Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Submission to the European Commission

Consultation on the Commission's Communication

'*A comprehensive approach on personal data protection in the European Union*', COM(2010)609, December 2010.

Principal author

Nigel Waters, Research Fellow[1]
With contributions from Professor Graham Greenleaf

Cyberspace Law & Policy Centre
University of New South Wales (UNSW) Faculty of Law

And with input from several other international colleagues and associates

http://www.cyberlawcentre.org/

nigelwaters@pacificprivacy.com.au

+61 (2) 4981 0828

[1] The author was principal researcher on the *Interpreting Privacy Principles Project, funded by the Australian Research Council, 2006-2010.* Nigel is also Principal of Pacific Privacy Consulting (www.pacificprivacy.org.au). He was Deputy Australian Federal Privacy Commissioner from 1989-1997, and before that Assistant UK Data Protection Registrar 1984-89. He holds Masters degrees from the Universities of Cambridge and Pennsylvania and from the University of Technology, Sydney. Nigel is a Board member of the Australian Privacy Foundation (www.privacy.org.au) and represents Privacy International (www.privacyinternational.org) at meetings of the APEC Privacy Subgroup and other international fora.

Submission to the European Commission

Consultation on the Commission's Communication *'A comprehensive approach on personal data protection in the European Union'*, COM(2010)609, December 2010.

http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm

The Communication is a good summary of the challenges facing data protection in the 21st Century, particularly in the context of new technologies, business models, and international data transfer trends.

While all of the five challenges identified on pages 3-4 are real, we are concerned that the emphasis in the supporting text is misplaced. The importance of ensuring 'that individuals' personal data are actually effectively protected...' (under 'Addressing the impact .. ' on p.3) and 'better enforcement' (under the same heading on p.4) should be the *prime* objectives, while 'lessen the administrative burden' (under 'Enhancing the internal market ...' on p.4) and 'make transfers simpler and less burdensome' (under 'Addressing globalisation ...' also on p.4) , while desirable, should be *secondary* objectives. The former objective is firmly based on the right to privacy enshrined in the EU Charter of Fundamental Rights (Article 8) (and in Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR)) and clearly a higher order value than the other two interests. It is important that effective protection (re-iterated under the fifth heading 'Improving the coherence ...' on page 4) and 'better enforcement' are not weakened in pursuit of administrative convenience or cost saving. The correct emphasis is better represented in the last paragraph on page 4, and in the first paragraph of 2.1.1 on page 5, and should be carried through into all subsequent work on review of the Directive.

In this respect, and leading into the first subheading 'Ensuring appropriate protection' (2.1.1), we support the suggestion that has been made by others that the powers of Data Protection Authorities should explicitly be extended to the processing of personal data in circumstances where the processing at issue is alleged to cause a breach of Article 8 of the ECHR. The recitals of Directive 95/46/EC already expressly refer to the ECHR. It would be a small step to specify in a revised Directive that each DP Authority should expressly be able to enforce the Data Protection law in circumstances when Article 8 compliance is at issue with respect to the processing of personal data. For example, it should have be possible for Commissioners to assess whether or not some processing is lawful (i.e. proportionate) in terms of Article 8 in cases such as international data sharing or with the retention of personal data.

The effect of this change would explicitly link the Human Rights and Data Protection regimes. This is of particular significance in relation to the proposed extension of the data protection regime to 'third pillar' institutions – see under 2.3 below.

Ensuring appropriate protection (2.1.1)

In 2.1.1 (page 5), the Communication correctly identifies the 'problem' of ensuring that the definition of 'personal data' covers all information which allows individual to be identified. We suggest that it also needs to cover information which allows individuals to be 'targeted' for customised action, whether involving direct contact or not, and even where the individuals cannot be actually identified. We have in mind the increasingly common use of 'analytics' which can select individuals for attention; e.g. for customised direct marketing, presentation of webpage content etc,

even though the data controller may not know, or even be able to find out, the actual identity of the target. The effect of this sort of intrusion on individuals' privacy, based on analysis of their behaviour, is just as much a matter of privacy concern as if the controller actually knows their identity. We refer to our submission to the Australian Government in relation to its current review of the Privacy Act 1988, in which we state:

> "This recommendation fails to ensure that the Act covers an increasingly important category of information which, while not in itself identifying an individual, allows interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis. A broader definition is necessary partly to respond to technological change ... Replacing "reasonably identifiable" with "potentially identifiable" would go some way towards remedying this deficiency, but is not in itself adequate."[2]

We also refer to the valuable 2007 report on this issue by the Article 29 Working Party.[3]

Increasing transparency (2.1.2)

In 2.1.2 (page 6), the Communication correctly identifies transparency as a key condition, and we agree that the relevant requirements in the Directive are not sufficient. However, we caution against any implication that increased transparency alone will address the multi-faceted reasons why existing data protection regimes have been less than satisfactory in operation. The idea that a 'notice and consent' model, which has tended to be favoured by US interests, but is also built in to the Directive, can be a sufficient basis for 'self-service' protection has, we suggest, been thoroughly discredited both by experience and by the increasingly well developed academic discipline of 'behavioural economics'. The power imbalances between data controllers and data subjects, complexity of data use and organisational relationships, limited time available to data subjects and many other factors mean that better information, while desirable, will not be effective on its own.

