Bird & Bird & data protection update

July 2013

We are enclosing our latest data protection update of news and developments in June.

Key points to note are as follows:

1. The ICO has released its annual report;
2. An Opinion by the Advocate General of the European Union Court of Justice states there is no 'right to be forgotten' by search engine providers;
3. A new Regulation altering the procedure for E-Privacy Directive telecoms breach reporting has been adopted; and
4. The Irish Presidency of the Council of the European Union has published a draft compromise text of the Draft General Data Protection Regulation.

Ruth Boardman
Partner
ruth.boardman@twobirds.com

Title	Description
UK	
Information Commissioner's Office (ICO)	
24 May 2013	**ICO sends letter to Ministry of Justice on draft EU Data Protection Regulation** ICO has published the letter sent to the Justice Secretary expressing concerns about the ability of the ICO to implement the draft Data Protection Regulation without additional resources. The main points covered in the letter are: • The Information Commissioner recognises the need for a new, effective data protection regime. • There are concerns about the burdens the proposals will place on the ICO and other data protection authorities (DPAs). Breach reporting, sanctions, prior assessment of transfers and the consistency mechanism are all singled out as being burdensome. • The ICO's funding concerns are compounded by abolition of the notification system, which the ICO anticipates will leave it with a £16 million funding shortfall. **The full letter can be accessed here.**
03 June 2013	**ICO publishes guidance on social networking and online forums** The new guidance replaces ICO's 2007 guidance on this topic. Issues covered include: • a summary of provisions of the DPA which relate to online forums; • guidance about how to determine whether an online forum is being used for non-domestic purposes; • guidance on running an online forum; and • information about ICO involvement in complaints against those running social networking sites (both organisations and individuals). The guidance is consistent with the Article 29 Working Party Opinion on online social networking in 2009, and takes on board comments made in the *Solicitors From Hell* case, which was critical of ICO's reluctance to intervene in cases where individuals complained about inaccurate data on such forums. The document also gives good guidance to data controllers on their responsibilities under the DPA. **The full guidance can be accessed here.**

20 June 2013

ICO releases Annual Report

Key statistics include:

- £2.6m total civil monetary penalties were imposed on 23 organisations;
- Fifty-five pieces of guidance on the Freedom of Information Act were published or revised;
- Following surveys it was revealed that 86% of individuals were aware of their specific rights under the Freedom of Information Act and 87% of individuals were aware of the right to see information held about them;
- Fifty-eight audits were conducted of data controllers, an increase of 38%; and
- 225,138 calls received by the ICO's helpline, an increase of 3.7%.

The full report can be accessed here.

Ministry of Justice

June 2013

Ministry of Justice call for evidence over proposed cybersecurity directive

This Ministry of Justice has closed its call for evidence over the proposed EU cybersecurity directive. The consultation speculated that similar triggers to those applied to telecoms breach reporting under the E-Privacy directive might apply to the new breach reporting requirements contained in the proposed legislation. The consultation in particular sought feedback from stakeholders on how the proposal might affect those businesses that would be required to report breaches as "market operators". The latest reports from Europe have suggested that several delegations in the Council would prefer a less prescriptive regime.

The call for evidence documents can be accessed here.

Case Law

Heard on 16 April 2013

EAT confirms that use of covert surveillance does not necessarily make a dismissal unfair.

In the case of *City and County of Swansea v Gayle UKEAT/0501/12* before the Employment Appeal Tribunal, the council successfully appealed against an Employment Tribunal decision that the council's investigation into Mr Gayle's misconduct had unjustly interfered with his Article 8 right to privacy and was contrary to the ICO's Employment Practices Code. The council had engaged a private investigator to check rumours that Mr Gayle was playing squash during work hours then returning to clock off. The investigator had covertly filmed Mr Gayle 5 times outside a sports centre, which led to his dismissal for misconduct.

The EAT ruled that Article 8 was not engaged, because:

- Mr Gayle was filmed in a public place, where he would not have a reasonable expectation of privacy;
- Mr Gayle was filmed during his work hours, when an employer is entitled to know his whereabouts; and
- Mr Gayle was defrauding his employer, and so was not entitled to a right to privacy.

