Date	Description
UK	
Information Commissioner's Office (ICO)	
15 October 2014	**ICO publishes updated surveillance code** On 15 October 2014, the ICO published 'A data protection code of practice for surveillance cameras and personal information', replacing the Commissioner's 2000 CCTV code of practice. The most obvious difference between the codes is in the name – the 2014 version covers surveillance generally so encompasses not only CCTV but also automatic number plate recognition; body-worn cameras; unmanned aerial vehicles (i.e. drones); and other similar systems that may be used to capture the activities of any individuals. The code works through the data protection principles in the context of surveillance (generally and method-specifically), offering examples of how surveillance can potentially cause the data controller to breach its obligations under the Data Protection Act as well as tips for compliance. Although much of the guidance will be broadly familiar to those working with the 2000 CCTV code, the guidance is in some cases linked to other topical issues (e.g. data security (and encryption), privacy by design and the use of the cloud to store the images captured). In keeping with the proposals for the draft Data Protection Regulation, the ICO also recommends conducting a privacy impact assessment prior to the roll-out of any surveillance (and at frequent intervals once surveillance is in place), through which the data controller (and the surveillance vendor, if different) should consider the (ongoing) need for surveillance and how surveillance can be conducted in compliance with the Data Protection Act. In appendix 2, the ICO sets out a brief checklist for small CCTV operations, although it may prove helpful as part of a PIA for other forms of surveillance (where a more detailed and in-depth PIA may be appropriate). **Read the updated code here.**
16 October 2014	**International Co-operation Agreement** Data Protection Authorities reached an agreement on international co-operation at the 2014 International Data Protection Commissioners Conference. The Agreement is intended to facilitate the sharing of information, expertise and experience between data protection and related enforcement authorities. This will allow them to better respond to complaints which, increasingly, have a cross border element and to make better use of scare resources.

Date	Description
	The Agreement contains brief arrangements setting out how requests for assistance should be made and handled. It commits participants to maintain the confidentiality of information received. It also sets out how authorities will ensure that they meet data protection requirements if co-operation involves the sharing of personal data. Work on the Agreement was led by the Information Commissioner's Office and the Office of the Privacy Commissioner, the Canadian federal commissioner. **Read the full Global Cross Border Enforcement Cooperation Agreement here.**
16 October 2014	**Commonwealth Privacy Network Formed** The International Data Protection Commissioners Conference also saw the launch of the Common Thread Network - a network for commonwealth privacy authorities. The network was the originally the idea of the Canadian (federal) Privacy Commissioners Office. It will allow for sharing of expertise - especially in matters concerning cyber security and cybergovernance. The network will be facilitated by the Commonwealth Telecommunications Organisation. **Read more on the Commonwealth Telecommunications Organisation's website here.**
Enforcement	
	Enforcement for the contemplated period includes: 1 monetary penalty notice, 3 new undertakings and 1 enforcement notice Please see the Enforcement Table below for more details.
Other	
1 October 2014	**Ofcom calls for inputs on nuisance calls** Ofcom is required, under section 131 of the Communications Act 2003 (the "Act"), to prepare and publish a statement of its general policy with respect to its legal powers to deal with persistent misuse of an electronic communications network or electronic communications services (an offence under section 128 of the Communications Act 2003). The Act allows Ofcom to revise its statement on 'persistent misuse' from time to time as it thinks fit. Currently, Ofcom is in the process of reviewing its policy and has published a call for inputs to update its understanding of nuisance calls (particularly abandoned and silent calls).

