not stand in the way of increased accuracy, and efficiency of use, which all users seem to agree is desirable.
- Telstra should be required to routinely arrange for 'washing' of the IPND against the White Pages directory database. Indeed, we submit that if Telstra does not supply up to date White pages information it must be in breach of its data supply obligations under the IPND scheme.

Access by consumers

The Report notes that there are concerns on the part of stakeholders, including consumers, regarding the accuracy of information held on the IPND. The APF considers that accuracy will

increase, as will consumer understanding of (and hence respect for) the IPND if people are able to update/correct data about themselves.

That consumer engagement is wholly consistent with the *Privacy Act 1988* (Cth) and with expectations overseas. The Report does not sufficiently acknowledge the fact that Privacy Act access and correction rights already apply both to CSPs and to the IPND Manager. The industry has unfortunately been allowed to operate on the basis that the administrative arrangements for exchange of information between CSPs and the IPND Manager, and the provisions of the Industry Code relating to updating replace or 'trump' Privacy Act access and correction rights

The APF notes the recent Office of the Australian Information Commissioner decision regarding access by a consumer to that individual's metadata held by Telstra – which resisted compliance with APP 6. We understand that Telstra has appealed this decision but fully expect the AAT to uphold the individual's right of access. The APF considers that a more positive approach to consumer access to IPND data will be of benefit to the IPND manager, CSPs, law enforcement and emergency service agencies, and other agencies. Put simply, enabling consumers to 'fix' their data will also provide a 'public good'.

The APF therefore welcomes Recommendation 2 relating to individuals' access to and correction of information in the IPND relating to themselves (which we believe simply confirms the existing rights under the Privacy Act). All parties need to be clear that the issues of updating the IPND and of subject access/correction rights are separate, though related. CSPs and the IPND Manager need to be reminded of their Privacy Act obligations. The routine mechanisms for updating/correcting IPND data set out in the Industry Code might be one way of meeting these obligations (providing they meet the Privacy Act requirements) but are not an alternative.

The APF submits that the Telecommunications Act be amended to remove any uncertainty about consumer access and correction rights, confirming an obligation on CSPs to provide access to IPND source information, and on the IPND Manager to provide access to IPND data (which may or may not be the same).

The APF draws attention to the joint APF and ACCAN 2014 submission that noted the importance of strong identity verification processes, consistent with the Government's emphasis on an enhanced nation identity verification framework. The Report also notes endorsement of consumer access by Optus, an indication that consumer access is technically feasible and not contrary to business principles.

The APF also welcomes Recommendation 3 to increase consumer awareness of the IPND (which the Woollcott research showed to be very low). **CSPs should be strongly encouraged to assist consumers to understand the way in which the IPND works, including how to gain access to the information that they may want to check. This might require standard protocols overseen by ACMA.**

In relation to consumer awareness we also support the submission by ACCAN that the name of the IPND be changed to something that is more reflective of its actual nature – ACCAN has suggested 'The National Phone Number Registry'.

Uses of IPND data

Critical vs Non-critical – Users or Uses?

From a privacy perspective the APF suggests – consistent with the reports and laws noted above – that the Department, and Parliament, when considering the policy framework should adopt a different approach regarding critical and non-critical users.

A distinction between critical and non-critical is helpful insofar as it raises the bar for access for secondary purposes, but we question the way in which the distinction has been applied.

The report focuses on 'critical *users*' of the IPND. **IPND policy should instead focus on critical *uses*. Users and uses are not synonymous** – for example all critical users have routine administrative functions for which IPND access would be both unnecessary and inappropriate.

An emphasis on uses rather than users – including in the wording of the legislation and related instruments, would foster legislative clarity and facilitate achievement of the objects underlying the Department's nine recommendations. Not all uses of IPND data are necessary, proportionate and appropriate, irrespective of which entity is seeking access or wishes to use IPND data for public interest, commercial or other purposes.

This matter is discussed further below.

