27 YEARS
1987-2014

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Privacy enforcement is strengthened in Australia

Civil penalties exceeding one million euros are possible but gaps remain in appeals and transparency. By **Graham Greenleaf.**

Australia's Privacy Act 1988 now includes considerably stronger enforcement powers, including civil penalties of up to AUD$1.7 million (1.15 million euros), in effect from 12 March 2014. This article first outlines the new powers, deficiencies in appeal rights and transparency which may reduce their effectiveness, and the Commissioner's draft 'enforcement policy'. Two further developments remain unresolved: mandatory data breach notification (MDBN); and a statutory 'privacy tort'.

The 2014 reforms are a result of the Privacy Amendment (Enhancing Privacy Protection) Act 2012 ('the Amendments'). It also amended the Privacy Act by including a new set of thirteen Australian Privacy Principles (APPs) to replace the National Privacy Principles (NPPs) previously applying to those parts of the private sector covered by the Act, and the Information Privacy Principles (IPPs) applying to the federal public sector. There is little innovative about the APPs, and in some respects they will weaken the NPPs and IPPs.[1] None of the thirteen APPs is, overall, an improvement, and eight are worse for privacy protection.[2] The new data export provision will in some cases require more disclosure by companies. The APPs

Continued on p.3

Issue 128 **April 2014**

Netherlands: Cookie provision and legislation on data breach

Ard Jan Dunnik and **Feyo Sickinghe** report on data protection developments in the Netherlands.

A proposal for the introduction of a notification obligation for personal data breaches (*meldplicht datalekken*) is currently being scrutinised by the Parliament. This legislation contains an amendment of the Data Protection Act (*Wet bescherming persoonsgegevens*). In case of a personal data breach the controller has an obligation to notify the data protection authority. In cases where the breach has adverse consequences for the private life of a data subject whose personal data it concerns, the controller must inform the data subject. Also, it is proposed to increase the maximum fine to €450,000 to be imposed by the Data Protection Authority.[1] In addition to the legislative proposal, the government will be presenting further amendments containing new provisions to improve the supervisory powers of the DPA.

The Dutch government acknowledges that a new European Union Data Protection Regulation is under discussion which also covers personal data breach notifications. However, the Dutch government expects that the Regulation will not enter into force before 2016, and therefore national legislation is to be put in place as a transitional measure.[2] Article 11.3a of the Telecommunications Act (TA) already encompasses a personal data breach notification obligation for telecoms operators. The Authority for Consumers & Markets (ACM) must be notified. Based on this new proposed legislation, the DPA, instead of the ACM, will be the competent authority.

Opinion on Google's combining of personal data

The Dutch DPA launched an investigation regarding combining personal data by Google pursuant to the company's privacy policy valid as per 1 March 2012. According to the policy, the company reserves the right to combine personal data from various Google services. The Dutch DPA decided that Google is the controller and therefore the Dutch Data Protection Act applies. The privacy policy's four objectives for combining of personal data are the personalisation of requested services, product development, display of personalised ads and website analytics. It was concluded that these objectives were ambiguous and insufficiently specified. Google's data collection objectives were judged to be in breach of the provisions of Article 7 of the Data Protection Directive. Furthermore, the information Google provided to data subjects was insufficient: Google's identity as a controller was not transparent. The types of processed personal data, including the purpose for collection, were not sufficiently specified.[3] Google stated three legal grounds for processing the data: unambiguous consent of the data subject, the processing was needed for the performance of a contract and Google claimed to have a legitimate interest in processing these data. The Dutch DPA rejected these claims.

First, according to the DPA's findings, Google gave incomplete or approximate information about the purposes and the categories of data collected. There was no evidence of unambiguous consent because Google did not offer data subjects any (prior) options to consent to or reject the examined data processing activities. Second, Google uses tracking cookies for combining personal data. Article 8 of the Data Protection Act requires unambiguous consent for personal data processing activities if no other legitimate grounds as set out in the article apply. The Dutch DPA concluded that there was no justification for the data processing activities in Google's relationship with the specific individual data subjects (and any agreement entered into with them). Third, the DPA found that Google's interests in processing the data did not outweigh the data subject's right to data protection. Google was summoned to seek consent from the data subjects for the combination of data and provide additional controls to users regarding these combinations. The combination of data must respect the principles of proportionality, purpose limitation, data minimization and right to object.[4]

Report on packet inspection of mobile networks

Mobile Networks Operators (MNOs) apply Deep Packet Inspection (DPI) to monitor data packets traveling the network by means of network management. DPI facilitates data header and in-depth data packet monitoring. As a consequence DPI has been subject to intense debates in terms of network neutrality and e-privacy since 2012. The Dutch DPA reported on the analysis of data traffic on the mobile network by KPN, Tele2, T-Mobile and Vodafone. It concluded that the MNOs stored data in terms of websites visited and applications used by their customers. Article 11.5 Telecommunications Act (TA) requires timely deletion of this data or irreversible anonymisation. The DPA considered these data personal data. Therefore data subjects were to be informed accordingly. However, the investigation showed that customers were not sufficiently informed about the data collection and the purpose of collection. Another breach of law was found in collecting personal data for the purpose of market research, which was not considered as a sufficient justification for processing. The data subjects were not asked for their consent (Article 8 Data Protection Act). The MNOs took some measures to adapt their policies. However, the Dutch DPA is considering taking enforcement measures. At this stage, no public information on enforcement actions is available.[5]

