February 2017 • Volume 25 • Number 2

IT Law Today

Europe's law and practice update for specialists in information technology

Editorial

This issue starts with some predictions for 2017 from Graham Hann of Taylor Wessing which provide much food for thought as 2017 beings. This issue also includes a report that the existing eprivacy directive will be replaced by a regulation (so will have direct effect – at least in the UK until Brexit).

Courtney M. Bowman of Proskauer Rose LLP looks at various new sets of guidance from the EU's Article 29 committee on the General data protection regulation including a set relating to data protection offices (a poisoned chalice role perhaps for some).

Rosie Duckworth of Squire Patton Boggs provides further guidance on the EU geo-blocking legislation plans, a topic very relevant to those readers like *IT Law Today*'s editors with clients involved in selling on-line.

Susan Singleton

TMC Predictions 2017

Given rather unexpected developments in 2016 on both sides of the Atlantic (and I don't mean that Leicester City thing), it's harder than ever to feel confident in predicting anything, let alone developments in the TMC sector. However, it's that time of year again for some bankable predictions for 2017. So, here goes…

Chatbots on the rise

Chatbots have been creeping into the customer service industry over the last two or three years, but their use has been limited and remains, to some, unwelcome (remember Microsoft's Clippy?!). However, 2017 could see a marked increase in their application and take-up, for various reasons:

- AI capabilities are developing apace. Chatbots are becoming able to analyse and apply a deeper understanding of human behavior and language, enabling more 'human' conversations to take place;
- speech recognition is also advancing, vastly improving customer experience;
- digital assistants like Siri, Alexa, and Google Now are used more widely than ever before – people are more used to talking to machines and getting them to do what they want. It is predicted that by 2019, over 110 million consumer devices with embedded intelligent assistants will be installed in US households;
- brand-conscious consumer businesses are able to bake their brand into chatbots' characteristics and behaviour much more effectively than they can with people – code being a far more effective tool than a call script can ever be; and
- the use of messaging apps, the rails on which chatbots run, is increasing massively – second only to social media apps in terms of downloads – and the messenger providers are creating platforms to allow for bots. In April 2016, Facebook launched its bots for messenger platform, to enable businesses to "build deeper interactions with their customers on Messenger in a way that is contextual, convenient, and delightful, with control at its core."

www.singlelaw.com

IN THIS ISSUE

The rise of bots will trigger interesting data protection issues in some markets, where automated processing of data for decision making purposes is specifically regulated. Data exports will also be an issue where bot servers are housed outside Europe. Also, of course, the technology will deploy new targets for cyber criminals. Much like Uber (as discussed below) the impact may, however, be greatest in terms of employment levels in the customer service sector rather than in terms of legal issues (although ironically, Facebook's release of its bot platform ends with a statement explaining how the business is "putting people first"). $1b dollar valuations for companies like Canada's Kik, as well as the publicly stated strategies of the likes of Google and Microsoft, evidence the investability and potential of bot technology. Like Arnie, Clippy may have been defeated in his first outing, but he'll be back.

...which will be part of further growth in the wider AI sector

According to IDC, by 2019, 40% of digital transformation initiatives, and 100% of IoT initiatives, will be supported by AI capabilities. IDC also states that the top three AI use cases in terms of spending are medical diagnostics and treatment, quality management in manufacturing, and automated service agents in retail. By 2018, IDC states that 75% of developer teams will include AI functionality in one or more applications or services (last year this prediction was 50%).

The legal issues raised by the increased use of AI in society will only really become clear as the technology develops and its impact on society is felt. We mention data protection issues above, relating to automated decision making and export, but the issues being discussed currently are more philosophical – who is responsible for the action of a robot or computer platform? The answer to this question (often asked rather dramatically in the context of a criminal act) is actually rather dull – the liability will almost always lie with the person responsible for operating the robot or platform.

The keenest impact of AI may well be felt in the legal profession with law firms (like us) already investing in technology to build efficiencies and lower the cost of advice – any decision or problem to be analysed on a repeated basis, with common variables, such as a compensation claim for late delivery of goods, can be processed and the outcome achieved by a relatively simple AI tool given the right information. The shape of our profession may not dramatically change in 2017, but we predict this coming year will see a significant increase in investment in AI technology in professional services generally.

Return of the IPO market, or the Trump effect?

