HUNTON& WILLIAMS

EUROPEAN PRIVACY & E-COMMERCE ALERT

July 2008

Contacts

Brussels Office
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium
P: +32 (0)2 643 58 00
F: +32 (0)2 643 58 22

Christopher Kuner
+32 (0)2 643 58 56
ckuner@hunton.com

Dr. Jörg Hladjk
+32 (0)2 643 58 28
jhladjk@hunton.com

Cédric Burton
+32 (0)2 643 58 29
cburton@hunton.com

London Office
30 St Mary Axe
London EC3A 8EP
P: +44 (0)20 7220 5700
F: +44 (0)20 7220 5772

Bridget C. Treacy
+44 (0)20 7220 5731
btreacy@hunton.com

EU: Article 29 Working Party Issues Recommendations on Data Storage by Search Engines

On April 4, 2008, the Article 29 Working Party published its opinion on search engines. The opinion first concludes that IP addresses — including dynamic IP addresses — are personal data, since the necessary data will be available to identify the user(s) of a particular IP address. Then, unless the search engine provider "is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side". Second, analyzing the applicable legal rules, the Working Party concludes that data protection rules apply to the processing of personal data by search engine providers in many cases, even when their headquarters are outside the EEA.

Following these two preliminary conclusions, the Working Party's main recommendation requires search engine providers to delete or anonymize any personal data after a maximum period of six months to avoid any misuse of the data. However, in the future, exceptions may be acceptable if the Working Party is provided with compelling reasons for a longer retention period. The opinion further imposes on search engine providers the obligation to process data only on the basis of a legitimate purpose and to delete or anonymize the data upon fulfilment of that purpose. In a final recommendation, the Working Party requires search engine providers to give the users an adequate right of access to their data, and to allow them to control and correct the data held about them.

The full text of the opinion (entitled "Opinion on data-protection issues related to search engines") is available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm.

EU: European Data Protection Supervisor Publishes Opinion on Review of e-Privacy Directive

On April 10, 2008, the European Data Protection Supervisor (EDPS) published its opinion on the Commission's proposal to review the e-Privacy Directive (Directive 2002/58/EC). The EDPS called for further improvements to the Directive, believing that the proposed amendments are not as ambitious as they should be. According to the EDPS, the coverage of a mandatory security breach notification system should be extended to apply to all providers which process personal data. Further, the EDPS proposed to broaden the scope of the Directive to include providers of electronic communication services in mixed as well as private networks. Finally, the EDPS proposed that the scope of the new right for legal persons to take action against spammers should also be extended to apply to breaches of any of the Directive's provisions.

The full text of the EDPS' opinion is available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/

Opinions/2008/08-04-10_e-privacy_EN.pdf.

Belgium: DPA Issues Opinion on Processing of Biometric Data and Authentication

On April 9, 2008, the Belgian DPA issued an opinion on the processing of biometric data and the authentication of individuals. In the opinion, the Belgian DPA underlines that biometric data is personal data, that it can sometimes constitute sensitive data, and that using biometric data constitutes data processing. Therefore, data protection rules apply to biometric systems used for authentication. Second, the Belgian DPA insists that data controllers should respect the proportionality principle. Finally, the DPA states that it considers a biometric system to be proportionate when: (1) the data controller may not achieve the objective pursued by the system with another technical solution; (2) the data controller uses a system which does not create any physical trace; (3) the system does not keep reference biometric data in a central database; (4) the system does not use raw data but rather template data; (5) no data is collected without informing the data subject; and (6) the system is adequately secured.

The Belgian DPA's opinion is available (in French) at: http://www.privacycommission.be/fr/docs/Commission/2008/avis_17_2008.pdf.

Germany: German Telecom Provider Involved in Major Privacy Scandal

On May 24, 2008, it emerged that Deutsche Telekom, Europe's largest telecommunications service provider based on revenue, had used an external agency to track phone calls made by senior executives and journalists. The company's intention was to identify leaks of financial information to the press. Call records included details of the time, duration and participants of the calls. Deutsche Telekom has announced that it would now conduct a thorough and independent investigation, and would fully support the public prosecutor in this matter. According to legal experts, the activity went beyond a violation of data protection regulations by violating telecommunications secrecy, an infringement which may lead to sanctions under criminal law. An examination is now under way as to whether to initiate proceedings against Deutsche Telekom.

Deutsche Telekom's full press release (in German) can be retrieved at http://www.telekom.com/dtag/cms/content/dt/de/51236?archivArticleID=534296.