New cookie provision

The e-Privacy Directive and article 11.7a TA require a user's informed consent for access and storage of data on end user terminal equipment. Article 11.7a TA is applicable to all cookies, except those that are technically necessary for communication. Informed consent is also required for analytical cookies. These cookies provide useful information for monitoring website traffic and visitors moving around a website. They enable website owners to improve their facilities and user experience. At the end of March, an amendment to article 11.7a TA was sent to the Dutch parliament. Analytical and related (i.e. performance) cookies used to collect information about the quality of service and effectiveness of information society services with limited or no impact on individual's private life will be exempted from informed consent. The official legislative proposal is similar to the version previously issued for public consultation. The amendment is expected to trigger a debate in Parliament about the use of cookies, transparency, informed consent and behavioural targeting. At the end of March, the ACM published a revised version of the cookie Q&A anticipating the exemption of analytic cookies.

Tax Administration's interests versus private life

SMS Parking B.V. processes customer data through online payment for car parking based on location data. The Dutch Tax Authority demanded that the company hand over the data to allow for detection of various types of tax evasion. SMS Parking rejected the demand on the basis of Article 8 European Convention of Human Rights. The Oost-Brabant regional civil court noted that the tax authority demanded the parking information on all customers, without any restriction. This was not proportional to the purposes of the tax authority (i.e. detecting tax evasion), and not in accordance with principle of necessity. Therefore the claim of the tax authority was denied. [6]

Processing of personal data from smart TVs

The DPA conducted an investigation into the collection of information through smart TVs built by TP Vision (Philips). Smart TVs allow for monitoring, storing and collecting customer online viewing data through the use of tracking cookies for personalised offers recommending future viewing. In a report published in July 2013, the DPA ruled that these cookies fall under the privacy regime and that storage, collection and processing of viewer data as being 'personal data' is subject to the user's prior informed consent. TP Vision did not seek unambiguous consent and was found to be in breach of article 34 of the Data Protection Act. TP Vision failed to inform the user of the identity of the controller (i.e. TP Vision), the types of data being processed and the storage period. TP Vision also failed to have a data processing agreement for the processing of personal data by Google Analytics. It is interesting to note that Google refused to engage in such an agreement. TP Vision announced that it will set up a proprietary analytics system.[7]

Patient's data on insurance claim forms

On 13 December 2011 the DPA approved a health insurer's code of conduct that, *inter alia*, allowed for the inclusion of a patient's health data (diagnosis and the like) on the invoices medical doctors sent to insurers. As expected, the Court of Amsterdam annulled the DPA's approval as the code of conduct unduly interfered with the right to a private life pursuant to Article 8 European Convention of Human Rights and did not contain sufficient safeguards in order to prevent presentation of medical personal data to third parties.[8]

AUTHORS

Ard Jan Dunnik, Associate, and Feyo Sickinghe, of Counsel Regulatory Communications, Bird & Bird Netherlands.
Emails: ard.jan.dunnik@twobirds.com, feyo.sickinghe@twobirds.com

REFERENCES

1 Kamerstukken II 2012/13, 33 662, nr. 2
2 Kamerstukken II 2012/13, 33 662, nr. 3, p.3
3 Article 33 and 34 Data Protection Act
4 CBP GOOGLE PRIVACY POLICY: MAIN FINDINGS AND RECOMMENDATIONS p. 2-5
5 Onderzoek naar de analyse van gegevens over en uit het mobiele dataverkeer door Tele2 Nederland B.V. (Rapport definitieve bevindingen van 12 juni 2013), Den Haag: CBP 2013)
6 Rb. Oost-Brabant (vzr.) 26 November 2013, ECLI:NL:RBOBR:2013:6553
7 Onderzoek naar de verwerking van persoonsgegevens met of door een Philips smart tv door TP Vision Netherlands B.V. (Openbare versie Rapport definitieve bevindingen van juli 2013), Den Haag: CBP 2013, p. 2-5.
8 Rb. Amsterdam 13 November 2013, ECLI:NL:RBAMS:2013:7480

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Online search function
Subscribers can search the *PL&B* website to access: back issues since 1998; special reports, slides, videos and recordings from *PL&B* events.

3. Regular e-news
Subscribers receive updates about relevant news as and when it happens. Choose international and/or United Kingdom data protection news.

4. Helpline Enquiry Service
Subscribers can request information about the current status of legislation and other information.

5. Index
Search a country, subject and company index (1987-2014) www.privacylaws.com/Publications/report_index/

Electronic Option
The electronic PDF format enables you to: receive the Report on publication; click-through from email and web addresses; and follow links from the contents page to articles.

Subscription Discounts
Discounts for 2-4 users or 5-25 users and 2 years (10%) or 3 years (15%). See www.privacylaws.com/subscribe

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists.*

Privacy Laws & Business also publishes the United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

❑ *PL&B International* Report Subscription **£500**

❑ *UK/International* Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users

Number of years: 2 (10% discount) or 3 (15%)

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com 24/04

www.privacylaws.com

Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.