Is the IPO market another likely comeback? CNBC recently reported that as uncertainty around the US election passes, investors should expect some big Nasdaq IPOs in 2017. 2016 was weak at best – 80 companies listing in the first three quarters, versus 143 in 2015. Those tipped for potential 2017 listings include messaging app Snapchat, vacation rental platform Airbnb, big-data analyser Palantir, ride sharing Lyft (possibly pipping Uber to an IPO), and music streamer Spotify.

Back here in the UK, 2016 data is also depressing, and no doubt reflects Brexit-related delays. According to figures from EY, while the number of listings on both the main market and AIM increased (by 43% and 17% respectively), aggregate values fell sharply (by 56% and 83%). According to EY:

> *"The resolution of political uncertainty due to the EU referendum will see IPO activity pick up on the back of reduced volatility, rising indices and strong aftermarket performance of new IPOs…*
>
> *US and Asian investors' interest will help drive pricing, making IPOs more attractive to business leaders and their backers…*

While 2017 looks set for an IPO resurgence, longer term it is possible that the triggering of Article 50 and the renegotiation of Britain's trading relationships will drive volatility, which will impact IPO windows".

Talk of an IPO revival led by Snapchat has been countered by voices recalling the hype and expectation surrounding Facebook's listing in 2012, and the subsequent downward spiral in its share price, in market conditions which, in many ways, were similar then to those now. Also, the Trump presidency is cited by some as very bad news for Silicon Valley, M&A and IPOs. However, as markets stabilise nothing seems certain, and the queue of capital-hungry businesses, built up during the hiatus in 2016, might seem more likely to suggest an uptick into 2017.

More people than ever before will use the internet... but more than half the world's population still won't

According to data published by the ITU, the beginning of 2017 will see 3.9 billion people, 53% of the world's population, not using the internet. In Africa, the figure rises to 75% (compared to 21% in Europe). The data also shows that:

- internet penetration rates remain higher for men than women in all regions of the world, with the most pronounced differences being in the least developed nations (a gender gap of 23% in Africa compared to 2% in the USA for example);
- the developed world has 1 billion internet users, while the less developed world has 2.5 billion;
- mobile is driving growth in the developing world. In developing countries the number of mobile broadband subscriptions continues to grow at double digit rates, reaching a penetration rate of roughly 41%, whereas fixed broadband subscriptions remain below 1%. To contrast that, seven billion people (95% of the global population) live in an area that is covered by a mobile-cellular network;
- in 2015, the Broadband Commission for Digital Development set a target: "By 2015, entry-level broadband services should be made affordable in developing countries through adequate regulation and market forces (amounting to less than 5% of average monthly income)". While five LDCs (Least Developed Countries) achieved the Broadband Commission target, in the majority of the world's poorest countries, broadband remains unaffordable; and
- broadband speeds remain much slower in the developing world. In early 2016, three out of four fixed-broadband subscriptions had advertised speeds of 10 Mbit/s and above in the developed countries, compared with two out of four in the developing countries. In the less developed countries only 7% of fixed-broadband subscriptions are advertised at speeds above 10 Mbit/s.

See our predictions for the telecoms sector at *https://united-kingdom.taylorwessing.com/download/article-telecoms-opportunities-and-challenges-for-sector-in-2017.html*.

The Internet of Things will remain unconnected, for now

There has been a lot of commentary on the growth of the Internet of Things (IoT) but not many of us have yet felt the impact. This is, perhaps, unsurprising – Cisco has stated that the IoT will grow in a similar way to the internet, with businesses leading the way followed by mass consumer adoption. Predicted figures for the number of devices vary greatly, but all are in the billions. Areas that are likely to fuel growth over the coming months and years include:

- **smart cities –** with around a half of the world's population living in cities, local governments' objectives to better manage resources and infrastructure such as traffic, power and waste systems will mean connected devices impact people's lives, albeit possibly without them being aware;

- **connected vehicles** – possibly the fastest growing consumer sector, the auto sector has embraced connectivity to enhance safety and security like no other sector. It is predicted that by 2020, more than 250 million cars will be connected worldwide;
- **connected homes** – despite high profile acquisitions such as Google's purchase of Nest, the connected home remains a niche play for now. The ability to control lighting and heating from outside the home is interesting to some but not exciting to most. However, as products enter the home that are pre-connected (rather than retro-fit), such as those compatible with Amazon's new Dash Replenishment Service (which allows, say, your washing machine to order new detergent directly), and as consumers become more used to using connected devices generally, take-up will increase; and
- **use of biometric data** – the monitoring of biometric data such as blood pressure has become an everyday part of life for users of some wearable technology, and such use is set to grow. It is even likely one day to form part of connected vehicles, for example, enabling the vehicle to monitor levels of wakefulness in long distance lorry drivers, and intervening or sounding an alarm where levels drop below a certain threshold.