Date	Description
	Ofcom has requested information on, for example: the drivers of silent and abandoned calls; harm caused by such calls; changes that could be made to the existing policy to improve enforcement; any technological changes in call centres. Responses are requested by 7 November 2014. Ofcom plans to publish a consultation on these issues in early 2015. **Read Ofcom's call for inputs here.**
3 October 2014	**Government Response to the Committee's Report on the Right to be Forgotten** The EU Sub-Committee for Home Affairs, Health and Education received the Government response to their report on the *Google Spain* case (*Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12)) on 3 October 2014. The key message from the Government is that while they do not support the "right to be forgotten" as it is currently drafted in the (draft) General Data Protection Regulation ("the Regulation"), they will continue to make representations and work with others on the Regulation with the aim of negotiating "a text that is more practical". The Government's main concern is that the right be forgotten of the Committee's formulation runs the risk of imposing "disproportionate or impractical burdens on businesses" when dealing with individuals' requests to have their personal data deleted. The Government's response emphasises the need to strike the appropriate balance between "the protection of personal data, and creating the right conditions for innovation and economic growth". It recommends a more proportionate, balanced and achievable framework for incorporating the right to be forgotten into the Regulation, which does not place unreasonable obligations on businesses. The Government therefore welcomes the work currently being undertaken by Article 29 Working Party [(see a summary on page 8 of this Bulletin) to support search engines and provide them with guidance in complying with the *Google Spain* case. **Read the full response here.**
25 October 2014	**Government publishes consultation on lowering legal threshold** The Government has published a six week consultation on lowering the legal threshold that must be met before the ICO can issue monetary penalty notices (up to £500,000) to firms and organisations responsible for nuisance calls and texts. The Privacy and Electronic Communications (EC Directive) Regulations 2003 stipulate the conditions in which direct marketing calls/texts are permissible. The ICO has the power to issue a monetary penalty of up to £500,000 for breach of the regulations. However, currently the ICO can only issue a monetary penalty where it can be proved that the breaching organisation's conduct is of a kind likely to cause 'substantial damage or substantial distress'.

Date	Description
	This threshold has proven problematic for the ICO. In October 2013 a monetary penalty of £300,000 issued against Mr Neibel, a joint owner of 'Tetrus Telecommunications' (which had sent unsolicited text messages on 'an industrial scale'), was overturned by the First-Tier Tribunal on the basis that the ICO failed to show that the legal threshold had been met. In June 2014, the ICO lost its appeal to the Upper Tribunal, however, the Upper Tribunal noted that, had the test been formulated in terms of 'annoyance, inconvenience and/or irritation', the case might have had a different outcome. The Government would like this standard reduced to 'annoyance, inconvenience or anxiety', with a view to making it easier for the ICO to deal with those breaking the law. The consultation will close on 7 December 2014. **Read the consultation documents here.**
Cases	
21 August 2014	***Atkinson v Community Gateway Association* UKEAT/0457/12/BA** *The facts and background* In this employment case, the Claimant claimed constructive unfair dismissal and that he had been exposed to detriment for making a protected disclosure (i.e. blowing the whistle). While investigating his conduct, the Respondents accessed his emails and discovered that he had been abusing the email system by sending overtly sexual messages to a female friend and had sought to help her obtain a position with the Respondent. He resigned before disciplinary proceedings were completed, complaining that they were being conducted in such a way as to amount to repudiatory breach. The Employment Tribunal decided that 1) the constructive unfair dismissal claim could not succeed as a matter of law because the Claimant was himself in repudiatory breach of contract 2) the Respondents' accessing of the Claimant's emails was not in breach of his rights under Article 8 of the European Convention on Human Rights and 3) the PID claim could not succeed because the Respondents were not in law vicariously liable for the employees who were said to have acted to the Claimant's detriment. The claimant appealed to the Employment Appeal Tribunal (EAT) which upheld the appeal referring the case back to be heard by a new Tribunal. The case is of data protection and privacy interest because of the remarks of the EAT about the privacy rights of an employee at work under Article 8 and the right of an employer to inspect an employee's emails.