Critical Users/Uses

The APF is broadly satisfied with the Report's assessment of critical uses – subject to the criticism above that the focus, and terminology, should be on uses rather than users.

There are sound public interest justifications for access to the limited current IPND information for the three categories of critical use.

The Report suggests that access rules should be more widely known (p.29) but this is not followed up with a recommendation. **The APF submits that there must be public reporting of the access rules and criteria for critical uses of IPND data.**

The Report discusses the definition of 'enforcement agency' but makes no recommendation. **The APF supports the implicit conclusion that the legislation be amended to ensure consistent definition of enforcement agency.**

Non-critical Users/Uses

Unlisted numbers

The Report correctly identifies the importance of the choices that are available to CSP customers. There seems to be a consensus that IPND data provided for non-critical uses should exclude unlisted numbers which are an expression of customers' preferences about how their personal information should be used. (The APF accepts that the public interest in the critical uses outweighs the application of those preferences for those users who qualify).

The APF agrees that the level of awareness of opt-out choices is unsatisfactory. But the Report does not follow through on its analysis with recommendations for greater obligations on CSPs, and the IPND Manager, to promote awareness of unlisted number options and their implications. We submit that some CSPs would appear to be in breach of their obligations both under the IPND regime and under the Privacy Act to explain the way in which personal information is used and disclosed and the control that customers can exercise by seeking unlisted numbers.

Whether or not a system of opt-out by categories of use is practicable – the Report concludes not but we submit that it should be – **there is no excuse for the Report not at least recommend that all CSPs clearly explain and offer at least a single and simple unlisted number option**.

The Report notes Telstra's contention that:

> 'while subscribers should be able to change their listing preference in the IPND for free, this should be 'independent from requests for unlisted numbers for the purposes of the White Pages® or CLI'.

The APF submits that this is a nonsensical self-interested proposition that should be rejected. Telstra's charging of a fee for its 'silent line' product is unconscionable and the 2008 ALRC Privacy Report agreed and recommended that it be prohibited (Recommendation 72-17).

Telstra should be prevented from playing games with a semantic distinction between unlisted number status and 'silent lines'. The policy objective is clear – that customers should have the option, free of charge, to not have their telephone number used for (in IPND language) 'non-critical purposes', and exercise of this choice must also flow through seamlessly to the IPND itself. **The APF submits that the Department should take this opportunity to implement the longstanding recommendation of previous reports to make unlisted number/silent line status a right free of any charges, across all directory services and products.**

The Report gives three reasons on p.35 for not applying an opt-out regime to Telstra's White pages and other directory products. None of these, in the APF's view, stand up to even cursory analysis. **Any opt-out regime must apply to all public directory products, including Telstra's White Pages – whether or not they are sourced from IPND data.**

Relationship to the Do Not Call Register

The Report discusses the Do-not-call (DNC) Register (pp.40 & 46-47) but fails to make any recommendation. **We can see no good reason why the IPND should not be used to 'clean' the DNC Register (which now has 'indefinite' registrations), and any impediment to this in the IPND regime should be removed. Conversely, the APF submits that a minimum measure to respect individuals' preferences should be the automatic 'washing' of any information made available from the IPND for non-critical uses involving contact with consumers against the DNC Register**.

Public Interest Tests for non-critical uses

In introducing discussion of additional users/uses, the Report asserts that 'The IPND must innovate and keep pace with technological and market changes if it is going to continue to be a valuable data source that serves the public interest.' (p.40). This is implicitly used as a foundation for canvassing a wider range of users/uses.

The APF has no problem with the assertion but rejects any automatic assumption that 'innovation' and 'keeping pace' necessarily implies or justifies widening the number and type of permitted users/uses. Similarly, Recommendation 4 refers to a broadening of access for a "wider range of researchers". **There should be no automatic presumption that a wider range or larger number of researchers (or other non-critical users seeking access for other purposes) will be able to meet the applicable public interest test.**

The APF rejects the finding on p.48 of the Report that:

> 'the public benefit in providing access to data (either at the aggregate or individual level) *[to non-critical users]* significantly outweighs the public benefit in protecting the privacy of individuals.

