Weil

Alert
Technology & Intellectual Property

Key Technology and Privacy Trends for 2016

Barry Fishley

2016 is set to be a year of change with the introduction of a raft of legislation which will impact all organisations, including most notably, technology-focused companies. Of particular note will be the much-awaited General Data Protection Regulations and the Network and the Information Security Directive ("**NIS Directive**").

General Data Protection Regulation ("GDPR")

In 2012, the European Commission issued a proposed revision of the data protection legal framework in the form of the new GDPR with the purpose to "*strengthen online privacy rights and boost Europe's digital economy*", along with promises to save billions of Euros in administrative costs through harmonisation. The reform package was agreed on 15 December 2015 and will be formally adopted in early 2016.

Key changes include:

- **Expansion of scope:** many non-EU businesses that are not subject to the current Directive will be required to comply with the GDPR if they are offering goods or services to EU citizens or monitoring their behaviour. It also introduces direct compliance obligations on data processors including, among others, providers of cloud services.
- **Stronger enforcement powers:** the GDPR will increase the maximum fine an organisation can suffer in the event of a serious data protection breach to the higher of €20 million or 4% of the organisation's total worldwide annual turnover.
- **Consent will become more difficult to obtain:** consent cannot be implied, it must be freely given, specific, informed and unambiguous.
- **Data Security:** these obligations will apply to both data controllers and data processors. There is a new universal obligation to notify regulators of a data breach which is likely to result in risk without undue delay and, where feasible, within 72 hours. This is accompanied by stricter data breach notification requirements to notify relevant individuals without undue delay where the breach poses a high risk to them.
- **Administration and governance:** both controllers and processors must maintain documentation covering all processing; this will replace the current obligation to register or notify with the local regulator. Further, a data protection officer must be appointed for organisations that regularly and systematically process data on a large scale as part of their core activities, such as an insurance company.
- **Right to be forgotten (i.e. for the data to be erased):** this has been enhanced, which may result in requisite costly changes to IT systems.
- **New data protection impact assessments:** the GDPR requires protection impact assessments to be conducted at the outset for any new technologies that involve processing personal data.

A key advantage of the proposal is that businesses will be able to deal with one single data protection authority as a "lead authority" across the whole of the EU.

Next Steps

We believe organisations should be undertaking the following actions in light of the GDPR:

- organise cross-departmental teams (which should include IT, marketing, finance, HR and

legal/compliance) to oversee the compliance program;
- assess the current level of compliance, including the use of standards (e.g. ISO27001) and codes of practice;
- identify all data flows (i.e. understand how and where personal data is used);
- start to document these data flows and uses and prioritise data at most risk (e.g. customer data);
- 'future proof' the procurement of new systems/applications so as to comply with individuals' right to be forgotten;
- check insurance position so as to ensure that both scope and amounts cover cyber security risk;
- if a processor, review and possibly renegotiate customer contracts; and
- consider linking with 'favourable' supervisory authority by ensuring processing decisions are in a 'friendly' country.

Replacement of US-EU Safe Harbour – 'Privacy Shield'

On 2 February 2016, the European Commission announced that the European Union had agreed a new framework for the export of personal data to the United States, provisionally known as the "EU-US Privacy Shield". The new framework replaces the safe harbor framework which was declared invalid by Europe's highest court in 2015.

Key Proposals

The full texts of the EU-US Privacy Shield will be published in a few weeks' time and there remain a number of significant question marks over the effectiveness of the data transfer deal. However, the key features of the new framework are expected to include a US commitment to limit access to European citizens' data by intelligence agencies, enhanced Federal Trade Commission monitoring and enforcement powers and the creation of a dedicated privacy ombudsman.

The EU-US Privacy Shield will not become effective until the European Commission has issued a supporting adequacy decision, which is expected in the coming weeks.

In the interim, we recommend that organisations exporting data to the US which previously relied on safe harbor continue to adopt alternative measures which are currently permitted (acknowledging that these may also be assessed), such as the execution of "model clause" data transfer agreements and/or binding corporate rules.

Privacy Litigation

In 2016 we will see an increase in privacy claims.

