Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

18 November 2016

Public Data Branch

Department of Prime Minister and Cabinet

PO Box 6500, Canberra, ACT, 2600

By email: ogp@pmc.gov.au

RE: Open Government National Action Plan

General comments

The Australian Privacy Foundation (APF) notes the release of a draft Open Government National Action Plan for public consultation. The APF is strongly supportive of open government and transparency, including appropriate forms of FoI, and 'open data' initiatives, when there are sufficient assurances that no data released into open data collections is, or is able to be, associated with an individual. Indeed, if a robust, open audit of the risk of re-identification is done prior to release, there will no doubt be many types of data sets which were not derived from personal information which may be relatively safe to use for 'open data', and which generate the sort of net benefits hoped for by enthusiastic proponents.

However, advances in 'big data' techniques, data matching and data linking increase the ability to identify individuals from seemingly anonymous or weakly de-identified data sets derived from personal information or records about individuals. These technologies can find matching attributes in other identified and anonymous data sets in order to ascribe identity to the de-identified data.

For example, a Stanford University computer science program titled 'Footprints' claims an 80% success rate for identifying individuals from Twitter data including who they follow and what websites they access from Twitter. More recently, Riziou and colleagues at Australia's NICTA analysed the continuing erosion of 'privacy protection' (erosion of effective de-identification) in over 100 million Wikipedia edits using only the broadest subject categories. The recent risk and identification literature (which does not appear to have been fully considered by the Plan) confirms this is a growing feature of large data sets and advanced analytics.

A more specific example is the recent proliferation of claims that Statistical Linkage Keys (SLKs), which are designed to link records of particular individuals, are somehow not 'personal information', do not raise privacy issues, or are an effective form of de-identification. These claims are not a good basis for trust in either linkage or release programs, since they fail to explore the growing weakness of these methods to secure long term protection against re-identification.

We believe the Draft Open Government National Action Plan may not adequately acknowledge or mitigate these risks, and that privacy and personal information security concerns from potential data linkage or unprotected publication should be identified more fully throughout the document such as to be considered before data is released. Individuals as data subjects remain exposed to the risks of re-identification, and subsequent abuses or unexpected uses, for an indefinite period into the future. (Riziou et al suggest that privacy risk increases into the future even after a data subject withdraws from the data-generating activity.) It seems a fundamental omission for the Plan to neither acknowledge, analyse nor propose remedies for these risks applying to a sensitive sub-set of potential 'open data' or linkable sources.

In addition, there appears to be no proposal to require ongoing future audits, checks or technical inquiries to determine if and when a given data set's security has been breached, whether by government, business, criminals or actors in other jurisdictions; nor to share the responsibility for such unintended consequences – it seems the data subject will bear the burden of both discovering and mitigating the effects of future such breaches alone, even though they may have no say in the release nor share in the benefits.

To address the potentially inevitable failure of the re-identification protection in some data sets, the government has proposed a new criminal offence, presumably to be investigated at the discretion of the AFP and prosecuted at the discretion of the DPP. It is not clear to us that the Privacy Amendment (Re-identification Offence) Bill 2016 will address these concerns. The introduction of an offence against re-identification of data released by government agencies may be effective to discourage certain entities from engaging in re-identification, but it offers significantly less protection than ensuring all data is released is subject to a full future risk audit and the most stringent de-identification processes, backed up by a right of data subjects to sue those responsible in the event of serious harm from the future re-identification of the released data. Released data may have substantial value to nefarious actors, or those in other jurisdictions, for both of whom the existence of the offence would be little or no discouragement.

In our opinion the text of the draft action plan should also draw closer attention to issues of data linking and re-identification as well as propose mechanisms for pre- and post-release audit (to identify those data sets which would not fit into a category of 'safe enough to release into the wild forever', and to identify those released data sets which have been breached after release, so as to warn data subjects of the need to consider personal action in mitigation of the discovered risk), checking and ongoing training about advances in de-identification and re-identification technologies. This would encourage greater consideration of privacy issues and the risk of privacy breaches when data is released.

We welcome the proposals to work with the OAIC to improve privacy risk management across the Australian Public Service, and believe more clarity is required in terms of training government agencies and entities. However, given the continuing overload of the OAIC and their closeness to agencies, it is important to consider involvement of outside stakeholders, and other entities like the

Australian National Audit Office, both pre-release and post-release, in assessing the safety of each data set prior to release, and in holding publishers responsible when and if the de-identification protection is breached in future and data subjects are exposed to unexpected data harm.

Recent examples such as the repeated data breaches and security flaws in the existing MyGov platform, the almost instant de-identification breach of the 10% Medicare data set, and the similar breach of the ABS internal workforce data set all suggest that 'data integration' and 'open data' (unprotected publication) risks require careful consideration in the development of 'digital' government services.

If these issues are not addressed adequately up front, there is a risk of growing loss of trust and confidence in the capacity of the agencies and the government to exercise their data custodian roles fairly, and to explore the new data opportunities in ways which do not turn certain data sets into future 'toxic assets' (as Schneier calls them), a liability for both the releasing agency and the affected data subjects.