This is merely an assertion/opinion unsupported by empirical evidence.

It is imperative that any widening of access should be transparent (i.e. there should be a clear, readily accessible notification that extension of access to a specific research body is proposed and has taken place). That transparency is a basis for best practice accountability regarding policy for and management of the IPND. Transparency is an appropriate cost under Australian telecommunications and competition law rather than a unique or onerous regulatory burden.

It is also imperative that any widening should be principles-based rather than merely on a 'case by case' basis. The principles centre on satisfaction of a transparent and robust public interest test that involves the decision-maker being able to demonstrate that there is a compelling public good. Public good is *not* the same as bureaucratic convenience (researchers should be reasonably expected to use alternate means of data collection/subject identification) and is independent of the researcher's status (i.e. the mere fact that a researcher is employed by/for a particular public sector agency should be insufficient grounds for authorisation).

In determining public interest the Department (in policy setting) and ACMA (in practice) should assess requests for access to IPND data in terms of the purpose of the proposed use, rather than the status of the entity seeking access; and also assess whether the outcome is proportionate (i.e. there is a clear public benefit that offsets the erosion of privacy).

The Report (and its Recommendation 4) appear to have been unduly influenced by the 'ambit claim' from the Research Industry Council of Australia (RICA) (replicated in detail on pp. 42-44 of the Report). We are disappointed that the Department has not taken on board the distinction made in our joint submission with ACCAN in 2014 between two types of research. We suggested that access to the IPND for research purposes that involved only aggregate analysis raised far fewer privacy concerns than research that involved contact with individuals. Acceptance of this distinction would, we suggest, have provided at least a partial solution to the issue of research access.

Access by researchers should be subject to a rigorous and independent privacy impact assessment. Importantly, PIA reports should be subject to review by ACMA, and should be published, both of which would address concerns within government, business and civil society bodies that the quality of some PIAs conducted to date is suboptimal.

The above comments are consistent with ALRC recommendation 72-14. They are also consistent with actual use of the IPND for research purposes. The APF and other bodies have highlighted that researchers have an increasingly broad range of options for contacting research subjects other than the IPND and that their engagement with research subjects is most productive when Australians perceive that the researchers treat them with respect.

Reports for ACMA and the Department over the past decade demonstrate that many people have chosen to go 'ex-directory' (despite the imposition of an unjustifiable fee by most CSPs) – and further to abandon traditional fixed-line telephony services – as a way of minimising unwelcome intrusion by researchers. That is consistent with the Do Not Call regime, which has a statutory basis. It reflects privacy as a legitimate freedom from interference.

Access by non-critical users

The report notes "a growing level of interest" on the part of "non-critical users" in accessing the IPND and "a wider range of information than is currently available", i.e. an enhancement of the IPND through inclusion of additional information.

The APF considers that interest is unsurprising, given that different entities can envisage uses for the existing IPND or for data that might be included in and accessed from the IPND. That interest is not synonymous with public good and should accordingly be subject to rigorous appraisal by the Department in accord with earlier comments.

The Report does not provide a compelling rationale for extending access by non-critical users. The APF suggests that the Department in considering claims of a public benefit that outweighs the public interest in non-interference should differentiate between users and uses. Access should be on the basis of demonstrable public benefit rather than the size, corporate structure, industry or other attribute of the user.

The ALRC review of privacy laws recommended amendment of the Telecommunications Act to clarify when a use or disclosure of information or a document held on the IPND is permitted. The ALRC did **not** consider every proposed disclosure to be appropriate and for example noted concerns that access is being used for political canvassing. It also recognised that demarcations between commercial and non-commercial research are blurring, through for example partnering between research institutions and commercial entities in the health sector.