Date	Description

The EAT Judgment – so far as it relates to the Article 8 issue

The EAT applied the guidance given by Mummery LJ in the Court of Appeal in *X v Y* [2004] IRLR 625. The EAT noted his remarks that it was not unlawful for a private employer to act inconsistently with the Human Rights Act 1998[1], but:

> 'If the dismissal of the applicant was for his "private" conduct, that will be relevant to the determination by the employment tribunal under s.98, of an unfair dismissal claim against the employer, whether or not the employer was a public authority. In either case the tribunal has to decide whether the dismissal for that reason was a sufficient reason for the dismissal and was fair.'

Mummery LJ had also said that:

> 'What is 'private life' depends on all the circumstances of the particular case, such as whether the conduct is in private premises and, if not, whether it happens in circumstances in which there is a reasonable expectation of privacy for conduct of that kind.'

The EAT following Mummery LJ's guidance found that the Employment Tribunal ought to have been referred to and would then have considered *X v Y*, but in that case would inevitably have found that there was no improper interference with the Claimant's private life, for he had used the employer's email system in clear breach of its email policy. It was 'untenable' to argue that the reliance in disciplinary proceedings by the employer on the emails which they had found was a breach of his Article 8 rights.

The Claimant argued that he had a 'reasonable expectation of privacy' in relation to the emails because of their sexual content. He relied, *inter alia* on *CC v AB* [2008] 2 FCR 505 and *Peck v UK* [2003] ECHR 44647/98 in which that court said:

> 'Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by art 8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature...'

The Information Commissioners Office "Employment Practices Code" published in 2005 was also cited to the EAT, but it found that it did not assist the Claimant because the Code 'contemplates that an employer may check emails sent by a particular worker in order to ensure the security of the system or to investigate an allegation of malpractice: see page 66.'

[1] NB Readers should note that Mummery LJ went on to say that 'it would not normally be fair for a private sector employer to dismiss an employee for a reason, which was an unjustified interference with the employee's private life.' He accepted that in employment cases s. 98(4) of the Employment Rights Act 1996 should, by virtue of s 3 Human Rights Act 1998, where possible be read compatibly with Article 8 ECHR, an approach that has more recently been followed by the Court of Appeal in *Turner v East Midlands Trains* [2012] EWCA Civ 1470. Consequently, the fact that the employee could not directly enforce Convention rights against an employer would be immaterial. Bear in mind also that an individual might have a right of action against any person – whether or not a public authority - for breach of privacy see *Campbell v Mirror Group Newspapers Ltd* (2004) UKHL 22, (2004) 2 AC 457.

Date	Description
	The EAT quoted lengthy extracts from the employer's email policy, of which the Claimant was the author. The Claimant, said the EAT, must have been aware of the policy which made it clear that emails might be accessed and consequently he could have no reasonable expectation of privacy. 'It is true,' conceded the EAT, 'that the European Court of Human Rights (in *PG and JH v UK* [2001] ECHR 44787/98) said that a person's reasonable expectations as to privacy might be a significant though not necessarily a conclusive factor; but we do not read that judgment as holding that Article 8 rights may be breached even where there is no reasonable expectation of privacy.' Consequently, the EAT went on to conclude that, 'We have not seen anything in the authorities which suggests that Article 8 may be deployed where there is no reasonable expectation of privacy.' Could the emails be used in disciplinary proceedings? The EAT dealt with this point very shortly: 'Nothing which we were shown in either the Act (the Data Protection Act 1998) or the Code (the Commissioner's Employment Practices Code) would have rendered it unlawful for the Respondents to act as they did. Once the emails to which objection was taken were found, without any infringement of the Claimant's Article 8 rights for the reasons we have set out earlier, we can see no basis on which it could be said that those emails, which were blatantly in breach of the Respondents' policy, could not be used in disciplinary proceedings.' Could the emails be used in disciplinary proceedings if they had been obtained in breach of the Claimant's Article 8 rights? The EAT considered written submissions from the parties and on the authorities concluded that in such a case a Tribunal has 'in deciding the admissibility issue which we have identified, to carry out a balancing exercise which will involve consideration of all relevant factors, including the probative value of the evidence in question and the nature and extent of the activity, which has infringed the right of privacy.' EAT's Conclusion For the Article 8 reasons and other matters not dealt with in this note the claims were remitted for re-hearing by a freshly constituted Tribunal. **Read the full judgment here.**
Europe	
CJEU	
13 October 2014	**Unforgettable that's what you are – Google Spain revisited** *by Anya Proops of 11KBW Chambers. This article was first published on the Panopticon blog on 13 October 2014 (www.panopticonblog.com).* The debates over whether the CJEU's judgment in Google Spain represents an unjustified attack on free speech rights have raged for