Two key challenges are holding back rapid growth: first, lack of trust, and second, lack of common standards. As businesses are able to demonstrate the benefits of connected devices to users (particularly consumers), the cynicism around allowing big business access to data about their use of devices may dissipate. As standards are developed between manufacturers, allowing an open architecture based ecosystem to develop around application development, someone may eventually come up with the killer use case that has thus far eluded the sector. All that being said, there is a long road ahead and we don't see 2017 as being the year that the IoT finally becomes mainstream.

...but connected devices will mean big websites are attacked, many more times

On 21 October 2016, a number of major websites including the New York Times, Spotify and Twitter, suffered a distributed denial of service (DDOS) attack, and shut down for several hours. The attack involved tens of millions of IoT devices being deployed to send a US domain name server, Dyn, overwhelming traffic. The attack was made possible by the devices becoming infected with malware known as "Mirai botnet" – a virus that looks for IoT devices including those in the connected home. The malware is designed to use the devices it infects to carry out cyberattacks, which is pretty easy given they mostly use default usernames and passwords published online. As more unsecured IoT devices become connected to the internet, through the home, car or otherwise, the likelihood of further successful attacks would seem to increase and we may see regulatory steps to combat this.

We will all be immersed

You may have noticed the proliferation of Virtual Reality headsets from the likes of Sony, Oculus, Samsung and even Google (at least, if you like wearing cardboard on your face). You may also have noticed that they're not exactly this year's Cabbage Patch Doll, with few models flying off shelves. However, Augmented and Virtual reality will continue to gather pace outside of Video Games. According to IDC, in 2017, 30% of consumer-facing Global 2000 companies will experiment with Augmented Reality and/or Virtual Reality as part of their marketing efforts. IDC states that more businesses will engage with customers through "immersive interfaces" including AR and VR, and also that, in 2018, the monthly active user base of consumers using mobile augmented reality apps (e.g., Pokemon Go) will exceed 400 million, with over 20% of commercial media on Facebook being 360 degree video enabled.

AR platforms can raise some interesting questions around advertising laws and, in particular, the regulators' (such as the UK's ASA) requirements to clearly distinguish

advertising content (including product placement) from other content. They also raise privacy issues to the extent advertisers collect and process personal data from users, especially as AR can be applied to track image and location of users. AR used on products (such as, say, alcohol, allowing users to experience video and other content through their screen when aimed at the product), must avoid obscuring product labelling or otherwise contravening packaging laws. As always, the industry will balance innovation and customer experience with the requirements of the law. 2017 will be no different.

...and we'll all be hapnotised (man)

Haptic feedback is the use of the sense of touch in a user interface, such as a virtual button, or keyboard whose individual keys provide tactile feedback when pressed. Apple has deployed this, for example, in the fixed trackpads on models such as the Macbook's "Taptic Engine" – an electromagnetic motor to trick your fingers into feeling things that aren't actually there by using the motor's oscillation to makes it feel like you're depressing a mechanical button, rather than a stationary piece of glass. The underlying technology relies on a core component, Electro-Active Polymer Actuators (EAPs), which are polymers that exhibit a change in size or shape when stimulated by an electric field. Advancements in the technology are expected to develop more quickly due to the decreasing costs of EAPS.

The consumer electronics sector has been the area of fastest growth for haptic technology recently, followed by healthcare, however, the development of the technology is likely to see more widespread use of basic 'button' functions, such as in cars (Audi having demonstrated a haptic feedback function in its forthcoming A8 dashboard at CES this year). It will also see more innovation, though, leading to ever more subtle and fascinating interactions between human and device – 'bumpy pixels' allowing screen interfaces to carry realistic physical forms, for users to receive feedback dependent on tasks (such as scrolling to the end of a video clip triggering a small bump), or for viewers of a tense moment in a film to feel the actor's heartbeat, for example. Haptics could be used to aid accessibility for partially sighted or blind users (and this may, in time, be required under disability discrimination laws). One of the most subtle potential use of haptics will be the influencing of customers' web journeys – perhaps exploiting positive subliminal tactile feedback to encourage them to remain on certain pages, or even make purchases.