Even had Article 8(1) been engaged, the EAT noted that the council could have relied on the legitimate aims of preventing crimes and protecting their own rights. The EAT also said that the Tribunal had overstated the importance of the Employment Practices Code, which should not be considered to have statutory effect – failure to follow the guidance shouldn't itself make a dismissal unfair.

The full judgment can be accessed here.

Title	Description
UK	
Enforcement	
02 June 2013 – 01 July 2013: Three enforcement notices, two undertakings and two monetary penalty notices	Two undertakings were given in respect of compliance with the seventh data protection principle; a third undertaking was given to Google in respect of payload data; and the two enforcement notices were in relation to the loss of unencrypted laptops and the erroneous dissemination of sensitive personal data by facsimile. **Please see the attached Enforcement Table for more details of the enforcement actions.**

Title	Description
Europe	
Cases	
Google Spain SL, Google Inc. v Agencia Española de Protección de Datos **Opinion of the Advocate General** **Court of Justice of the European Union** **Case C- 131/12** **25 June 2013**	**Advocate General opines that search engine service providers are not data controllers for the personal data appearing on web pages indexed by their service** In February 2010, the subject of a national newspaper article from a decade ago contacted Google Spain and requested that the search results show no links to the newspaper when his name and surnames were entered into Google's search engine. Google Spain forwarded the request to Google Inc. in California taking the view that the latter was the undertaking providing the internet search service. The Agencia Española de Protección de Datos (Spanish Data Protection Agency, AEPD) upheld the complaint against Google Spain and Google Inc., calling on them to withdraw the data from their index and to render future access to them impossible. Google Inc. and Google Spain brought two appeals before the Audiencia Nacional (National High Court, Spain), seeking annulment of the AEPD decision. The Audiencia Nacional referred a series of questions to the European Court of Justice. Advocate General Niilo Jääskinen's Opinion firstly addressed the question of the territorial scope of the application of national data protection legislation. He argued that Member State law applies where there is an establishment in that state involved in selling targeted advertising to inhabitants of a Member State, even if the technical data processing operations are situated in other Member States or third countries. The Opinion concludes that national data protection authorities cannot require an internet search engine service provider to withdraw information from its index except in cases where this service provider has not complied with exclusion codes or where a request from a website regarding an update of cache memory has not been honoured. A possible 'notice and take down procedure' concerning links to source web pages with illegal or inappropriate content is a matter for national civil liability law based on grounds other than data protection. The Advocate General was also of the view that the Data Protection Directive does not establish a general 'right to be forgotten'. The opinion of the Advocate General is not binding. A full decision is to be made by the EU Court of Justice by the end of the year. **The Opinion of the Advocate General can be read here.**

Title	Description
Europe	
Draft Data Protection Regulation and Directive	
06 June 2013	**Draft compromise text of the General Data Protection Regulation released** The Irish Presidency of the Council of the European Union released its response to Chapters I – IV of the draft General Data Protection Regulation. Comments include: • The addition of 'pseudonymised' data as a sub-category of personal data, rather than a sub-category of anonymous data or as a third type of data at Article 4(2a); • The addition of a recital clarifying the right to data protection as a qualified right; • A reversion to the current position for valid consent under the Directive ie a requirement of 'unambiguous' consent. (Except in the case of processing sensitive personal data (Recital 25 and Article 9(2)); and • Data controllers should not be required to provide fair processing notices where data is collected from publicly available sources (Article 14a(4)(c)). **The complete text can be accessed here.**

Title	Description
Europe	
Article 29 Working Party	
17 June 2013	**Concerns regarding the proposed Entry Exit System** The Article 29 Working Party (WP29) adopted an Opinion on "Smart Borders": the proposals for an Entry Exit System (EES), and a Registered Traveller Programme (RTP) for the Schengen Area. The Entry Exit System proposes a centralised storage system for the entry and exit data of third country nationals admitted to the Schengen area for short stays. A centralised system means that entry data can be checked no matter where the third country national exits the Schengen Area. The primary purpose of the system is to counteract the problem of overstay in the Schengen Area of third country nationals who originally entered for a short stay (max 90 days out of 180 days) on a valid visa or for a valid purpose. The Working Party recognises the aim to have an integrated border management system for the management of migration flows and prevention of irregular migration. However, it also recognises how the system, for which there are alternative measures, would create a colossal new database which could potentially interfere with the right to protection of personal data as set out in Article 8 of the EU Charter of Fundamental Rights. **The full Opinion can be accessed here.**
20 June 2013	**Joint letter shows increased appetite for co-operation with other authorities outside Europe** The Article 29 Working Party recently wrote a joint letter with several other heads of data protection authorities outside Europe, in a sign that regulators are more and more keen to operate in co-operation with each other across international borders. The letter, sent to Google's CEO Larry Page asking for more information on Google Glass, was signed by the heads of the Canadian, Australian, New Zealand, Mexican, Israeli and Swiss data protection regulators, as well as by Working Party Chairman Jacob Kohnstamm. **The letter can be found here.**

