Published on *The National Law Review* https://natlawreview.com

Top 10 International Privacy Developments of 2014

Article By:

Daniel P. Cooper

1. **The CJEU "Right to be Forgotten" Ruling**. In May 2014, the Court of Justice of the European Union (CJEU) delivered an important judgement in a referral from Spain's National High Court involving Google, a Spanish national, and the Spanish data protection authority (Case C-131/12). The CJEU's decision re-interpreted European data protection law to include a so-called "right to be forgotten" that enabled individuals to request search engines to block links that appear on searches of their names if the links go to information that is incomplete, inaccurate, irrelevant, or otherwise damaging to an individual's privacy. (This right is limited in the case of public figures, however.) The decision also found that Google was subject to European data protection law because it operated subsidiaries in Europe whose business was to raise advertising revenues in relation to the search engine's data processing activities. The decision triggered an immediate tidal wave of tens of thousands of requests to Google and other search engines that continues to raise controversies to this day.

2. **CJEU strikes down the Data Retention Directive as invalid.** In April 2014, the CJEU took the rare step of annulling the controversial Data Retention Directive, which mandated the systematic ("bulk") retention of communications metadata by telecommunications companies in the EU, for potential access by law enforcement authorities (see our blog post here). The Court criticised the Directive's indiscriminate targeting of suspects and non-suspects alike, and the law's general lack of safeguards, finding that it amounted to an "interference with the fundamental rights of practically the entire European population" contrary to Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The Directive's invalidation raised questions about the continuing validity of the national laws that had implemented the Directive throughout the EU. In the UK, this lead to the accelerated adoption of substitute legislation, the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), and its implementing regulations.

3. **Safe Harbor Under Review.** 2014 saw a continuation of the uncertainty around the future of the EU-U.S. Safe Harbor Agreement. In March 2014, the European Parliament voted to suspend the Agreement as a result of Edward Snowden's revelations on the mass surveillance carried out by the U.S. Government. Following on from the Parliament's vote, the Trans-Atlantic Business Dialogue continues to negotiate the areas where the Safe Harbor

Agreement can be improved, as detailed in our blog post here. The dialogue seeks to reach agreement on 13 areas of potential improvement proposed by the European Commission in its report of 2013. Eleven out of the 13 recommendations were close to final agreement by end of 2014; the final two are the most contentious, as they involve the activities of U.S. intelligence agencies. The uncertainty was reiterated by Andrus Ansip, Vice-President for Digital Single Market, who said he might be willing to suspend the Agreement unless the security of EU citizens' data could be guaranteed by the U.S. Looking ahead, the CJEU is expected to examine the legality of the Safe Harbor Agreement in 2015 following a referral from Ireland's High Court of a case brought by privacy activist Max Schrems against the Irish Data Protection Commissioner effectively challenging the validity of Safe Harbor in Europe in relation to transfers from Facebook Ireland to Facebook's U.S. parent company.

4. **Russia's New Data Localization Rules.** On July 21, 2014, Russian President Vladimir Putin signed into law an amendment to the Russian Federal Law on Information, Information Technology and Information Protection (Law No. 152). The amendment introduced a range of new provisions into Law No. 152, including a requirement for data relating to Russian citizens to be physically stored and processed in Russia (a data localization requirement). However, the scope of the amendment — including the scope of organizations that must comply with the data localization requirement — is unclear, and its practical requirements remain to be determined. Although Russia's data protection authority (Roskomnadzor) has argued that the data localization requirement does *not* restrict cross-border transfers or the outsourcing of processing operations outside of Russia, it remains to be seen how the rule will be applied in practice. This remains to be confirmed by official guidance, expected to be issued by Roskomnadzor during spring 2015. The amendment, originally scheduled to come into force on September 1, 2016, has now been accelerated and will come into force on September 1, 2015.

5. **Increased Enforcement of Data Protection Rules Across the EU.** In 2014, European DPAs adopted an increasingly proactive approach to enforcement. For example, the French DPA (the CNIL) imposed a €150,000 fine on Google for breach of applicable notice and consent requirements relating to Google's 2012 Privacy Policy, among other violations. More recently, in December 2014, the Dutch DPA issued an order against Google specifying measures Google must implement to comply with Dutch data protection law. Failure to comply with the Dutch DPA's order can result in fines ranging from €20,000 to €5 million per day per non-executed measure. The expected maximum fine could reach €15 million. Italy and Germany also have issued a range of non-monetary penalties against Google. Separately from Google, the Spanish DPA handed out the first fines in the EU for infringement of the cookie rule (or Article 5(3) of the European e-Privacy Directive 2002/58/EC). The Spanish DPA imposed a €5,000 fine on two jewellery companies for failure to provide comprehensive information to visitors of their promotional websites.