Date	Description
	months now. Interestingly, it seems that some judges at the local level at least are proving somewhat resistant to this highly privacy-centred judgment. Thus, according to online reports, in recent weeks a Dutch preliminary court has apparently held that a man convicted of a serious offence dating back over some years could not rely on Google Spain to have the links to websites referring to the offence excised. According to reports about the judgment (which seems only to be available in Dutch), the court held that information revealing that someone has committed an offence has relevance notwithstanding its vintage and, as such, should not be de-indexed by Google (see here). Outside of Europe, a judge sitting in the Israeli magistrate's court has apparently refused to countenance a claim against Google based on the so-called right to be forgotten. According to a report in the Israel Hayom online newspaper, the judge held that imposing an obligation on Google to de-index results, even if they were defamatory, would entail converting Google unjustifiably into a 'super-censor' (see the report here). It will be interesting to see how the English courts, with their strong tradition of upholding free speech rights, will in due course seek to navigate their way through the challenging jurisprudential landscape set by the CJEU in Google Spain. **Read the blog post on the Panopticon website here.**
28 October 2014	**Questions on dynamic IP addresses referred to the CJEU** The Federal Court of Justice of Germany - the ***Bundesgerichtshof*** **(BGH) –** has referred two questions on interpretation of the Data Protection Directive (95/46/EC) to the CJEU. The references arise from a case in which an individual is seeking an injunction, preventing the Federal Republic of Germany from storing dynamic IP addresses of website users. Access to the majority of the Federal Republic's publically available internet portals is recorded in log-files for security and enforcement purposes. The information stored beyond the end of the user's online activity includes: the name of the page downloaded, the date of the request and the IP address of the user's computer. The two questions that have been referred to the CJEU are: 1. Does an IP address stored by a service provider in the context of accessing a website amount to personal data, despite the fact that only a third party with its additional knowledge can identify said person? 2. If such IP addresses do constitute personal data, is Art. 15(1) of the Telemedia Act (which states that, where consent has not been obtained, a service provider may collect and use the personal data of a user only to the extent necessary to enable use of, and charging for, the telemedia) compliant with the Data Protection Directive (which offers greater scope for the collection of personal data where there is no consent). **Read the full press release (available in German only) here.**
EDPS	
21 October 2014	**A new European Data Protection Supervisor (EDPS) – Some Progress**

Date	Description
	The LIBE Committee of the European Parliament has chosen Giovanni Buttarelli, the current Assistant EDPS, to be the new EDPS in succession to Peter Hustinx. Wojciech Wiewiorowski, head of the Polish Data Protection Authority, was selected as Assistant Supervisor. This is not the final decision. The European Parliament has to approve the committee's proposal in a plenary vote and the Parliament's decision has then to be agreed to by the Council of Minister. This process will take some weeks. **Read the press release here.**
Article 29 Working Party	
23 September 2014	**Google's Privacy Policy: compliance measures issued** Article 29 Working Party (WP29) has recommended a range of compliance measures for Google to better meet its obligations under the Data Protection Directive (1995/46/EC), following an investigation into Google's consolidated privacy policy where the French and Spanish data protection authorities imposed fines of EUR150,000 and EUR900,000, respectively, for failure to comply with national data protection laws. The Dutch, Italian and Hamburg data protection authorities have also found the policy to be in breach of their national laws, while the UK Information Commissioner's investigations are still ongoing. The measures include: • adopting a multi-layered approach to the presentation of its privacy policy (i.e. first layer being a the general policy; second layer, the "service specific" policy; and third layer, the "in product notice"); • ensuring that its privacy policy is immediately visible and accessible via one click on each service landing page; • including important new processing activities in its privacy policy instead of in its terms of service; • obtaining user consent prior to processing; • informing users of any new recipients of their personal data ("and our partners" is too vague) and how their personal data will be used; • avoiding indistinct language such as "we may ...", and rather saying, for example, "if you used services A and B, we will ..."; • providing users with tools to manage and control the use of their data between its services; • defining its data retention policies; and • providing clear, internal policies for its employees to follow. The WP29 has said that it may in the future issue guidance on specific issues to the industry at large. **Read the WP29's letter here and appendix (detailing possible compliance measures) here.**