Title	Description
Europe	
EDPS	
17 June 2013	**EDPS says cyber security is not an excuse for the unlimited monitoring of individuals** Following the publication of his opinion on the EU's strategy on cyber security, the European Data Protection Supervisor (EDPS) has criticised the lack of clarity as to how the principles of data protection will be applied to reinforce cyber security. This is in response to the Commission's adopted proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. **The Opinion can be accessed in full here and the EDPS press release here.**

Title	Description
Europe	
Other	
30 May 2013	**Sweden fined €3,000,000 for delay in transposing the Data Retention Directive** The Court of Justice rejected the justifications put forward by Sweden in imposing this fine; namely that its non-compliance was attributable to its legislative procedure, extensive political debate on the Directive, and the need to weigh the issue of protection of privacy. In doing so it held that the country had failed to meet its obligations under EU law since the initial judgement against it in 2010, undermining the private and public interest in ensuring that data is available for the investigation, detection and prosecution of serious crime. **Full text of the judgement is available here.**
14 June 2013	**Transatlantic group to be set up to discuss PRISM and MINERVA** A group of EU and US experts is to be set up to address the nature and safeguards of the US anti-terrorism data collection programmes. EU Commissioner for Home Affairs, Cecilia Malström, made the announcement at the end of the EU-US summit in Dublin where the US agreed to share relevant information. The extent of US surveillance on phone and internet communications came to light after former National Security Agency (NSA) employee Edward Snowden shared top secret NSA documents with The Guardian newspaper. **The full text of the speech is available here.**

24 June 2013

European Commission adopts new regulation in relation to telecoms data breaches

The European Commission adopted on 24 June a Commission Regulation on data breaches for telecoms operators and Internet Service Providers (ISPs) to handle situations where their customers' personal data is lost, stolen or otherwise compromised. The Regulation was published in the OJEU on 26 June and will come into force on 25 August 2013.

Companies will have extra clarity about how to meet those obligations, and customers will have extra assurance about how such breaches will be dealt with. Companies must:

- Inform the competent national authority of the incident within 24 hours after detection of the breach, in order to maximise its confinement. If full disclosure is not possible within that period, they should provide an initial set of information within 24 hours, with the rest to follow within three days;
- Outline which pieces of information are affected and what measures have been or will be applied by the company; and
- Make use of a standardised format (for example an online form that is the same in all EU Member States) for notifying the competent national authority.

In assessing whether to notify subscribers (i.e. by applying the test of whether the breach is likely to adversely affect personal data or privacy), companies should pay attention to the type of data compromised, particularly, in the context of the telecoms sector, financial information, location data, internet log files, web browsing histories, e-mail data, and itemised call lists.

The Commission also wishes to incentivise companies to encrypt personal data and has published an indicative list of technological protection measures, such as encryption techniques, which would render the data unintelligible.

Please find the Regulation here.