Historically, litigation has been relatively rare, owing principally to the low quantum of damages awarded in successful cases and the need to prove financial loss in order to claim compensation under section 13 of the Data Protection Act 1998 ("**DPA**"). However, as a result of the Court of Appeal decision in *Vidal-Hall v Google*[1] that proof of pecuniary loss is not necessary to bring claims for damages and the approval by the High Court of a group privacy litigation order against Morrisons, the historic high bar to individual claims has been significantly lowered.

A successful class action could result in the award of substantial damages in aggregate, fundamentally changing the financial risk presented from individual claims brought under section 13 of the DPA.

Cyber Security and the NIS Directive

We have already witnessed further high profile cyber attacks this year and this is expected to continue. The final text of the NIS Directive (the "Cyber Security Directive") will be published in the Spring and will introduce a number of well-conceived obligations aimed at ensuring a high common level of security of networks and information systems across the European Union.

The NIS Directive will create a framework for national and pan-European information sharing with operators of "essential services" and providers of "digital services" obliged to report major security incidents. Amongst the organisations that are expected to fall within the scope of legislation implementing the NIS Directive are high level domain name registries, stock exchanges and app stores.

The NIS Directive is subject to a 21 month implementation period, which means the provisions of the NIS Directive are unlikely to affect organisations until 2018. However, there will be considerable preparatory work to be undertaken by organisations subject to NIS Directive obligations which we expect to commence this year.

Brexit

The UK's relationship with Europe will remain precarious, regardless of whether it leaves or remains in the European Union.

Following David Cameron's reform package agreement with Europe, Britons will head to the polls in 2016 to decide whether or not the UK should leave the European Union. If Britain votes to leave the EU, the Brexit would be prefaced with a two year transitional period during which the complex legal dissociation with Europe would need to be addressed.

During that period, the scope of European Regulations would need to be analysed and in many cases replaced with national legislation covering the subject matter of the relevant Regulation to avoid the creation of legal vacuums. The government would also be at liberty to repeal or amend national legislation

implementing European Directives (with such laws not automatically ceasing to have effect in the event of a Brexit).

We expect that the Data Protection Act 1998 (which implements EU Directive 95/46/EC) would remain in force broadly in its current form with the UK electing not to optionally strengthen individual rights (such as the introduction of a statutory "right to be forgotten") in line with the recently finalised EU General Data Protection Regulation.

Community trade marks would cease to provide protection within the UK. Accordingly, the UK may elect to voluntarily recognise community trade marks and afford such trade marks the same protection as national UK marks, and/or introduce a process permitting the fast-track conversion of existing community trade marks to UK national marks.

Other areas such as e-commerce, cookies and notice and take-down orders which originate from EU Directives are unlikely to be initially repealed or substantially amended following Brexit in light of their generally modest compliance burdens and the existing measures which organisations have taken to comply with the existing laws.

The Digital Single Market strategy

In May 2015, the European Commission announced its plans for the creation of a Digital Single Market ("**DSM**"). The aim of the DSM is to remove existing barriers which currently prevent organisations from delivering their digital goods and services across the EU. The Commission aims to deliver 16 initiatives of the DSM by the end of 2016 and claims that a successfully implemented DSM could contribute €415 billion per year to Europe's economy. However, with hurdles such as competition law, geo-blocking, tax, copyright and data protection to contend with, we suspect the timetable for implementing the initiatives will slip considerably.