The APF endorses moves to clarify use/disclosure, founded on disclosure being in the public interest (see preceding comments regarding proportionality) and – if disclosure involves non-critical uses – subscriber consent. That consent might be signalled by a code (which could be built into the new system referred to above) and through provision for consumers to wholly opt out of non-critical uses.

The APF notes, consistent with studies by ACMA and the Department (and with independent research in comparable jurisdictions), that an increasing number of consumers are acting to minimise inappropriate interference. Those people may respect the IPND as a base for the provision of emergency services (and law enforcement). However they do not consider that data about themselves should be automatically accessible for non-critical uses/users.

If access to the IPND for non-critical uses is widened consumers should be provided with an effective mechanism to enable them to opt out. The reference to 'effective' is deliberate, given the difficulty evident in accessing/correcting IPND data, which the Report acknowledges is significantly easier to do in theory than in practice. In the absence of a compelling reason for mandatory coverage any consumer should be able to opt-out of access by non-critical users. The Report has not provided a strong rationale (as distinct from what amounts to self-interest on the part of commercial entities) for access for non-critical uses. As noted in the submission annexed to this document

> The IPND is essentially 'marketed' to the public as an emergency database – consumers are encouraged to provide correct and current information to their CSP specifically so that they can be found in an emergency…. Consumers should be able to opt out of having their IPND information accessed by non-critical users on a category by category basis.

We refer to our discussion of unlisted numbers above. The Department should question the opposition by Telstra to "altering the approach to unlisted numbers", an opposition that is not shared by all CSPs and appears to reflect Telstra's commercial priorities rather than a legitimate public interest.

Ongoing/Periodic Access

Recommendation 5 (p.63) is for the ACMA to be able to approve ongoing or periodic access for non-critical user applicants, provided that the ACMA regularly reviews access and that a privacy impact assessment is completed. This recommendation is unhelpfully detached from the relevant analysis and findings on p 48. **The APF is not opposed in principle to 'standing authorisations' for some non-critical uses, subject to the recommended conditions** (which is consistent with practice in other areas (e.g. review by the Australian Competition & Consumer

Commission of each edition of the Medicines Australia Code as a condition of approving that Code).

It is however imperative that any such review by ACMA should be transparent (e.g. public notice that a review is underway, with adequate opportunity for public comment, and reporting of that review, and including publication of any privacy impact assessment in time for it to inform submissions). It is also imperative in establishing best practice that ACMA engages in a substantive rather than merely nominal review. Put simply, ACMA must do more than 'tick a box' that a privacy impact assessment has been completed; in conducting reviews it must consider whether the assessment was thorough and adequate.

Unlimited Displays of search results

Recommendation 6 refers to ACMA being authorised to approve display of "unlimited numbers of entries from the IPND if appropriate 'anti-scraping' measures are in place".

The APF considers that there is no compelling public interest to justify weakening of the current regime and that the recommendation should not be embraced unless there is an authoritative independent publicly-accessible advice regarding the effectiveness of anti-scraping measures. The Department should be sceptical about claims by particular commercial entities regarding their needs or the efficacy of solutions.

Additional data

The APF submits that the Department should resist appeals for additional data to be collected and held in the IPND.

In particular, the suggestion by one interested party that other data fields should be added for use in credit reporting and AML-CTF identity verification checks (p.49) should be rejected as an ambit claim unrelated to the public interest purpose of the IPND. Similarly, the discussion of date of birth information on p.54 is a clear ambit claim – and besides the acknowledgment of the potential costs and practicalities, there should be a clear recognition that it would raise significant privacy issues. In contrast, the Report appropriately defers further consideration of adding 'type of service' information to the longer term review of a new system.

The 'gap analysis' of critical users' needs in the table on pp.51-52 of the Report is interesting, but is only relevant to the longer term review of a new system flagged in Recommendation 9 (see below).

If and when these issues are considered, and in the context of the mention of IP addresses and service information in the table, it is essential that the relationship of the IPND to the new mandatory telecommunications data retention scheme is considered in detail.

