Updates to Chapter on Privacy in Cyberspace (2): Developments in Australia & Europe

M. E. Kabay, PhD, CISSP-ISSMP

Here's some more new material I just added in another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008.

* * *

The Office of the Privacy Commissioner of Australia summarizes the emerging principles for privacy protection as its *National Privacy Principles* (NPPs), as follows (quoting directly):

- NPP 1: collection. Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.
- NPP 2: use and disclosure. Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are also rules about direct marketing.
- NPPs 3–4: information quality and security. An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.
- NPP 5: openness. An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.
- NPP 6: access and correction. Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.
- NPP 7: identifiers. Generally prevents an organisation from adopting an Australian Government identifier for an individual (eg Medicare numbers) as its own.
- NPP 8: anonymity. Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.
- NPP 9: transborder data flows. Outlines how organisations should protect personal information that they transfer outside Australia.
- NPP 10: sensitive information: Sensitive information includes information relating to health, racial or ethnic background, or criminal records. Higher standards apply to the handling of sensitive information.[5]

State of Implementation of the EU Privacy Directive

As of July 2013, the 28 member countries of the European Union, including the new members states, have passed legislation fully implementing the Privacy Directive.[6]

In January 2012, the EU received a plan for improving privacy protection:

The European Commission has … proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.[7]

According to a press release,

> Key changes in the reform include:
>
> - A single set of rules on data protection, valid across the EU. Unnecessary administrative requirements, such as notification requirements for companies, will be removed. This will save businesses around €2.3 billion a year.
> - Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors – a requirement that has led to unnecessary paperwork and costs businesses €130 million per year, the Regulation provides for increased responsibility and accountability for those processing personal data.
> - For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours).
> - Organisations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.
> - People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability). This will improve competition among services.
> - A 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
> - EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
> - Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.
> - A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data.[8]

Readers committed to following the Directive will want to keep tabs on developments as these proposals wend their way through the EU deliberative process.

Establishment of the European Data Protection Supervisor

In 2002, the European Parliament and the European Council established the office of the European Data Protection Supervisor (EDPS), described as follows:

> The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:
>
> - monitoring the EU administration's processing of personal data;
> - advising on policies and legislation that affect privacy; and
> - cooperating with similar authorities to ensure consistent data protection….
>
> The supervisory task is to ensure that the EU institutions and bodies process personal data of EU staff and others lawfully. The EDPS oversees Regulation (EC) 45/2001 on data protection, which is based on two main principles:
>
> The responsible data controller needs to respect a number of obligations. For instance, personal data can only be processed for a specific and legitimate reason which must be stated when the data are collected.
>
> The person whose data are processed - the data subject - enjoys a number of enforceable rights. This includes, for instance, the right to be informed about the processing and the right to correct data.
>
> Every institution or body should have an internal Data Protection Officer. The DPO keeps a register of processing operations and notifies systems with specific risks to the EDPS. The EDPS prior checks whether or not those systems comply with data protection requirements. The EDPS also deals with complaints and conducts inquiries.[9]

In July 2013, the EDPS issued a report strongly criticizing the European Commission's plans for implementing computer-assisted border checks (*smart borders*). Peter Hustinx, the Director of the EDPS, was quoted as saying,

> "In the absence of such a policy, the creation of yet another large-scale IT database to store massive amounts of personal information is a disproportionate response to a problem that other recently created systems may be able to help solve. It would be prudent both economically and practically to evaluate the existing systems at least to ensure consistency and best practice."[10]

On July 31, 2013, the positions of EDPS and Assistant Supervisor became vacant.[11] It was not known whether there was a relationship between the EDPS criticism of smart borders and the vacancy.

ENDNOTES

[5] According to the Australian Government, "The Privacy Amendment Act includes a set of new, harmonised, privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs). They will replace the existing Information Privacy Principles (IPPs) that currently apply to Australian

government agencies and the National Privacy Principles (NPPs) that currently apply to businesses.

[6] Under the changes, there will be 13 new APPs. A number of the APPs are significantly different from the existing principles, including APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information." See http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform/what-s-changed

[7] "Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data." European Commission (2013-07-16). http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm

[8] "Commission proposes a comprehensive reform of the data protection rules." European Commission (2012-01-25). http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[9] "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses." EUROPA Press Releases (2012-01-25). http://europa.eu/rapid/press-release_IP-12-46_en.htm

[10] European Data Protection Supervisor. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS

[11] "EU Data Protection Supervisor slams 'smart borders'." NewEurope Online (2013-07-19). http://www.neurope.eu/article/eu-data-protection-supervisor-slams-smart-borders

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