In mobile, the spread of the technology will, to a degree, depend on motor technology and power consumption, but widespread growth is likely to gather pace in 2017. User Interface designers are referring to the developing technology as Hapnotic Feedback, so prepare to be hapnotised.

Uber will continue to Uberise

According to Wikipedia, the term "Uberisation" means "a transition to an operational model which enables economic agents to exchange underutilized capacity of existing assets or human resources with close to zero transaction cost". This model has propelled Uber quickly to become the world's largest private venture-backed startup, raising more than more than $9 billion in funding, and disrupting the taxi markets in 527 cities across 77 countries. Uber's ride has not been as smooth as their cars, with cities, taxi lobbies and even drivers taking legal action threatening to slow or halt its growth, and some extremely negative PR along the way. Key victories such as the win against Transport for London have been tempered by rulings relating to the employment status of its drivers (leading to a potential obligation to pay employment-like benefits such as paid leave). In addition, while its finances are not published, leaked documents, and evidence of its heavy upfront investments in entering markets and fighting opposition to gain traction, suggest it is some way from being profitable. Given all this, one might be forgiven for thinking its growth will slow one day soon, as investors demand a chink of light at the end of the tunnel. However, there are a few key reasons to follow the money here:

- Uber is in 527 cities. That's a lot, but there are over 4,000 cities in the world with populations of over 100,000 (and only 295 of these are the US). Uber has not even launched yet in most of its addressable market (for its current core products, that is).

As mentioned above, the two key threats to Uber's current model are state regulation regarding the taxi market, and the possibility that its drivers need to be treated as workers or employees. State regulation has not, so far, stopped Uber from expanding more quickly than anyone could have predicted. The employment issue, could, however, slow it down and significantly impact its business model, although as these claims have only recently started to emerge, it is unclear whether they will be upheld and whether they will apply across multiple jurisdictions. However, driverless technology, already being trialed by Uber and competitors, could dispense with the need for any kind of workers, let alone those with employment status.

Lastly, and, perhaps, most importantly, when we think of Uber we tend to think of taxis (usually Black Toyota Prius') taking people from place to place within urbanised areas – such as San Francisco, London and Toronto. However, Uber's success has not come about due to its cars or its drivers, it has come from the game-changing effect of its technology on an inefficient market. Leveraging a simple combination of the internet, mobile devices, the rise of the gig economy, and the simple premise of deploying under-utilised capacity with real-time demand, has enabled it to transform the taxi market. How many more markets can be Uberised? Uber has entered the food delivery market (UberEats), the consumable delivery market (UberEssentials), and even the ice cream truck delivery service. However the possibilities are almost endless, and its financial muscle and unrivalled experience (or perhaps only rivaled by Airbnb) in developing processes and playbooks for launching new products in new cities, means it's better placed than any other business to grow into new sectors.

The dilemma will be which use cases to prioritise within the sharing economy – distribution of food waste? Use of under-utilised freezer space (and note that Electrolux is rumored to be building capabilities around fridge sharing technology for its users)? Use of someone's garage to store goods? Use of un-used wifi capacity? We've long accepted the concept of "surge pricing" (albeit not in name) for airline tickets, and it's easy to see how it could be applied to add efficiencies to numerous markets globally. Put simply, the sharing economy is in its infancy and Uber is ideally placed to become to that market what Google is to adtech. Other businesses in the same space will need to gain ground rapidly to keep up.

Facebook's existential crisis?

The power of social media to influence politics and government is not a new concept. Obama's presidential win in 2008 was dubbed the "Facebook election" and the catalysing effect of social media on the Arab Spring is well documented. However, the 2016 US election and the Brexit vote have taken the debate about the effect of social media to a new level. Remain voters are wondering how their Facebook feeds got the results SO wrong. Facebook has confirmed: "We believe that our role on News Feed is to help people connect to the stories that matter to them most,". What this means is that the Facebook news feed is curated by software to be tailored specifically to your likes and dislikes – so if you spent time liking pro-Hilary comments or publications and reading pro-Hilary articles, then it is exactly that sort of content that Facebook will show you – creating a kind of snowball effect re-inforcing your views. There is also the phenomenon of 'fake news' which was cited as influencing a percentage of the voters (although the percentage of news stories published by the fake sites is estimated as being less than 1%).