Date	Description
Other	
18 September 2014	**The European Commission: The Right to be Forgotten"** The European Commission issued a "myth-busting factsheet" on the much debated "right to be forgotten" on 18 September 2014. This right was considered in relation to search engines in the CJEU's (Court of Justice of the European Union) decision earlier this year in *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-131/12) (the *Google Spain* case). The factsheet aims to put right the "exaggerated and simply unfounded" concerns that have arisen out of the *Google Spain* case: • **Myth**: The judgment does nothing for citizens. **Fact**: "The right to be forgotten is about making sure that… people themselves decide what information is available about them online"; • **Myth**: The judgment entails the deletion of content. **Fact**: "The Court's judgment only concerns… search engine results involving a person's name. This means that the content [on the web page] remains unaffected by the request lodged with the search engine"; • **Myth**: The judgment contradicts freedom of expression. **Fact**: The right to be forgotten must always be "balanced against other fundamental rights, such as the freedom of expression and of the media – which are not absolute rights either… the company running the search engine must assess requests on a case by case basis"; • **Myth**: The judgment allows for censorship. **Fact**: "The right to be forgotten does not allow governments to decide what can and cannot be online or what should or should not be read"; • **Myth**: The judgment will change the way the internet works. **Fact**: "The internet will remain an important source of information as content will remain in the same location…The way search engines function will also remain the same"; and • **Myth**: The judgment renders the data protection reform redundant. **Fact**: "The reform includes an explicit right to be forgotten. It is a fundamental modernisation of the rules". **Read the full factsheet here.**

Date	Description			
UK Enforcement				
Date	**Entity**	**Enforcement notice, undertaking, monetary penalty, or prosecution**	**Description of Breach**	**Summary of steps required (in addition to the usual steps)**
1 October 2014	EMC Advisory Services Limited ('**EMCAS**')	Monetary Penalty Notice	EMCAS makes direct marketing calls to consumers relating to claims handling and mis-sold financial products. Between 1 March 2013 and 28 February 2014, the TPS and ICO received a total of 630 complaints from subscribers to the TPS who had received unsolicited direct marketing calls from EMCAS. Using, or instigating use of, a public telecommunications service for the purpose of making unsolicited direct marketing calls to TPS subscribers (who have registered with TPS at least 28 days before the call and have not given prior consent to receive calls) breaches reg. 21 of PECR. The ICO was satisfied that EMCAS's contraventions were 'serious' (as required by s. 55A(1)(a)) as, in particular, the calls were on-going and repeated, despite recipients making clear that they did not wish to be contacted and that numbers were TPS registered. Further, EMCAS appeared in the TPS top 10 most complained about organisations in the 12 month complaint period (despite correspondence and meetings between the ICO and EMCAS). The ICO was satisfied that the contraventions were of a kind likely to cause substantial distress (as required by s. 55(1)(b)) given the number and nature of complaints received. The evidence also included evidence of the impact of the calls.	Monetary penalty of £70,000.
8 October 2014	South Western Ambulance	Undertaking to comply with the First, Third and	The Commissioner was informed that seven discs containing personal data of 45,431 patients were shared with a Clinical	SWAST must: • Undertake and document a

