High level principles informing policy on the use of Big Data analytics by national security and law enforcement agencies

Comments from Australian Privacy Foundation (APF)

Overview

These invited comments are directed to the draft high level principles relating to the use of Big Data analytics by national security and law enforcement agencies and produced by the Law and Policy Program of the Data to Decisions Cooperative Research Centre (D2DCRC). While grateful for the opportunity to provide comments, in doing so the APF wants to make it clear that we do not endorse the principles as drafted and we do not give permission for our name to be used in publicly promoting the principles in any way, shape or form. We will explain the reasons for our strong reservations.

Fundamental objections to high level principles

The APF has fundamental objections to both the way in which the project of formulating principles is conceived and executed. The APF is especially concerned that the draft principles have the potential to legitimise highly privacy-invasive practices by Australian national security and law enforcement agencies (NSLEs). In particular, the APF is concerned that the principles, as drafted, could legitimise mass, dragnet collection, storage and use of highly revelatory data and metadata, without proper procedural safeguards, and in breach of the fundamental rights to privacy and data privacy.

The objectives of the draft principles are said to include informing policy to support assessments of the existing regulatory framework, but do not envisage a new regulatory framework. The APF considers that the existing legal framework relating to the collection and use of data by security and law enforcement agencies, including but not confined to the *Telecommunications (Interception and Access) Act 1979* (Cth) and *Privacy Act 1988* (Cth), is manifestly inadequate for the protection of privacy of Australians. Unless the serious deficiencies in the legal framework, including the lack of protection of fundamental rights, are acknowledged and remedied, a set of principles such as those proposed is likely to do no more than legitimise highly privacy-invasive practices, which are effectively sanctioned by the weak legal framework. It is therefore completely artificial to separate the formulation of principles from analysis of the adequacy of the regulatory framework.

Secondly, the principles are drafted at such a high level of generality, and include wording that is so flexible or ambiguous, that they would seem to be capable of justifying almost any practice, including highly privacy-intrusive practices. For example, draft Principle A states that:

> *Big Data analytics involving personal information should only be employed when reasonably necessary to achieve defined NSLE objectives.*

Given the ambiguity and flexibility in what is meant by 'reasonably necessary', not to mention uncertainty concerning the meaning of 'personal data' (in the Big Data context) and 'NSLE objectives', it is almost impossible to ascribe any practical content to this principle. Moreover, the breadth of the proposed definition (or description) of 'Big Data analytics', suggests that this principle might be used to justify almost any practice. At a minimum, there is a need for the meaning of all principles to be spelt out in more detail, potentially involving practical examples. Without this there is very little scope for informed assessment of the principles as, in effect, there is nothing (or very little) to analyse.

Particular issues

This section of our comments briefly addresses some of the most important specific weaknesses we have identified with the draft principles.

Proportionality

Principle B states that:

> *Proportionality must inform and guide the design, operation and management of all elements of the information lifecycle.*

The APF agrees that the proportionality principle must be applied to ensure the legitimacy of data processing. But we have two objections to how this principle appears in the draft principles.

First, the principle should state not simply that proportionality should 'inform and guide', but that any application of Big Data analytics to the information lifecycle MUST be proportionate. The principle should therefore read more like the following:

> *The application of Big Data analytics to the information lifecycle, or to any element of the information lifecycle, must in all cases be proportionate.*

Secondly, there are problems with the way in which the proportionality principle is described or explained in the draft paper. As is abundantly clear from European human rights jurisprudence, including the judgment of the European Court of Justice in *Digital Rights Ireland Ltd v Minister for Communications,*[1] the proportionality principle must be 'strictly' applied whenever the rights to privacy and data privacy are implicated. Moreover, according to the European jurisprudence, the mass, unconstrained collection and analysis of data and metadata can never be proportionate, especially where there are inadequate procedural safeguards, such as prior approval by a lawful authority, such as a court. As referred to above, the APF believes that the procedural safeguards in the Australian regulatory regime are manifestly inadequate.

A further problem with the explanation of the principle is how it deals with the objectives or purposes of relevant data processing, which are expressed in terms of 'statutory purpose'. In line with accepted understanding of international human rights law, not just any statutory purpose is acceptable as a starting point for the proportionality principle: the purpose must be a 'legitimate purpose'. In other words, it is important that, in properly applying the proportionality principle, some normative assessment of the relevant legislation is undertaken. This goes back to one of our main points; which is that it is mistaken simply to accept the existing regulatory regime as a given.

Finally, although the explanation does refer to civil liberties including privacy, we believe that it fails to sufficiently emphasise the importance of protecting the rights to privacy and data privacy. We would therefore recommend adding something like the following to the explanation: "In applying the proportionality principle, particular emphasis should be given to the rights to privacy and data privacy".

In summary, then, the APF submits that:

- The principles should be redrafted to make it clear that mass, undifferentiated collection and processing of data and/or metadata can never be proportionate.
- The principles should incorporate a principle relating to procedural safeguards, which makes it clear that collection and processing of revelatory data and/or metadata requires prior approval by an independent body, such as a court.