Enforcement notices and undertakings

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
07 June 2013	**Glasgow City Council**	**Enforcement Notice**	The ICO has served an enforcement notice on Glasgow City Council following the theft of two unencrypted laptops from the councils' offices, one of which contained the personal information of 20,143 people. There had been previous thefts of equipment from these offices but physical security measures had not been improved. 70 other unencrypted laptops were also unaccounted for. A monetary penalty of £150,000 was issued by the ICO.	The Council has been ordered to: - Conduct a full audit of IT assets used to process personal data by 30 June 2013; - Create a new asset register by 31 July 2013; - Ensure that the register is up to date on a yearly basis; - Provide training to managers in relation to asset management by 30 June 2013; and - Reissue information on security guidelines and update information security training for all staff by 30 June 2013. The Notice can be read here.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
11 June 2013	**Google Inc.**	**Enforcement notice**	In 2010, the Information Commissioner's Office became aware that the data controller's Street View vehicles had mistakenly collected personal data relating to thousands of individuals. This information included email addresses, URLs and passwords. An undertaking was entered into by Google to delete all payload data collected in the UK which the data controller had no outstanding legal obligation to retain. Following this, in 2012, the data controller reported that they had accidently retained five discs which contained payload data collected in the UK.	The ICO issued an enforcement notice, with the data controller to: 1) securely destroy within thirty-five days, any personal data held on vehicles discs and collected in the UK using Street View vehicles; and 2) promptly inform the Information Commissioner should they discover a Street View vehicle disc holding personal data collected in the UK. The full enforcement notice can be found here.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
12 June 2013	**Central Bedfordshire Council**	**Undertaking**	An individual's sensitive personal data had been made publicly accessible without consent via a planning portal on the Council's website. The data controller also reported the inappropriate obtaining and use of sensitive personal data held in a social care database by two employees. Central Bedfordshire Council undertook to ensure that that the procedures covering the preparation of planning application documentation for publication would be followed by staff and that all legacy data from the previous authority would be removed by 31 March 2013.	The data controller undertakes to ensure that: (1) The procedures covering the preparation of planning application documentation for publication are followed by staff; (2) Staff are aware of the data controller's procedures for the preparation of planning application documentation for publication and are appropriately trained how to follow those procedures; (3) By 31 March 2013 the social care database referred to in this undertaking contains a completely cleansed dataset free from unnecessary legacy data originating from the previous local authority; and (4) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage**.** The full undertaking can be found here.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
12 June 2013	**Bedford Borough Council**	**Undertaking**	A social care record, containing sensitive personal data, was inherited by two new unitary local authorities from the previous authority's social care database. This record had been compromised by the inappropriate actions of two of its employees. As a result both new unitary authorities inherited records not relevant to their provision of social care services. Bedford Borough Council undertook that all legacy data from the previous authority would be removed by 31 March 2013.	The data controller undertakes to ensure that: (1) By 31 March 2013 the social care database referred to in this undertaking contains a completely cleansed dataset free from unnecessary legacy data originating from the previous local authority; and (2) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage. The full undertaking can be read here.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
13 June 2013	**North Staffordshire Combined Healthcare NHS Trust**	**Monetary Penalty**	The data controller sent several faxes containing sensitive personal data about vulnerable adults to a member of the public in error. The faxes were intended for a Wellbeing Centre which provides psychological therapies. The ICO report found a serious contravention of section 4(4) of the Data Protection Act through a failure to ensure a level of security appropriate to the harm that might result from such unauthorised processing and the inappropriate organisational measures taken by the data controller.	A monetary penalty of £55,000 was issued by the ICO. The monetary penalty notice can be read here.

UK				
Date	**Entity**	**Enforcement notice, undertaking or monetary penalty?**	**Description**	**Summary of steps required (in addition to the usual steps*)**
18 June 2013	**Nationwide Energy Services & We Claim You Gain**	**Monetary Penalty**	Both companies are part of Save Britain Money Limited and were found to be responsible for over 2,700 complaints to the Telephone Preference Service or reports to the ICO over a 19 month period from May 2011 for direct marketing. The ICO found these activities to be a breach of Regulation 21 of the Privacy and Electronic Communications Regulations (PECR) on numerous grounds but particularly noted that both companies ignored recognised industry practices to avoid breaches of PECR and showed complete disregard for the requirements of the law.	Monetary penalties of £125,000 and £100,000 were issued by the ICO to Nationwide Energy Services and We Claim You Gain respectively. The monetary penalty notice for Nationwide Energy Services can be read here. The monetary penalty notice for We Claim You Gain can be accessed here.

*The usual steps required of an entity are to give undertakings that:

1. Staff are made aware of the data controller's data protection policy and procedures, and are adequately trained on how to follow these; and

2. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction and/or damage.

twobirds.com