Germany: Constitutional Court Decides to Limit the Scope of the Data Retention Act

In a preliminary ruling on 19 March 2008 the Federal German Constitutional Court found certain parts of Germany's Data Retention Act to be unconstitutional, thus delaying the implementation of Directive 2006/24/EC. In particular, the claim challenged the obligation to store data and the use of data under the German Telecommunications Act. The ruling, while not completely prohibiting the collection of data, restricts use of the Act to cases of serious crimes in which a judicial warrant has been obtained. In the future, this means that the retained data may only be used to support the prosecution of a case in which sufficient evidence is lacking or inaccessible. Before reaching a final decision, the German Constitutional Court will wait for the outcome of the European Court of Justice's (ECJ's) decision in *Ireland v. Council of the European Union, European Parliament* (Case C-301/06), a case involving an action to repeal the Data Retention Directive. Meanwhile, the Court ordered the German Government to report on the effects of data retention as well as the implementation of its decision by September 1, 2008.

The full text of the Federal German Constitutional Court's press release (in German) is available at http://www.bundesverfassungsgericht.de/en/press/bvg08-037.html.

Germany: Constitutional Court Rules against Online Searches by Government Agencies

In a landmark judgment handed down on February 27, the German Federal Constitutional Court placed severe restrictions on the law enforcement monitoring of online activities and private computer usage. Finding that monitoring computer use creates even greater dangers to privacy than does wiretapping telephone use or bugging private homes (as it allows the creation of comprehensive personal profiles), the Court created a new fundamental right of computer privacy. While the case applies directly only to law enforcement activities, its wide-ranging nature means that it will probably also further limit the ability of companies to carry out such activities as monitoring employee computer usage and creating customer profiles.

The full text of the Federal German Constitutional Court's press release (in German) is available at http://www.bverfg.de/pressemitteilungen/bvg08-022.html.

Italy: DPA Declares Spying on P2P Users Illegal

In a press release dated March 13, 2008, the Italian data protection authority (Garante) declared that some private companies were in breach of Italian

data protection law when monitoring the activities of peer-to-peer (P2P) users in order to take legal action against them. The decision was made following proceedings in the Peppermint case. Peppermint, a German record label, made use of Logistep's services to collect thousands of IP addresses of users that were exchanging songs via P2P networks. Peppermint used that data to obtain users' physical addresses and to threaten them with legal action. The Court of Rome had previously declared unlawful the disclosure of P2P users' identity by Internet service providers. The Italian DPA now expressly prohibited the collection of IP addresses. The rationale is that this type of collection is in contravention of various principles established by Directive 2002/58/EC. The Italian DPA thus ordered the removal of all personal data collected from P2P users by those companies by March 31, 2008.

The text of the decision and the related press release are available at: http://www.garanteprivacy.it. A copy of the decision (in Italian) is also available upon request.

United Kingdom: ICO Publishes New Guidelines on Data Security Breach Management

On March 27, 2008, the Information Commissioner's Office (ICO) issued guidelines containing the appropriate steps an organization should take in the case of loss of personal data. At the same time, it urged Parliament to criminalize data security breaches. The move followed the Government's loss of some 25 million citizens' personal data in November 2007 and numerous other breaches. Pursuant to the guidelines, organizations which have experienced a security breach should incorporate the following four stages into a breach management plan: (1) containment and recovery; (2) assessing the risks; (3) notification of breaches to the ICO; and (4) evaluation and response. At present, however, there is no general obligation to notify a data security breach, although different rules apply to each particular sector.

The full text of the guidelines is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf.

United Kingdom: ICO Issues New Guidelines on Transfer of Employee Information

On June 4, 2008, the Information Commissioner's Office (ICO) issued guidance setting out compliance with the Data Protection Act 1998 with regards to a transfer of employee data under the Transfer of Undertakings (Protection of Employment) Regulations 2006 (TUPE). TUPE is applicable to organizations transferring their business to new employers who intend to retain the employees of the transferring business. In this case, the transferring business is required to supply to the new employer the so-called "employee liability information" containing details such as name, age or disciplinary/legal actions taken. The guidance states that the transfer ought to be for the purposes covered by TUPE, but at the same time includes exceptions that fall outside the scope of TUPE; in these cases, the guidelines recommend to anonymize the transferred data. On a final point, the guidance gives advice on the retention of employee data after the employee transfer is complete.

The full text of the guidelines is available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/gpn_disclosure_employee_info_tupe_v1.0.pdf.