The 'standard form privacy information notices' suggested on page 6 could be useful if offered as models or guides, but making their use mandatory could result in notices being used where not appropriate, potentially confusing and misleading data subjects. Data controllers should instead be encouraged to write their own 'plain language' notices that explain their particular circumstances. The test of compliance with notice requirements should be 'comprehension by a reasonable person'.

We strongly support the introduction of a mandatory data breach notification requirement across all sectors, but consistent with the requirements of the e-Privacy Directive, as suggested on page 7.

Enhancing control (2.1.3)

We support the proposed investigation of ways of implementing both a 'right to be forgotten' and 'data portability' (2.1.3, page 8). While there are significant practical challenges involved, these are increasingly important rights in the context of cloud computing and social networking.

---

[2] Submission 25 at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/submissions.htm

[3] Opinion 4/2007 – WP 136 at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Raising Awareness (2.1.4)

We support the suggestion that the legal framework should include an obligation to carry out awareness-raising activities (2.1.4, page 8), at least for larger data controllers, going beyond the specific transparency/notification requirements. Data protection authorities and government departments rarely have sufficient resources to make a major impression on public awareness of rights and obligations – an obligation on large data controllers to contribute would both spread the cost, and increase the effectiveness, of awareness activity. We refer to the relevant report which the Commission itself published in 2009[4].

Consent (2.1.5)

The importance of ensuring that consent is a 'freely given, specific and informed indication' is of the utmost importance. As explained in 2.1.5 (page 8) consent requirements have often been interpreted in ways which do not benefit data subjects, and indeed often serve to legitimise inherently objectionable practices, such as effectively requiring consent as a condition of receiving goods or services. We strongly support the proposal for further examination of this issue, and suggest that 'revocability' should be another express element in any new definition of consent for the purposes of data protection law.

Sensitive data (2.1.6)

We have reservations about the overall value of additional controls on defined categories of 'sensitive data', because sensitivity is dependent on context. However, if special controls are to continue, then as suggested in the Communication, genetic data should certainly be included, given the potential uses to which it can be put and the effect on individuals. We note that in 2006, 'genetic information' was added to the definition of sensitive information in the Australian federal *Privacy Act 1988*, in response to an Australian Law Reform Commission report on genetic privacy.

Remedies and sanctions (2.1.7)

We strongly support the proposals for more effective enforcement of data protection rules, including by giving 'right of action' to representative groups, as well as individuals, and strengthened sanctions. While criminal sanctions have a part to play, the burden of proof involved can make them a blunt instrument, and we suggest that it is equally important to provide for a graduated range of sanctions, including civil penalties that can be imposed more quickly, easily and with a lower burden of proof, to address less serious but still significant privacy breaches.

---

[4] KANTOR Management Consultants S.A., *Evaluation of the Means Used by National Data Protection Supervisory Authorities in the Promotion of Personal Data Protection – Final Report*, European Commission: Directorate-General Justice, Freedom and Security http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm .

Legal certainty (2.2.1)

While we support the 'internal market' objectives, we re-iterate that these should be considered secondary to the protection of individual privacy. Examination of means to achieve further harmonisation of rules should have a clear preference for 'levelling up' to a highest common standard, and not 'levelling down' to the lowest.

Administrative burden (2.2.2)

We support a review of the existing notification/registration requirements, which we suggest have not been a particularly effective, useful or cost-efficient part of the data protection regime. We suggest the value of a register such as that kept by the UK Information Commissioner is very limited as the 'generic' descriptions used do no usually convey much useful information.

Applicable law (2.2.3)

We support further clarification of applicable law, and note in this context the valuable Opinion 8/2010 issued in December 2010 by the Article 29 Working Party.

Data controller's responsibility (2.2.4)

We strongly support the statement that (any) "administrative simplification should not lead to an overall reduction of data controllers' responsibility in ensuring effective protection" (page 11). We note the context of a current debate about an 'accountability principle'. We have been active participants in this debate, specifically in the context of the APEC Privacy Framework. It is in our view essential that any accountability principle should be seen as a (valuable) additional obligation – to demonstrate responsibility in practice – but must not in any way relieve data controllers of responsibility to comply with other data protection principles. Any suggestion that controllers can be trusted with greater flexibility in compliance in exchange for some token acceptance of 'accountability' should be resisted. Privately operated voluntary accountability mechanisms may be have a place, but their adoption should not diminish in any way the formal obligations of record keepers, the authority of data protection authorities, or the range of official sanctions or private remedies available.