Media bias is, of course, nothing new – we all know the political leanings of the *Daily Mail* and *New York Post*, and readers select these publications where they reflect their own views. Facebook is only doing the same, by allowing the users to select their own bias,

however the difference is the scale – never before has there been a publisher with around two billion readers – in fact it's hard to think of a company that has ever had that many customers. Facebook has understandably said that it leans towards allowing users to circulate and consume anything they want but it is also planning to take steps to address fake news. Our predictions around the tension between freedom of expression and truth in the world of user generated content and how, or whether, regulation can help, are discussed in our article – at *https://united-kingdom.taylorwessing.com/download/article-2017-dawn-of-a-post-truth-era-for-platform-liability.html*.

.

...and in other predictions... South Korean publisher ETNews has reported that Samsung is working to mass produce foldable displays by the end of this year, with market availability set for 2017. It has been said by some that foldable screens will be as big a breakthrough as touchscreens were ten years ago.

Moscow will continue its cyber offensive, and the Trump administration may require security access to technology devices, a combination likely to generate further innovation in cybersecurity products?

Protests around the Investigatory Powers Bill are likely to gain momentum but come to little, for now. As the Bill has received Royal assent, the protests are too late to derail it. The law will require IPSs to retain data about customers browsing behaviour for up to 12 months. It is striking that such a controversial piece of law made it through Parliament so easily, with the volatile political events in the second half of 2016 certainly playing their part in burying this bad news. A recent petition will, at least, trigger a Parliamentary debate, and current legal challenges on the data retention requirements may lead to a tabling of amendments, but don't expect any dramatic changes any time soon.

Graham Hann, Taylor Wessing

EPrivacy Directive – all change

On December 12, 2016, it was reported that the European Commission intends to replace the e-Privacy Directive with a Regulation. The planned shift from a Directive to a Regulation has important legal consequences under EU law, as it means that instead of creating a floor upon which EU Member States may base the creation of their own versions of the law, a Regulation will create a harmonized set of requirements at the EU level that are directly applicable in the Member States.

The e-Privacy Directive was enacted in 2002 and designed to protect the right to privacy and confidentiality of users of electronic communication services, such as Internet service and broadband providers. Since its enactment (and subsequent amendment in 2009), the communications industry has evolved significantly, with an explosion in the availability and usage of so-called "over-the-top" communications services that provide their services via Internet-based applications. The European Commission's new draft Regulation, which was leaked to Politico, intends to include within its scope these "over-the-top" service providers, such as Skype and WhatsApp, that were not previously regulated under the e-Privacy Directive. The draft Regulation also addresses access to electronic communication services by government agencies for surveillance and monitoring purposes.

The draft Regulation is intended to complement the EU GDPR, and contains a number of provisions that mirror those of the GDPR. Consent under the Regulation will, for example, be based on the requirements for consent under the GDPR.

The draft was last amended on November 28, 2016, and is expected to be formally published shortly.

European DPAs Issue First GDPR Guidance

At the end of last year the EU the Article 29 Working Party issued official guidance relating to the General Data Protection Regulation, or GDPR (see overview of GDPR at *http://privacylaw.proskauer.com/2016/08/articles/european-union/an-overview-of-the-new-general-data-protection-regulation/* and *http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/* (The Article 29 Working Party comprises representatives of the various EU Member States' data protection authorities (DPAs), so this marks the first time that the DPAs have revealed their thoughts on how they plan to interpret and enforce specific GDPR provisions. This is welcome news for companies that, until this point, have been left to figure out compliance strategies without any indication as to how some of the newer concepts the GDPR introduces will operate in practice when the Regulation begins to apply in 2018.

The new guidance takes the form of three separate sets of guidelines: one addressing the right to data portability – *http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf*, another on identifying the lead supervisory authority for a controller or processor *http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf*, and a third on data protection officers – *http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf*. Each set of guidelines contains a detailed analysis of its specific topic and includes examples illustrating methods of compliance. Some of the most important points are summarized below.