Commitment 1.2 re Beneficial Ownership Register

We support this action, provided it is limited to beneficial ownership of legal entities. Such a register should be available to the public, not just competent authorities – those accepting the benefits/protections of incorporation have to accept a loss of financial privacy (privacy rights under Australian laws do not and should not apply to legal entities other than natural persons).

Question arises as to whether the register will leverage existing requirements under AML-CTF legislation for reporting entities to record beneficial owners of all bank accounts (including those belonging to individuals). Notwithstanding the potential for unscrupulous individuals to 'hide' corporate activities, it is an important to uphold the current position that individual's financial affairs are NOT routinely made public or any further erosion of financial privacy of individuals.

The Privacy Commissioner should be identified as a relevant actor for this commitment.

Commitment 2.2 re public trust in data sharing

Public trust in data sharing is a key part of any open government plan. Privacy is about ensuring that individuals have control over their personal information. Trust will be destroyed when there is no transparency (and consent if personal information) with sharing information. The plan clearly recognises the privacy issue which is good but relies on assumptions about the adequacy of privacy protection in Australia. The privacy protections and regulatory oversight in Australia are inadequate by best practice world standards and this needs to be addressed to build trust.

The Australian Bureau of Statistics has been identified as a lead agency when it is the subject of an enquiry following the Census 2016 debacle. The ABS did a Privacy Impact Assessment for the Census that was completely inadequate and did not comply with the OAIC guideline. We contend that in these circumstances, the ABS would undermine trust further as a lead agency.

The other actors involved from non-government needs to include privacy advocates.

Milestone 4 – improving privacy risk management capability is very important. It is noted that this is an area where Government needs to improve significantly. A common problem is Privacy Impact Assessments being done poorly, without consultation, not released or not done at all.

Commitment 3.1- modernise Information Access laws

We support this objective provided it doesn't swing the balance away from privacy protection where personal information is concerned, other than where it is used as an excuse for withholding 'business information'.

The FOI Act was undermined in 1988 when the concept of 'personal affairs' as a reason for withholding was replaced with 'personal information' to align with the then new Privacy Act. This allowed agencies to withhold information because it included anodyne information about public servants carrying out their functions which should be publicly available for accountability.

There is a wider problem with the FOI Act including two regimes with different objectives – access to and correction of one's own personal information (which should logically sit solely in the Privacy Act) vs access to information about the workings of government (transparency and accountability) which should be the primary focus of the FOI Act, and where reasons for withholding should be trimmed back including spurious claims of privacy for public servants in the performance of their duties.

There is an urgent need to counter a disturbing continuing persistence by even some senior public servants to see FOI laws as incompatible with good governance and an impediment to 'frank and fearless' advice. There also needs to be reversal of recent cuts to the resources and constraints on independence of the Information Commissioner. The welcome advances in the 2010 FOI Act amendments have lasted barely five years before being undermined. To be effective (a fundamental objective of the OGP), FOI laws need a well resourced 'champion' with guaranteed independence.

Harmonisation of privacy and FOI laws across all Australian jurisdictions (by levelling to highest common standards) should be a high priority – current inconsistencies are a major impediment to a clear public understanding of the laws, rights and obligations, and all too often lead to spurious claims that privacy prevents uses and disclosures of information which is clearly in the public interest. Commitment 3.2 already addresses monitoring of information access laws across all jurisdictions, and COAG processes should also be used to advance the cause of harmonisation of information laws, and we understand that the OGP has a project on sub-national jurisdictions. We understand that Information Commissioners from a number of Australian jurisdictions are currently engaged in an inventory/review which could inform OGP work in this area.

The Commonwealth Attorney-General's Department is arguably conflicted in having responsibility for information laws as well as for national security and law enforcement – the interests of which will always prevail over human rights considerations where there is a tension. Consideration should be given to moving responsibility for information laws to a more 'neutral' department or agency which could be a more enthusiastic champion of such rights.

Commitment 4.2 - improving integrity

Current calls from across the political spectrum for a 'federal ICAC' need to be recognised with the case for a new body at least on the table for discussion. Agencies such as the ACLEI, AFPs, FACC, ASIC etc all have an important role but it should not be assumed that they will be able between them to adequately address all the challenges faced in ensuring integrity and combatting corruption in both the public sector and the corporate world

Commitment 5.1 – consultation and engagement

We strongly support the multi-stakeholder approach, and welcome the opportunities for early engagement to date. We would like to see privacy interests expressly included in stakeholder consultation arrangements – obvious candidates for inclusion are APF, EFA and Councils for Civil Liberties. Also, while Transparency International will not generally hold a privacy brief, we are surprised that it does not appear in any of the lists of OGP stakeholders we have seen.

We are very alarmed to hear that ACMA has de-registered the Calling Number Display (CND) Code effective 13 October 2016. Some interested parties were only advised 'after the event' by letter dated 21 October, thereby denying anyone the opportunity to make last minute submissions to prevent this extremely damaging decision.