6. **Data Protection Reform Continues to Progress.** During the course of 2014, the European Union institutions moved further towards agreeing a framework for the General Data Protection Regulation (the GDPR). In March 2014, the European Parliament endorsed its significantly amended GDPR proposal, which contained stronger privacy safeguards, increased fines, and some significant changes to key definitions. Since then, the Council has reached partial "general approaches" on a number of chapters of the regulation, including on

international transfers, and it is hoped that further general approaches covering all of the relevant issues may be reached by the summer of 2015. Despite the progress that was made during 2014, however, it is not anticipated that agreement will be reached on the GDPR before mid-2016. For a comprehensive overview of the development of the GDPR to date, see our previous InsidePrivacy blog post here.

7. **CJEU judgment on scope of "household exemption" to Data Protection Directive (the CCTV case).** In December 2014, the CJEU ruled that owners of personal surveillance cameras could be breaching the EU Data Protection Directive 95/46/EU (the Directive), when those cameras are used to monitor public spaces (for more details, see our blog post here). The ruling came following a referral from the Czech Supreme Court, which was required to decide whether an individual's use of a video camera outside his home to protect his property and his family's safety against intruders could be considered to fall within an exception contained in the Directive for processing activities "in the course of a purely personal or household activity." The CJEU found that: (i) the recording of individuals in a public space constitutes the processing of personal data, and (ii) the exemption in the Directive did *not* apply because the notion of a "purely personal setting" must be interpreted strictly and narrowly in light of the rights of privacy that individuals are guaranteed in the European Union. The case is due to go back to the Czech Supreme Court in 2015, who will need to weigh up the rights of privacy of those being recorded against the interest the individual has in protecting his property and his personal security.

8. **New European Data Protection Supervisor.** In November 2014, Giovanni Buttarelli was appointed as the next European Data Protection Supervisor (EDPS), the data protection watchdog and independent advisor to the various rulemaking and supervisory bodies that make up the EU. Mr Buttarelli replaced Peter Hustinx, under whom he served as Deputy EDPS. Mr Buttarelli will take an active role in the ongoing reform of the General Data Protection Regulation. Once the Regulation is adopted, Mr Buttarelli will also likely head the newly created European Data Protection Board (EDPB), which will replace the Article 29 Working Party (WP29). The EDPB's role will likely be to promote cooperation among the EU's data protection authorities, including the coordination of joint operations, and strengthen the dialogue with relevant stakeholders. (Note that the EDPS' role may evolve further, if new revisions are introduced to the draft Regulation before its adoption.)

9. **ISO/IEC 27018: A New Code of Practice for the Cloud.** In the summer of 2014, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) adopted ISO/IEC 27018 – a voluntary international code of practice governing the processing of personal information by cloud service providers. The standard builds on existing international information security standards, such as ISO 27001 and ISO 27002, which set out general information security principles (e.g., securing offices and facilities, media handling, human resources security, etc.). But ISO 27018, in contrast, is tailored to cloud services specifically. The code of practice requires that cloud providers (among other things): help cloud customers comply with individuals' access rights; process personal information only in accordance with the customer's instructions; only process personal information for marketing or advertising purposes with the customer's express consent; help customers manage access controls; offer various security tools (e.g., cryptographic protection); notify data breaches; and subject their services to independent

information security reviews. A number of cloud companies are expected to seek certification under ISO 27001, with ISO 27018, controls in the course of 2015 to increase transparency of their data processing practices and reassure customers.

10. **New Data Protection Legislation Around the World**. The number of countries adopting new data protection laws continued to grow throughout 2014. For example, Singapore saw the main data protection rules contained in its Personal Data Protection Act 2012 (PDPA) and enacting regulations go into effect on July 2, 2014. Australia also adopted new rules in March 2014. These introduced a new, unified set of 13 privacy principles known at the Australian Privacy Principles (or APPs) and aim to update and future-proof Australia's privacy framework. The APPs also strengthen the Australian Commissioner's enforcement powers. Brazil is also making progress. Despite the uncertainties around its Data Privacy Bill, Brazil made positive steps in the privacy space by enacting the "Marco Civil da Internet" (which came into effect on June 23, 2014), also known as the "Internet Law". The Marco Civil is significant in that it specifically applies – for the first time – a number of existing civil (consumer protection) and constitutional privacy/data protection rights to most of the Internet sector. As a result, Courts already have experience applying these provisions, even though the act itself is new. South Africa, Turkey, and Chile also have data privacy laws in the pipeline, although it is unclear when these will come into force.

National Law Review, Volumess V, Number 35

Source URL:https://natlawreview.com/article/top-10-international-privacy-developments-2014