Guidelines on the Right to Data Portability

For many companies, the GDPR's provisions relating to data portability present some of the biggest hurdles to achieving compliance by the time the GDPR begins to apply in May 2018. Article 20 of the GDPR states that a data subject has the right to receive the personal data that he or she has provided to a controller "in a structured, commonly used and machine-readable format," and to transmit that data to another controller (for example, a different service provider). It goes on to clarify that this provision applies in situations where the controller's basis for processing the data subject's personal data is based on the data subject's consent or on a contract to which the data subject is a party, and if the processing is carried out by automated means. Article 12(3) requires that controllers provide the requested information to the data subject without undue delay, but otherwise within one month of the receipt of the request (or three months for complex cases, in which case the data subject should be notified of the reasons for the delay).

While the Directive currently provides data subjects with a right of access to their data, Article 20's data portability right is different – and potentially more onerous for controllers. The provision is meant to give data subjects more control over their personal data, but for many companies, developing the capabilities to provide individuals with GDPR-compliant data transfers may take a significant amount of effort and resources over the next year and a half. For example, a company may have to assess where it stores customer data (and it may not all be in one place), evaluate what type of data it has collected, and implement a system that can generate the required transfers for those individuals that request them.

Unfortunately, this new guidance does not provide much peace of mind for data controllers, as it illustrates the considerable breadth of data the regulators consider to be subject to this provision. Some notable points are broken down below.

How Portable Data Should Be Provided to Users

The guidelines recognize the many types of data that data subjects may request, and therefore clarify that there is no one appropriate format for providing this data, as long as it is "interoperable" for ease of sharing with other controllers.

Types of Processing Operations that Fall Under the Scope of Data Portability

The guidelines re-emphasize the point that only data processed by automated means is subject to the data portability provision, and that paper files therefore are outside the scope of data portability.

The guidelines provide two examples of the types of data typically collected pursuant to a contract with a data subject: information subject to the data portability requirement includes titles of books published from an online bookstore, or songs listened to via a music streaming service. These examples provide a reminder of the wide scope of the definition of "personal data," and give insight into the considerable range of transactions that regulators could consider to arise out of a controller's contract with a data subject.

Data "Provided By" a Data Subject

The data portability right applies only to personal data "provided by" a data subject. However, this includes data beyond that knowingly provided by a data subject, such as name and address. A data subject may be considered to have "provided" data that was generated as a result of the individual's use of a service or device. Examples include search history, location data, and browsing behaviour.

Data Retention and Erasure

Data portability does not affect data retention. In other words, a company does not have to retain personal information just in case a data subject chooses to exercise his or her data portability right. Likewise, a data subject's data portability request is not, alone, to be taken as a request to delete that individual's personal data. Retention requirements with regard to personal information apply in parallel to portability requirements.

Rights of Third Parties

Some of the data that must be transmitted to a data subject who has made a data portability request will contain the personal information of third parties. The "new" controller (i.e. the entity to which the data subject transmits the data) must respect the privacy rights of these third parties. For example, if a webmail provider transmits the data subject's email contact directory to the data subject, and that individual then transfers the directory to a new provider, the new provider cannot then use the third parties' data for a purpose other than that for which it was originally collected. It cannot use the email addresses included in the directory to send its own marketing emails, for example. The guidelines recommend that controllers implement tools that will allow data subjects to exclude third party data from their portability request, and/or tools allowing third parties to consent to the transfer of their personal data.

Informing Data Subjects

Controllers must notify data subjects about the new right to data portability, and must "distinguish" this right from other rights. The Article 29 Working Party recommends that controllers make clear to data subjects what data they may request and receive when exercising their data portability right – a suggestion that may be hard to implement without an even fuller list of examples of the types of data subject to this requirement.

Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority

This set of guidelines is especially helpful for those companies that carry out "cross-border processing of personal data," which GDPR Article 4(23) defines as processing that takes place when a controller or processor has establishments in multiple Member States, or where the controller or processor is established in a single Member State but the processing "substantially affects or is likely to substantially affect" data subjects in multiple Member States. In these situations, the GDPR allows controllers and processors to designate a single local authority to act as the "lead supervisory authority" charged with overseeing their operations from a data protection perspective. This has become known as the "one stop shop" approach. The GDPR's provisions relating to "lead supervisory authorities" are meant to simplify and streamline privacy regulation, as under the Directive a company operating in multiple Member States may be subject to multiple DPAs.