Relaxation of the binding requirements to notify consumers about CND, its privacy implications and protective measures will mean that thousands of people whose safety could be at risk from disclosure of their telephone number may no longer receive the information that they need in order to safeguard themselves. Those placed at potential risk include victims of domestic violence, women's refuges, family law lawyers, psychiatrists, and people involved in disputes of any kind. Moreover, there is no longer any guarantee that telecommunications service providers will continue to provide consumers with the tools they need to block transmission of CND information, which can be a vital safety measure.

We call for immediate steps to re-introduce binding requirements relating to provision of CND services.

The entire process leading to this de-registration, initiated by Communications Alliance in 2015, has been largely opaque, with no consultation with interested parties other than ACCAN, the Privacy Commissioner and the TIO. These parties have made their objections to de-registration very clear – on the basis that the Code contains binding requirements that are not replicated either in the Privacy Act or in the TCP Code.

Privacy advocates were closely involved in the development by the Australian Communications Industry Forum (ACIF) of the original CND Code (C522: 2000) and subsequent amendments, and have consistently had to defend the rights of telecommunications customers to be made aware of CND and its implications against industry attempts to weaken the requirements.

In early 2015, Communications Alliance, the successor to ACIF, commenced a process to unilaterally 'downgrade' the CND Code to a non-binding Guideline. They had to be reminded that de-

registration of the Code by the ACMA would be a pre-requisite, and in July 2015 deferred the process of developing a Guideline.

In May 2016 Communications Alliance indicated to ACCAN that it was proceeding with development of a Guideline and was applying to ACMA to de-register the Code.
Ever since Communications Alliance replaced the former Australian Communications Industry Forum (ACIF) in 2006 direct consultation ceased with the APF and other public interest groups, leaving ACCAN (formerly CTN) as the only 'consumer' organisation to be routinely consulted by CA. Because of CA's unwillingness to engage directly with APF and other public interest groups, privacy advocates have had to rely on ACCAN as the only channel by which concerns could be raised.

In a letter to ACMA dated 13 July 2016, ACCAN re-iterated serious concerns already raised in its 2015 submission, and we understand that the Privacy Commissioner and the Telecommunications Industry Ombudsman (TIO) have also repeated their 2015 concerns.

The ACMA letter of 21 October lists three 'considerations' it must take into account in Code registration/de-registration decisions – these go to the process and content of consultation.
Despite the first consideration being public consultation, the ACMA does not address it – had it done so it would have been clear that there has been no effective 'public' consultation on the proposed de-registration – only belated, limited and sporadic consultation with ACCAN.

We note that The Telecommunications Act 1997 does not require consultation for deregistration (s.122A) in the way that it does for registration (s.117) – this is an unfortunate anomaly that should be rectified by legislative amendment. Notwithstanding the lack of a requirement, we note that CA did consult with a selected number of interested parties (the OAIC, TIO and ACCAN), but not with other 'known' interested parties or the general public.

The ACMA letter claims that it has given careful consideration to concerns raised by ACCAN, the Privacy Commissioner and the TIO, but effectively dismisses them without any argument or justification. After its own 'desktop research' (no details given) and consultation with CA, the ACMA appears to have concluded that the concerns are either unfounded (but no explanation given) or that they can be satisfied by monitoring of de-regulated CND practices by CA and ACMA (this is however time limited to 12-18 months). It is suggested that 'in the event that problems are identified', provisions could be included in other Codes.

Leaving aside the very real prospect of safety risks to consumers while the new regime is being 'monitored' the ACMA appears to have completely overlooked the importance of the mandatory awareness provisions of the Code, which will become purely advisory in a Guideline.

The ACMA appears to place great faith in the provision of easy means of CND blocking continuing on a voluntary basis, and on voluntary provision of information. CA's undertaking to:

> 'Develop information materials targeting consumers in vulnerable circumstances, to engage with relevant consumer bodies to develop these materials, and to circulate them among relevant parties'

together with the residual *recommendations* in section 4 of the Guideline, is in our view not an adequate substitute for the *requirements* for provision of information to customers in the now de-registered Code (section 4).

In summary, we strongly object to the removal of important privacy safeguards through a flawed process, without adequate consultation, and in flagrant disregard for the significant concerns expressed by ACCAN, the Privacy Commissioner and the TIO.

The safeguards in the former Code must be re-introduced without delay, either by re-registration of the Code or in other binding instruments. In the absence of these safeguards, there is a very real risk of telecommunications customers, particularly vulnerable consumers, being harmed by the unintended disclosure of telephone numbers.

Concluding remarks

In closing, we look forward to working with the branch to identify the sorts of protections that would be necessary to avoid the risk of future problems with this new direction for government, including by identifying the sorts of data sets too unsafe to release, the clear problems with de-identification strategies that expose people to unexpected future re-identification, and the sort of remedies that would ensure that those impacted by such future breaches are notified and not left to suffer the consequences alone and without support. When these aspects are resolved, the Plan will be ready for implementation, and the rewards from the new data activities will not be compromised by projecting unwelcome risk onto data subjects.

If you have any questions please do not hesitate to contact the writer.

Yours sincerely

Kat Lane,
Chair
Australian Privacy
Foundation
P: 0447 620 694
Kat.Lane@privacy.org.au