e-commercelaw&policy

THE MONTHLY JOURNAL FOR ONLINE BUSINESS
JUNE 2014 VOLUME 16 ISSUE 06
WWW.E-COMLAW.COM

Google break-up "last resort" in Germany

Germany's Economy Minister and Vice Chancellor Sigmar Gabriel declared that a break-up of Google, similar to that of gas grids in the country, must be "seriously considered" as a "last resort" in order to prevent discrimination against alternative search engine providers, in an article published in the *Allgemeine Zeitung* newspaper on 16 May.

Further to discussing such an option, Gabriel also described how the German Ministry of Economy and Federal Cartel Office are investigating how Google uses its market position with regards to search results, with the Ministry considering, said Gabriel, "anti-trust style regulation of internet platforms" as an option. The investigation into Google's search results is part of a wider examination by the Ministry into Google's policies and practices, including on other issues such as privacy.

On 15 May, a number of European companies, collectively known as the Open Internet Project, filed an anti-competition complaint with the European Commission in regard to, *inter alia*, Google's data practices and use of search algorithms.

IN THIS ISSUE

The aftermath of the ECJ's right to be forgotten ruling

Google introduced on 30 May an online form that allows users to request the removal of links that they think are 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed.' Following the European Court of Justice's (ECJ) ruling on 13 May in case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, that an internet search engine is responsible for the processing that it carries out of personal data that appears on web pages published by third parties, search engines must now comply with EU law, which includes the right to be forgotten. Online search engines must now review right to be forgotten requests from individuals and decide whether to take down the information or not, and as described by Google on its online form 'attempt to balance the privacy rights of the individual with the public's right to know and distribute information.'

"An online form is certainly a good step to streamline requests. However, if taken seriously, requests need to be evaluated on a case-by-case basis - making it almost impossible to implement a one size fits all approach," said Ulrich Baumgartner, Partner at Osborne Clarke. "There is some guidance in the ruling, but in the end, providers are on their own to check whether a request must be followed. The good news is that sooner or later, we expect the rules to clear on what is a justified take down request and what is not."

Google's online form requires that users provide a copy of a valid form of photo ID, allows individuals to list as many URLs as they would like and provides an opportunity for the user to explain why each link should be removed.

"In our view, any operators of data driven web services similar to search engines like social networks and online platforms will be impacted by the decision," said Baumgartner.

Germany's Interior Ministry has warned against search engines relying on computer software to determine which information should be removed and is considering setting up arbitration courts to decide. "The background behind this proposal is the fear that search providers might introduce automatic deletion mechanisms. As a consequence, public information could be at risk, the German government has said," concludes Baumgartner. "This proposal is a clear sign that governments do see a danger to the right of information and attach great importance to the public's right to know."

Two UK Parliament committees highlight copyright reform fears

The UK Parliament's Joint Committee on Statutory Instruments (JCSI) has delayed the passing of draft regulations to extend copyright exceptions, asking on 8 May for further time to consider the private copying and parody exceptions.

"The JCSI has very usefully taken a hard look at the planned exceptions," said Ted Shapiro, Partner at Wiggin LLP. "The private copy exception would usher in an unprecedented new level of consumer confusion; one provision would require consumers to delete private copies of works they have made when they give away or sell the original." The Government has yet to announce whether it will amend either exception.

The House of Lords' Secondary Legislation Scrutiny Committee (LSLC) published on 9 May a report highlighting the 'strength of concern expressed' around the reforms, on matters such as 'contractual override,' which would prevent rightsholders from overriding the extensions through contracts. "This provision could be particularly harmful in the online 'on-demand' environment," adds Shapiro.

The LSLC urged the Government to monitor the impact these changes bring. However, Lorna Brazell, Partner at Osborne Clarke, believes "It will be up to the rightsholders to monitor specific works being used outside current prevalent usage, and provide evidence of erosion of their economic returns from their works. Copyright in music, film, and art is too vast a field for a government agency to monitor."

e-commercelaw&policy

THE MONTHLY JOURNAL FOR ONLINE BUSINESS
VOLUME 16 ISSUE 06 JUNE 2014
WWW.E-COMLAW.COM

EDITORIAL BOARD

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Associate Editor Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions Adelaide Pearce
adelaide.pearce@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com

E-Commerce Law & Policy
is published monthly by
Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street,
London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

 ISSN 1466-013X

The right to be forgotten: the unanswered questions

On 13 May, the European Court of Justice decided in Case C-131/12 that search engines must comply with requests from individuals to remove search results linking to information which is 'inadequate, irrelevant or no longer relevant.' The content remains on the webpages where it is published, although finding it may be hindered. To determine what this means in practice, Patrick Van Eecke and Anthony Cornette of DLA Piper contrast what we can discern so far from the decision with the many questions that remain unanswered at this time.