---

1 Joined Cases C-293/12 and C-594/12, 8 April 2014.

- The principles must make it clear that any data collection or processing can only be justified if it furthers a legitimate purpose, and not just any legislative purpose.

Accountability

Principle F states that:

- ***Data use at all stages of the information lifecycle should be accountable***

The APF agrees with the accountability principle; but it needs to be explained in greater detail, and substantially improved. First, there is little value in an accountability principle if it is after the fact (ie. the horse has already bolted). This is why procedural safeguards prior to the collection or processing of data are of prime importance. Secondly, any *ex post* accountability mechanisms must be sufficiently robust and properly resourced. The APF does not consider that the accountability mechanisms in the current regulatory regime are sufficiently robust to deal with the challenges of Big Data practices. Moreover, any bodies charged with performing accountability and overview of such practices must have sufficient expertise to be able to engage in a reasoned assessment of the relevant activities; and we are unconvinced that existing bodies have that expertise. In addition, the accountability principle raises the question of accountable according to what criteria? As the APF considers that the existing regulatory framework is neither adequate nor appropriate, there is a need for the development of proper criteria for assessing Big Data practices, which properly take into account the importance of protecting the right to privacy. Finally, for the accountability principle to be effective there needs to be proper enforcement, including penalties for failing to meet the relevant standards. As drafted, the principles do not mention enforcement – including how the principles might be enforced – which is clearly a major omission.

Transparency

Principle H states that:

The regulatory framework should support openness and transparency while safeguarding operational secrecy, where necessary.

To begin, the drafting of this principle seems strange, as it appears to imply an evaluation of the regulatory framework, which has previously been ruled out. The APF submits that any evaluation of the existing regulatory framework (and practices) suggests that there be a serious and abiding concern about the degree of transparency including, for example, broad exemptions for NSLEs. The inclusion of an ill-defined exemption for 'operational secrecy' in this principle suggests that the tradition of hiding behind this as an excuse for all or any activities, including privacy-invasive activities, may well be legitimised by the proposed transparency principle.

As far as the explanation of the principle is concerned, the relevant practices should be transparent to the public at large, and not simply to interest groups or those potentially adversely affected: potential invasions of privacy are of interest to everyone, and not just sections of the public.

Finally, the transparency principle should be linked (at least as a matter of explanation) to the accountability principle, especially in that there should be independent review of decisions to withhold information (such as on operational grounds) and mechanisms for enforcing a failure to comply with the transparency principle.

Scope

The scope of the principles are essentially established by the proposed definitions, especially the definitions of 'Big Data analytics' and 'information lifecycle'. The APF submits that there are some problems with these definitions, especially in so far as they may be interpreted as legitimising serious invasions of the rights to privacy and data privacy. In these comments we refer to only some of our most important concerns, which relate to the definition of the 'information lifecycle'.

First, in relation to 'access to data by NSLE agencies' (b), this is extended to include 'data held by foreign governments'. The APF is very concerned that, within the current, extremely weak regulatory framework, this may be used to legitimise very serious invasions of privacy by foreign governments that do not adequately protect the human rights of Australians. This includes, but is not limited to, governments that are involved with the highly concerning 'Five Eyes' programs.[2] Furthermore, the purchase of bulk data sets by NSLES from private brokers for the purpose of Big Data analytics

2Â Zouave, E (2015), 'Five Eyes integration and the law', *Privacy International*, https://www.privacyinternational.org/node/575.

has recently gained attention as an invasion of privacy that potentially violates existing rights in the United States and Canada.[3]

Secondly, 'access to data by NSLE agencies' (b), is extended to include 'appropriate decryption of encrypted data where appropriate'. If we leave aside the repetition of the word 'appropriate', this part of the definition has the potential to legitimise wide scale decryption of encrypted data. In particular, the circumstances in which decryption of data might be considered appropriate are not spelt out and are completely unclear. Promoting decryption 'where appropriate' could well provide justification for practices that disproportionality undermine the security and integrity of essential information infrastructures, where trust and security properly depends upon encryption. Accordingly, the APF submits that serious consideration must be given to the relationship between this part of the definition of the 'information lifecycle' and the proposed principles.

Conclusion

The formulation of proper principles for the application of Big Data analytics, including by NSLEs is extraordinarily challenging. The APF appreciates the challenges involved in maximising the advantages and minimising the risks of Big Data analytics. We are not, however, convinced that public policy making in this important area can be advanced in any way by an attempt to formulate extremely high level principles without (a) proper evaluation and analysis of the regulatory framework; (b) spelling out the operation of any principles in appropriate detail; and (c) evaluating the need for principles that may well conflict with the existing regulatory framework, such as an enforcement principle. Unfortunately, as drafted the high level principles fall well short of being either appropriate or adequate for the protection of the right to privacy and data privacy against the serious challenges posed by Big Data analytics, especially as potentially used by NSLEs.

3Â Freeze, C (2016), 'Social media sites cut off data flow to U.S. company who resells it to police'. *The Globe and Mail,* 11 October 2016, http://www.theglobeandmail.com/news/national/us-police-used-social-media-data-to-track-protestors-aclu/article32322710.