This set of guidelines recognizes that the designation of a lead supervisory authority necessarily is a very fact-specific inquiry. Although it provides some generalized advice, it also includes illustrative examples and factors for companies to consider in making the determination for themselves. To that end, the guidelines also include an annex meant to guide companies going through the designation process. Some of the more general points are described below.

Identifying the Lead Supervisory Authority

For controllers, the GDPR provides that the lead supervisory authority should be the authority in the Member State in which the controller has its "main establishment" – in other words, the place where the controller has its "central administration" and makes "decisions on the purposes and means of the processing." The guidelines acknowledge that a controller could have multiple decision-making centers, and provide several detailed examples as to how to determine which center is the "main establishment."

Companies Not Established in the EU

If a company does not have any establishment in the EU, it cannot take advantage of the one-stop shop system and must deal with the supervisory authorities in each Member State in which it operates. Simply having a single representative in one Member State does not mean that person can serve as a "main establishment" for one-stop shop purposes. This may prove to be an especially large headache for small companies that reach out to consumers in multiple EU Member States but do not have the resources to create any EU establishments (i.e. some smaller app companies and start-ups), as they will have to expend the time and resources to tailor their compliance practices to each Member States.

Guidelines on Data Protection Officers ("DPOs")

Article 37 of the GDPR requires public bodies, as well as controllers or processors whose "core activities" involve (1) processing "special categories of data" (often referred to as "sensitive data") on a "large scale" or (2) regularly and systematically monitoring individuals, to appoint a data protection officer (DPO). The DPO is tasked with advising the company as to proper practices for GDPR compliance, among other responsibilities. This new requirement has attracted a lot of attention, not only because it requires many companies to designate a DPO for the first time, but because the GDPR appears to provide a fairly high degree of job security for DPOs, as Article 38(3) forbids companies from dismissing or penalizing a DPO for performing his or her responsibilities.

The guidelines make clear that the DPO requirement will apply to many companies. Key points include the following:

Definition of "Core Activity"

Although the guidelines' definition of "core activity" – those activities that "can be considered as the key operations necessary to achieve the controller's or processor's goals" – is not very enlightening in and of itself, the document does provide some helpful examples of what "core activity" does not include. For example, the guidelines acknowledge that IT support and employee compensation are activities common to almost all organizations, and even though they are essential, they generally may be considered "ancillary functions" rather than a company's "core activity."

Definition of "Large Scale" Processing of Sensitive Data

As defined in the GDPR, special categories of personal data (referred to here and many other places as "sensitive data") consists of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." The guidelines essentially punt on what constitutes "large scale" processing of sensitive data, stating that a "standard practice" for what may be considered "large scale" may develop over time and that companies should consider a number of factors in making the determination for themselves in the meantime. The guidelines do provide a few fairly

obvious examples of "large scale" sensitive data processing, such as a hospital's processing of patient data, as well as a few examples of non-"large scale" processing, such as an individual lawyer's processing of criminal convictions.

Definition of "Regular and Systematic Monitoring"

The guidelines explicitly state that "all forms of profiling and tracking on the internet, including for purposes of behavioral advertising," are considered types of "regular and systematic monitoring," thereby indicating that behavioral advertising agencies should designate a DPO. Although the guidelines do not state so explicitly, a company that drops cookies might also be viewed as engaging in a form of "profiling and tracking on the internet." Taken to its extreme, this could include the use of a cookie as benign as a log-in cookie triggering the requirement for a company to have a DPO. We hope to receive additional guidance from the DPAs as to what kinds of Internet "tracking" give rise to this requirement.

DPO Qualifications and Job Description

The more sensitive, complex, and substantial an organization's data processing is, the more qualified a DPO must be. The guidelines state that a DPO must have a level of expertise "commensurate with the sensitivity, complexity, and amount of data an organization processes."

All DPOs should possess "an in-depth understanding of the GDPR" – so companies planning on designating a current employee as the DPO must ensure that person is up to speed come May 2018.

A DPO need not always be an individual, as the guidelines clarify that a team can function as a DPO, provided that a single person serves as the lead contact and tasks are clearly allocated to the different team members. Likewise, a DPO does not even need to be a company employee or team of employees, as a company may contract out the DPO's responsibilities to an outside service provider.