Under European data protection law (the Data Protection Directive (the 'Directive') of 1995, as implemented in each Member State), people may request the 'rectification, erasure or blocking of data,' if the processing of their data does not meet certain conditions. Such conditions include that the data are adequate, relevant and not excessive in relation to the purposes for which they are processed. There are some exemptions provided by European data protection law, for instance regarding processing carried out solely for journalistic purposes or the purpose of artistic or literary expression, which may apply to newspapers and their websites. Search engines typically do not fall under this exemption.

The right to be forgotten is not a newly created right, but rather a means to enforce existing rights under the current Directive. The court ruled that search engines results can produce a 'detailed profile' of an individual and search engines are responsible as controllers of the personal data they index, even if the webpages themselves are published lawfully (e.g. because they fall under the exemption for journalism). An individual may wish embarrassing information about himself or herself not to be easily found and may 'request that the information in question is no longer made available to the general public.' It is this ability to direct a request to the search engine that constitutes the right to be forgotten.

How to exercise the right to be forgotten?

After a request, the search engine would then have a decision to make about whether the information is 'inadequate, irrelevant or no longer relevant.' There is also a balance to be made with the public interest. According to the court this balance may depend 'on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.'

Not only is 'relevance' highly subjective, but it also fluctuates over time. Not all information about someone becomes less relevant over time. For example, information concerning someone's conduct in the past may be considered no longer relevant, only to become relevant again if that conduct is repeated on a later date.

If the search engine refuses to remove search result links, then the decision can be appealed before national data protection authorities or national courts. The search engine may incur liability if it does not comply with requests, and it is likely that search engines will weigh the disadvantages of complying with the request (such as having search results that are less complete) with the advantages (such as avoiding liability), in a way similar to intellectual property infringement claims.

However, search engines could also refuse to make the assessment regarding the relevance of the data and forward many, or most, requests to data protection authorities or the national courts. The search engine could also systematically appeal decisions. This could mean additional delays in obtaining an order to remove search results and this would limit the practical effectiveness of the court's ruling.

Who can invoke the right to be forgotten and against whom?

The facts of the case involve a Spanish citizen against Google Spain and Google, Inc. The court ruled that Spanish data protection law was applicable to both Google Spain and Google, Inc. However, it is unclear who else might invoke a right to be forgotten and against whom.

The judgment refers to the fact that Google keeps the location of where the processing of the index occurs secret for reasons of competition. The judgment refers to the consumer side and the advertising side of Google as 'inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.' The main factor for the application of Spanish data protection law was the fact that Google has establishment on Spanish territory, by engaging 'in the effective and real exercise of activity through stable arrangements in Spain.' Selling advertising to Spanish businesses therefore seems sufficient to trigger the application of law, but it is

unclear what the court would have decided if Google had no offices and no employees in Spain. For a search engine which does not have a national presence, and which does not sell any or much advertising in the country, it is unclear if data subjects in that country can make a similar right to be forgotten request.

The judgment refers explicitly to Google Search to denote both Google.com and Google.es. However it is unclear if Google could refuse to remove search results from Google.com. It is likely, but not clear at this point, that both sites may be ordered to stop displaying the search results in the case at hand. If the decision were to be interpreted such that Google.com could continue to display the results, then the decision would have limited to no practical effects.

Non-European citizens would at first sight not benefit from the protections afforded by European data protection law. However, the applicability of the law does not depend on the nationality of the data subject. For instance, a non-Spanish citizen living in Spain could have made the same request, or the data subject could have lived abroad. This raises the question whether non-European citizens can submit requests to European data protection authorities or courts in the event that a search engine refuses to fulfil a right to be forgotten request. We will have to see how the court's decision is interpreted before national courts.