Self-regulatory initiatives (2.2.5)

We strongly caution against any greater reliance on self-regulation as an alternative to clear, strong and binding rules, and vigorous and proactive regulation by data protection authorities. The history of 'self-regulation' in most sectors is one of dismal failure, with consumers invariably losing out to powerful commercial interests. We support intelligent cooperative solutions to data protection, under what is more appropriately labelled 'co-regulation'. Self-regulation that consists only of standards and mechanisms controlled exclusively by those who are being regulated does not work. Any self-regulatory activities must include meaningful participation by representatives of those who are the beneficiaries of regulation. Under any circumstances, we suggest that such initiatives are only truly effective when they are backed up by the prospect of strong enforcement action by independent supervisory authorities. In particular, an accountability principle (see above) must not be allowed to become a substitute for data export restrictions based on the law and practice of the receiving jurisdiction (see further on international transfers below).

We have strong reservations about the value of 'privacy seals', which can often create an illusion of privacy protection without delivering anything additional to legal obligations[5], and we especially question the value of privacy seals operated by for-profit companies when the profits of the seal program are wholly dependent on the revenues from seal holders.

Police and criminal matters etc (2.3)

We strongly support the proposed consideration of extending general data protection rules to the areas of police and judicial activity, and of harmonisation of any specific provisions considered necessary in these areas. We suggest that 'blanket' across-the-board exemptions from data protection rules can rarely be justified for entire agencies or sectors – instead, specific exceptions or provisions can address particular difficulties that the normal application of data protection rules may pose for other important public interests such as law enforcement and national security.

Any revised Directive must ensure that a regulator with privacy responsibilities in the area of national security and law enforcement (not necessarily the main data protection authority) has sufficient powers to monitor compliance and to make effective interventions. Member States should not be given the discretion to draft exemptions so wide that it allows them to negate any privacy protection the Commission seeks to introduce. Identification of the necessary powers of a regulator in these areas would help harmonise third pillar activities as part of the drafting of the Directive, and minimise the need to have the Commission involved in the post-implementation harmonisation procedures that are identified in the Communication.

International transfers (2.4.1)

We agree that the implementation of adequacy assessment under the existing Directive has been inadequate and confusing, with too many delays and bureaucratic processes. We therefore support the proposed review of these provisions, provided that the core principle of ensuring no loss of effective protection, when data is transferred, is not compromised. We refer to earlier work for the Commission in which the author was involved.[6] We also suggest that the EU-US Safe Harbor Framework be expressly included in this review, as several studies have documented major compliance failures and lacklustre enforcement.[7] As already noted above, an accountability principle is not a sufficient substitute.

Furthermore, any review must consider the confusion over international transfers that has been cause by the lack of transparency on the Commission's own procedures in relation to Article 25, and by its inaction in reaching decisions. Which jurisdictions are being assessed, the procedure by which jurisdictions are chosen for assessment, and the stage that each assessment has reached, remain opaque. There are too many jurisdictions with data protection laws, whose level of data protection has been assessed by the Commission, but where it is still unknown whether their laws are considered adequate. The end result is that the Article 25 process, and the Commission's role, has

[5] See report by Galexia Consulting on white lists at http://www.galexia.com/public/research/articles/research_articles-pa09.html

[6] See http://ec.europa.eu/justice/policies/privacy/studies/method-adequacy_en.htm

[7] See Galexia Consulting report at http://www.galexia.com/public/research/articles/research_articles-pa08.html

been brought into unnecessary disrepute. This needs to be remedied by transparent and efficient procedures.

Universal principles (2.4.2)

We support the continuation of a strong leadership role for the EU in promoting strong international data protection standards. Co-operation with other international bodies is essential to ensure consistency and harmonisation, but without loss of effective protection for individuals. We acknowledge the valuable work resulting in the Madrid Resolution of 2009, but also emphasise the significance of the contemporaneous Madrid Declaration by civil society organisations.[8]

Institutional arrangements (2.5)

We support the proposals to strengthen the role of Data Protection Authorities, and to ensure their independence and adequate resourcing. However, DPAs also need to repay this support with more effective and proactive enforcement activity, including acceptance of international benchmarking of performance standards, greater transparency and accountability – not just to the governments to which they report, but also directly to the public and civil society, and to the community of regulated data controllers.

In relation to international benchmarking, it is important that the EU continues to aspire to set the highest standards. We stress that it would be a serious mistake if the principles in the Directive were changed to 'harmonise' them with those in the APEC Privacy Framework, which are in significant respects weaker and less comprehensive than those in the Directive, and add nothing to it. We have documented this in a number of publications.[9]

The way forward (3)

We support the proposed next steps, including pursuit of an active infringement policy to ensure that individual member states do not lag behind in the promotion and enforcement of highest common standards.

---

[8] Both at http://www.privacyconference2010.org/adopted.asp

[9] See Waters N, The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation? UNSW Faculty of Law Research Series, 2008 [2008] UNSWLRS 59; Connolly C, 'Asia-Pacific region at the Privacy Crossroads', Galexia Research Articles, August 2008; Greenleaf G, The APEC privacy initiative: 'OECD Lite' for the Asia-Pacific? *Privacy Laws and Business International Newsletter* 71 (UK) (2004)