Policy Transparency

The APF strongly endorses Recommendation 7, i.e. that "ACMA should publish information about applications and decisions made under the IPND Scheme".

Timely and readily accessible publication is productive of informed policy-making (for example as a basis for advice from business and civil society entities) and of the accountability that all Australians expect of government.

As importantly, it will go some way to alleviating what the Report acknowledges is lack of awareness and uncertainty about both the IPND per se and about the specifics of its management.

Publication is an appropriate measure and is wholly consistent with recommendations in a range of reviews, for example the Harper Review on competition policy.

IPND operator

Preceding paragraphs have noted that Telstra has a privileged position through its legacy as the dominant telecommunications provider prior to 1997, and still now the dominant landline provider. From a competition policy and privacy perspective it is highly appropriate that Telstra's current management of the IPND be more open to public scrutiny in the immediate future and that as soon as possible, management of the IPND be open to competition.

The APF accordingly supports Recommendation 8 that calls for Telstra to make available the measures it takes to separate its role as part-owner of the publisher of the White Pages® and the manager of the IPND, its standard form of agreement with data users and its annual audited financial reports for the IPND.

In endorsing that recommendation the APF considers that the information should be readily and publicly available, i.e. should not be restricted to ACMA or Department staff. It is appropriate to consider the IPND as a public resource rather than a proprietary database.

In relation to Telstra as the IPND Manager, the report implicitly accepts that Telstra can continue to perform this role pending development of a replacement system (see below). Given that development and implementation of any new system will inevitably take years, **the APF does not see this as a reason to put off terminating Telstra's contract and putting IPND Management out to competitive tender from entities without a direct conflict of interest.**

Transition to a new system

The report recognises that there is support for transition to a new system, reflecting changing patterns in consumer use of telecommunications, but also acknowledges significant privacy concerns. **We therefore welcome the Review's conclusion (embedded in Recommendation 9) that consideration of moving to a dynamic system should be deferred, at least until after completion of the Triple Zero review.**

The APF encourages the Department to conduct a rigorous and public investigation of any proposed new system. That review should involve civil society and other consumer stakeholders, recognise changing consumer and other practices, and be respectful of recommendations in a range of authoritative studies of the Australian privacy regime.

The APF disagrees with provisional suggestions that the IPND or equivalent should contain other personal information, such as the subscriber's birth date. There has been no substantive evidence that inclusion of the date will significantly assist law enforcement or emergency services; in many emergency situations a caller may not be the registered subscriber and indeed may be unaware of the subscriber's age. **The APF suggests that the Department should differentiate between data that is functionally important and data that is merely commercially interesting or convenient**.

Additional protection - Data breach notification

Australia appears to be slowly emulating practice in other jurisdictions that have statute-based mandatory reporting of data breaches. Such reporting has received strong industry, consumer and legislative support overseas. It has not, contrary to some self-interested claims, served to inhibit innovation or place an onerous burden on commercial enterprises and public sector entities.

The IPND is governed under the national telecommunications regime, which does not provide for timely and clear public reporting about IPND breaches. ACMA has responded to a succession of data breaches involving major CSPs in a way that is stronger, more visible and significantly more timely than that by the Office of the Australian Information Commissioner, which has limited its involvement to encouragement of voluntary reporting. ACMA's performance in this area is consistent with that of peers such as the Federal Trade Commission and Federal Communications Commission in the US. But we submit that it is desirable to move to another level.

The Report sees merit in data breach reporting (p.37) but makes no recommendation. **The APF submits that the IPND should be subject to mandatory data breach reporting**. That reporting should be public rather than restricted to a disclosure to ACMA, the OAIC and/or the Department. In other words, individual consumers should be alerted if their subscriber information is disclosed on an unauthorised basis, given that consumers have no choice regarding the IPND and that the legitimacy of the IPND is founded on its value in facilitating law enforcement and emergency service provision.

For further information please contact: Nigel Waters 0407 230 342 nigel@watersofthebay.com
Australian Privacy Foundation APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.