Date	Description			
	Service NHS Trust ('**SWAST**')	Seventh Data Protection Principles in Part I Schedule I of the Act.	Commissioning Group ('CCG') by SWAS. Some of the information on the discs related to health of the data subjects so was sensitive personal data. The CCG received the discs safely (sent by recorded delivery to a specific member of staff), however, CCG found that the discs were not encrypted which presented a potential security risk. The Commissioner also found that: • Monitoring of staff data protection training was lacking; • There was no justifiable legal basis for CCG to have access to the patient data; • No information sharing agreement was in place; and • CCG had requested additional data fields which put SWAST at risk of providing excessive information. CCG's request had not been properly considered.	Privacy Impact Assessment relating to its data sharing with any organisation; • Ensure appropriate information sharing agreements are in place and maintain/review a register of such agreements; • Amend its notification to ensure that it covers data sharing and provide a relevant privacy notice; • Ensure that all staff undertake mandatory data protection training at the outset of their employment and record/monitor such training; and • Establish a refresher-training programme.
10 October 2014	Abdul Tayyb	Enforcement Notice	In February 2014, the Commissioner reviewed complaints of unsolicited marketing communications made via the online reporting tool on the Commissioner's website. The Commissioner found that 974 complaints had been made about text messages offering assistance with PPI claims, sent or instigated by Mr Tayub. In addition, unsolicited marketing text messages can also be reported to GSMA's Spam Reporting Service. The Commissioner found that, as at June 2014, 49,645 complaints had been made about the same messages.	Mr Tayub must not: • Transmit nor instigate transmission of unsolicited communications for the purposes of direct marketing unless the recipient has previously consented; • Transmit or instigate transmission of a communication for the purposes of direct marketing by electronic mail unless Mr Tayub is clearly identified in the communication as the sender.

Date	Description			
24 October 2014	Gwynedd Council (the '**Council**')	Undertaking to comply with the Seventh Data Protection Principle in Part I Schedule I of the Act.	The Council informed the Commissioner that a social care record relating to one individual had been posted to the incorrect address, as a result of the address being handwritten and ambiguous. The Council submitted a further breach report, concerning a file (containing personal data of an individual) that had gone missing whilst being transported between offices. Both incidents occurred in the same Council department and the employees involved had not undertaken the Council's mandatory data protection training. Whilst overarching data protection policies were in place at the Council, these policies did not address transporting documents or preparing documents for sending.	The Council must: • Monitor and enforce mandatory data protection training; • Provide and monitor refresher training; and • Ensure that staff are regularly reminded of the Council's policies on transportation, exchange and use of personal data and are trained to follow such policies.
24 October 2014	Disclosure and Barring Service ('**DBS**')	Undertaking to comply with the First Data Protection Principle in Part I Schedule I of the Act.	Under s 42 of the Data Protection Act, any person affected by processing of personal data can request that the Commissioner make an assessment of whether it is likely that the processing is being carried out in compliance with the DPA. The Commissioner considered two such requests concerning DBS's application form. Question e55 of the form asked the applicant: *Have you ever been convicted of a criminal offence of received a caution, reprimand or warning?* This wording fails to reflect recent 'filtering' provisions allowing minor cautions and convictions information to be omitted from the application form. In March 2014, DBS undertook to amend e55 and to provide supplementary information on filtered matters to applicants and employers, among others. The DBS undertook to ensure that the supplementary informed provided continued to be current, accurate and relevant.	DBS must: • Ensure that, as soon as practicable (by 31 December 2014 at the latest), legacy application forms are either rejected or removed from circulation; and • Provide fortnightly updates to the Commissioner on progress.

Date	Description	
		However, the Commissioner found that unaltered versions of the application form remain in circulation as many third party organisations continue to use legacy application forms. The Commissioner determined that this could amount to unfair processing of conviction/caution information (which is sensitive personal data).