Key reform	Explanation and Timeline
New European copyright framework	The Commission believes Europe needs a more harmonised copyright regime which provides incentives to create and invest whilst promoting transmission and the consumption of content across borders. The Commission sees the territoriality of copyright and difficulties associated with clearing of rights as a major barrier to cross-border access to copyright-protected content services which it seeks to remove by reducing the differences between national copyright regimes. This will be achieved by harmonising the permitted exceptions to copyright, particularly in respect of research and education. The Commission is also intending to introduce an exception for commercial/non-commercial text and data mining. The Commission will review the Satellite and Cable Directive and assess whether the "country of origin" principle, which allows broadcasters to broadcast to the whole of the EU once rights are cleared in the country of origin, should be extend to cover broadcasters' online transmissions.
Preventing unjustified geo-blocking	The ability for online providers to deny access to digital services based on Member State residency, or to offer different prices on the basis of geographical region will be restricted if they cannot be justified. The Commission recently announced its first concrete proposals to tackle unjustified geo-blocking in the form of a Regulation 'on the cross-border portability of online content services' (see below).
Further harmonisation of e-commerce legislation	The rules which apply to cross-border transactions can be complex and differ between Member States. Certain areas of consumer law have already been harmonised, but others such as remedies for defective digital content purchased online remain untouched. The Commission seeks to harmonise, simplify and modernise e-commerce legislation. Measures are also planned to ensure greater co-operation between national enforcement agencies in tackling infringements on online markets. Two new Directives have been proposed by the Commission: ■ Directive concerning contracts for the supply of digital content; and ■ Directive concerning contracts for the online and other distance sales of goods, along with a plan to produce a "health check" report on the full spectrum of consumer law Directives by 2017.

Regulation on the cross border portability of online content services

What do the proposals aim to do?

The Regulation focuses on removing restrictions which prevent EU citizens who have paid for online services in their home country from being able to access such services when temporarily present in a different Member State.

The Regulation will apply to all providers of 'online content services'. This includes:

- audio-visual media services provided online on a portable basis with a function to "inform, entertain and educate the general public". Examples of audio-visual media services include Netflix and Amazon Prime Instant Video; and
- the provision of access to and use of other works and transmissions of broadcasting organisations, whether live or 'on-demand'. This includes subscription services such as Sky Sports & Movies, BT Sport, BBC iPlayer, 4oD and HBO.

What are the implications of the proposals?

The Regulation entitles subscribers to online content services in one Member State to access and use these services when 'temporarily present' in another Member State. For example, a UK subscriber to Sky Sports would be able to access the same online service whilst on holiday in Spain.

'Temporarily present' is defined very broadly to include any situation where a subscriber is present in any Member State other than the one in which he/she is resident. This has given rise to concerns that the reforms may result in customers buying cheap subscriptions from Member States where citizens pay less for such online content in order to avoid paying higher domestic subscription charges.

Consequences:

- Online content providers will be required to remove any restrictions they currently implement which prevents online services being accessed by EU citizens when travelling across Europe.
- In the absence of clear guidance on the meaning of "temporarily present", online service providers will review and possibly increase subscription charges in certain Member States (where historically rates have been lower) so as to hedge against any adverse impact on sales in higher charging Member States.
- The Regulation will not permit organisations to mitigate the Regulation's effects by changing the content or format of the services in order to reduce cross-border portability.
- Online service providers will not be obliged to meet the same quality standards of domestic subscriptions, for instance due to variances across Member States in respect of their internet capabilities.
- Businesses cannot contract out of these provisions and any contractual terms which are contrary to the obligations of the Regulation will be unenforceable.

[1] The Court of Appeal decision is currently the subject of a Supreme Court appeal.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Technology & IP Transactions Group:

Barry Fishley Bio Page barry.fishley@weil.com +44 20 7903 1410

©2016 Weil, Gotshal & Manges. All rights reserved. Quotation with attribution is permitted. This publication is provided for general information purposes only and is not intended to cover every aspect of corporate governance for the featured jurisdictions. The information in this publication does not constitute the legal or other professional advice of Weil, Gotshal & Manges. The views expressed in this publication reflect those of the authors and are not necessarily the views of Weil, Gotshal & Manges or of its clients.

The contents of this publication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome. If you require specific legal advice then please contact any of the lawyers listed above.

The firm is not authorised under the Financial Services and Markets Act 2000 but we are able, in certain circumstances, to offer a limited range of investment services to clients because we are authorised and regulated by the Solicitors Regulation Authority. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

We currently hold your contact details, which we use to send you information about events, publications and services provided by the firm that may be of interest to you. We only use your details for marketing and other internal administration purposes. If you would prefer not to receive publications or mailings from us, if your contact details are incorrect or if you would like to add a colleague to our mailing list, please log on to www.weil.com/weil/subscribe.html, or send an email to subscriptions@weil.com.