An organization must always consider the DPO's position and, if it disagrees with the DPO, it should document its reasons for not following the DPO's advice. The guidelines emphasize that a DPO cannot be terminated or otherwise penalized (i.e. via denial of promotion) for providing advice within the scope of his or her responsibilities with which the organization does not agree.

With approximately a year and a half to go until the GDPR begins to apply, additional regulatory guidance is expected. Check back here for analysis of forthcoming guidance and other GDPR developments as they become available.

Courtney M. Bowman, Proskauer Rose LLP

Digital Single Market update: Council confirms approach to EU geoblocking ban will not apply to sports broadcasts

At the end of last year the European Council announced (see *www.consilium.europa.eu/en/press/press-releases/2016/11/28-geo-blocking/*) that it has agreed a general approach (at *http://data.consilium.europa.eu/doc/document/ST-14663-2016-INIT/en/pdf*) to a draft regulation to prohibit "unjustified geoblocking" between member states, including confirmation that the regulation should not apply to sports broadcasts. The draft regulation formed part of the proposals adopted by the Commission earlier this year on the Digital Single Market (DSM) strategy (which Sports Shorts has previously discussed (see *www.sports.legal/2016/09/commission-announces-latest-development-in-digital-single-market-strategy/*). The Council's general approach will form the basis of its negotiations with

Parliament under the EU's ordinary legislative procedure following the draft regulation originally proposed by the Commission in May 2016.

The stated aim of the geoblocking regulation is to boost e-commerce and remove discrimination based on customers' nationality or place of residence. Broadly speaking, geoblocking is any measure which blocks cross-border access to a website, or compulsorily reroutes the user to their 'home country' website so that they can only purchase from there, or permits cross-border access to a website but denies the user the ability to make a purchase (for the Commission's full definition of geoblocking and more detail on proposals to curtail it, see https://ec.europa.eu/digital-single-market/en/geo-blocking-digital-single-market).

Why does this matter for sport?

As Sports Shorts has discussed previously (see *www.sports.legal/2016/09/commission-announces-latest-development-in-digital-single-market-strategy/*), sports rightsholders have been understandably concerned by the possible impact of the DSM on their ability to maximise revenue by selling media rights on a territory-by-territory basis. Traditional licensing models, which have generated a huge proportion of rightsholders income, rely on the ability to sell in this way. In the online environment, a key tool in doing so is geoblocking. Thus, from a rightsholder's perspective, the broad application of concepts like digital portability and the potential prohibition on geoblocking presents a real threat and, for this reason, they have been somewhat wary of the DSM initiative, particularly in light of comments such as those of EU Digital Single Market Commissioner, Andrus Ansip (commenting in May this year): "Today's situation is lose-lose: people are ready to pay, but we do not accept their money. There are two logics – geoblocking or the internal market. Those two cannot coexist… Deep in my heart, I hate geoblocking. It is old-fashioned and it is not fair. We do not have to use these instruments in the 21st century."

Fortunately for rightsholders, the Council confirmed (paragraph 6 of the agreed general approach) that "certain activities" including "Audio-visual services, including services the principle purpose of which is the provision of access to broadcasts of sports events and which are provided on the basis of exclusive territorial licenses, are excluded from the scope of the Regulation."

Whilst the exclusion of this type of audio-visual content was not unexpected (the Commission confirmed last December that it would be focusing on cross-border digital portability but made no mention of banning geoblocking in relation to sales of content), sports rightsholders will nonetheless welcome the confirmation. However, whilst they may be breathing a small sigh of relief, they will still need to be prepared to adapt to the other aspects of the DSM initiative, such as digital portability which may still affect current licensing models.

Rosie Duckworth, Squire Patton Boggs

ISSN 0969 3297

IT Law Today is published by: Singlelaw, The Ridge, South View Road Pinner HA5 3YD • Tel 020 8866 1934
www.singlelaw.com

Editor: Susan Singleton, Singletons, Solicitors www.singlelaw.com
Production: Frida Fischer • email: fridafischer@hotmail.com
Marketing: Susan Singleton • Tel: 020 8866 1934 or email: susan@singlelaw.com
Publisher: Susan Singleton

Subscription orders and back issues, sales and renewals: Call 020 8866 1934 • email: susan@singlelaw.com
For legal advice and training on IT/ecommerce/internet and data protection law, email susan@singlelaw.com.