Harbottle & Lewis

9 February 2017

# The latest on Trump, GDPR prep, proposals for a new E-Privacy Regulation and recent lessons learnt


**BUSINESS CONTACTS**

**Daniel Tozer**
Partner
daniel.tozer@harbottle.com

**Jeremy Morton**
Partner
jeremy.morton@harbottle.com

**Jo Sanders**
Partner
jo.sanders@harbottle.com


Welcome to our first eBulletin of 2017. We've made it through what's been an eventful January from both a political and data and privacy perspective. In this eBulletin we reflect on some of the key developments since October 2016.

## Trump attacks Privacy Shield?

Trump's executive order on immigration has led to some voicing concerns that it calls into question the ongoing status of the 'EU-US Privacy Shield' and the 'EU-US Umbrella Agreement'. The particular wording in question reads: "Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information." Looking at the wording, there doesn't appear to be cause for concern – for now. As the EU-US Privacy Shield doesn't offer EU citizens protections under the Privacy Act but by other means and the EU-US Umbrella Agreement (relating to the exchange of law enforcement data) is implemented in the U.S. by the Judicial Redress Act, the executive order does not exclude EU citizens from the protections of the Privacy Act as guaranteed under the EU-US Umbrella Agreement. That said, Trump's executive order could mark the start of a change of U.S. policy regarding privacy rights of non-US citizens under the new US administration and so we will continue to keep an eye on developments.

## General Data Protection Regulation (GDPR) – keep calm and carry on … your preparations

For reasons discussed in an earlier eBulletin, it was always highly likely that the new European data regime, known as GDPR, would still apply in any Brexit scenario. But don't just take our word for it… unsurprisingly the UK government has now made explicitly clear that come May 2018 the UK will be adopting the GDPR.

## First official (but draft) GDPR guidelines issued

The Article 29 Working Party (A29WP), has finally published it's first set of draft 'Opinions' addressing three aspects of the GDPR: 'Data Protection Officers', 'Data Portability' and 'Lead Supervisory

Authorities'. While eagerly anticipated, in some respects the Opinions raise more questions than answers. One particularly interesting point to take note of in relation to the Opinion on Data Protection Officers is that if you voluntarily appoint a 'Data Protection Officer' where one is not mandatory, the provisions of the GDPR that would apply if a Data Protection Officer were mandatory apply regardless. Be careful giving anyone the title of 'Data Protection Officer' or similar.

We can expect to see further GDPR guidance documents on administrative fines, high risk processing and data protection impact assessments, certification, profiling, consent, transparency, notification of data breaches and tools for international transfers. The Information Commissioner's Office (ICO) continues to play an active role in the A29WP group but has confirmed that, where appropriate, it will also publish its own additional advice to explain anything particularly relevant to the UK. We have been told to expect ICO guidance on both 'contracts and liability' and 'consent' in early 2017.

## E-Privacy Directive reforms announced

The E-Privacy Directive is the piece of European law from which our UK laws relating to cookies, electronic direct marketing and security of communications data all derive. It has long been criticised for being ineffective. The Commission's proposed reforms were published on 10 January 2017.

The current proposals are obviously early stage drafts and highly likely to be subject to change following reviews by the EU Parliament and Council, but some of the current headline changes will undoubtedly be of interest.

The current proposal is that a new E-Privacy Regulation should be implemented at the same time as the GDPR (25 May 2018), meaning that the proposed changes would have direct effect in the UK before the UK leaves the EU. Second, consistent with the aim to align the E-Privacy Regulation with the GDPR, the Regulation borrows the same sanctions regime that exist under the GDPR with the highest fines under the Regulation (i.e. the greater of 4% of worldwide turnover and €20million) being available for breaches of the security of communications obligations. Third, the security of communications obligations will be extended to apply to a broader definition of communications services, now to include over-the-top communications services such as email and instant messaging services like WhatsApp, Skype and even gaming messaging services. Fourth, it has been clarified that there will be no need to obtain user consent to use first party cookies (i.e. cookies not operated by a third party) for analytics or operational purposes.

Controversially, website browser operators will now be tasked with responsibility for obtaining opt in consent to the use of any other cookies. This may lead to a significantly reduced number of people consenting to the use of cookies and therefore negatively impact online advertisers reliant on behavioural monitoring cookies. We'll be keeping a close eye on the proposed reforms and will keep you

updated.

## UK's "Snooper's Charter" found incompatible with the European Charter of Fundamental Rights

The UK government lost the case brought against the Investigatory Powers Act 2016 by two MPs, David Davis and Tom Watson. The European Court (CJEU) found that the general and indiscriminate retention of citizens' personal data "cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the Charter [of Fundamental Rights]". The Court did, however, approve of specific and targeted data retention as a means of fighting crime and terrorism. It's now likely that the government will have to revisit the relevant provisions of the Act to bring them in line with the ruling.

## CJEU decides that dynamic IP addresses *may* be personal data

In a landmark case decided at the end of last year, the CJEU decided that 'dynamic IP addresses' (i.e. IP addresses assigned by a network and likely to change over time) held by a data controller may amount to personal data, even when only a third party is able to make the identifying link between the IP address and the data subject. The Court found that this is only the case where the third party's means to make the identifying link is 'likely reasonably to be used'– for example, if such use were prohibited by law, then the dynamic IP addresses would not constitute personal data.

It has long been accepted that static IP addresses (i.e. IP addresses which do not change) constitute personal data but this case stretches the definition of personal data. In practical terms, the case is unlikely to have a significant impact for responsible data controllers already treating IP addresses as personal data, however, it nevertheless signals the increasing tendency to treat the definition of personal data very broadly.

## Northern Irish Court of Appeal rules on Facebook's liability for UGC

In *CG v Facebook*, the Northern Ireland Court of Appeal held that Facebook Ireland Ltd (an Irish company which hosts and operates the Facebook website outside of North America) is a data controller established in the UK for the purposes of the Data Protection Act 1998. It followed the reasoning behind the well-known Google Spain case, in a move which is significant for the social media giant. The decision also examines the complex questions around notice and takedown for website operators providing hosting services, and while the Court rejected Facebook's submission that complainants should be required to notify only via Facebook's online reporting tools it did appear to require a high level of specific detail to be included in a complaint before an operator would be fixed with notice.

## Lessons learnt from recent ICO enforcement action

The ICO recently indicated that it intends to fine 11 charities for breaching data protection laws in the latest developments in the

ICO’s ongoing investigations into the charity sector’s data practices launched in 2015. Several charities found themselves on the receiving end of ICO enforcement action only at the end of last year when the ICO found that a number had been improperly sharing and analysing donor data for the purposes of profiling and targeting of communications

The ICO continues to hand out hefty fines to companies sending unsolicited text messages, with Nouveau Finance Limited being ordered to pay £70,000 for sending 2.2 million of them and LAC Media Limited £50,000 for sending 400,000.

Royal & Sun Alliance Insurance PLC was also fined £150,000 for a breach of the data security obligations, following the loss of personal data of nearly 60,000 people.