What about social media sites and news aggregator sites?

Equally unresolved is the situation where people start sharing links that are omitted from a search result on social media sites such as Twitter. It is unclear whether the filtering of search results by Google would also need to operate on indexed public social media posts (as new links are posted). It is also unclear whether the search functionality of social media sites would fall under the same criteria established by the court as for search engines.

Depending on its application, the judgment could have limited effectiveness, due to the many ways information can surface, including through social media

The answers to such questions may strongly reduce the effects of the court's ruling in practice. The court's decision says that the technology to create a 'structured overview of the information relating to [an] individual that can be found on the internet […] and thereby to establish a more or less detailed profile of him' does not make it justified to do so. The court stated that the potential interference of a person's rights 'cannot be justified by merely the economic interest which the operator of such an engine has in that processing.' However, depending on its application, the judgment could have limited effectiveness, due to the many ways information can surface, including through social media. Similarly, regarding news aggregators and search engines run by journalism outlets, it is unclear how the ruling of the court should be interpreted. Such services could be regarded as falling under the journalism exemptions of data protection law, as interpreted in each country.

If Google is a controller, does it need permission to process the data? How can it process special categories of data?

The Directive provides limited grounds for controllers to process data. Data subjects do not provide Google with permission for the processing of their data on third party webpages. Such data processing by Google must therefore be considered to be grounded on the necessity of the processing for its 'legitimate interests.' This means that the court ruled that Google may process the data because it has a business interest to do so. The court decision could therefore be considered to lower the requirements for processing under the Directive, since Google's business interests suffice to engage in the processing and no consent of the data subject is needed. The ruling therefore legitimises the 'opt-out' Google stance on data protection (which it also takes on copyright law in the case of YouTube): the law generally imposes consent of the data subject (or the copyright holder), but Google chooses to process the data and to publish materials first, unless the processing or the publishing is challenged later on.

Furthermore, special categories of data processing can only occur under certain strict conditions. Such data includes that concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning a person's health or sex life. As the Advocate General pointed out, if Google is a controller, then any processing of special categories of data is likely not to occur in accordance with the requirements of the Directive. This would mean that such processing is not allowed. However, the court's ruling does not address this issue and we will have to see how the decision is further interpreted by national courts.

Although the court decision seems to be quite straightforward at first sight, a second reading shows a Pandora's Box has been opened. It is now up to the national courts to ensure a workable and consistent interpretation of this right to be forgotten.

Patrick Van Eecke Partner
Anthony Cornette Lawyer
DLA Piper, Brussels
patrick.vaneecke@dlapiper.com
anthony.cornette@dlapiper.com

Vodafone: many of the net neutrality fears are unfounded

The net neutrality debate has been an emotive one, concerning issues such as freedom of expression, innovation, discrimination and corporate motives. But there have been very few articles about how networks actually work and why it matters. In this article, Lisa Felton, Head of Consumer Policy and Content Standards at Vodafone Group Services Limited, explains her view that net neutrality needs to be grounded in an understanding of the underlying technology in order to achieve its aims of a better internet for all.

The 'Connected Continent' package was presented by the European Commission on 11 September 2013 and was intended to create a single market in communications technology. For the first time, the package included net neutrality rules. This was a sea change from the Commission's previous position, expressed in the Commission's Communication of 19 April 2011, entitled 'The Open Internet and net neutrality in Europe,' where the existing transparency and low switching costs were seen as sufficient to ensure customers could find the right service to meet their needs. The unstated reason for this change was the increasing pressure for national legislation on net neutrality, giving rise to a concern from the European Commission that this would result in a fragmented approach across Europe.

The net neutrality proposals introduced by the European Commission have steadily become more extreme during the European Parliamentary review process, culminating in the proposals approved by the European Parliament on 3 April 2014. Under these proposals, net neutrality is defined as 'the principle according to which all internet traffic is treated equally, without discrimination, restriction or interference, independently of its sender, recipient, type, content, device, service or application.'

There are many policy drivers behind the net neutrality proposals, for example the fear of internet speeds being degraded if operators sell faster speeds to companies, which then becomes a fear about a new type of digital divide where some users are relegated to a 'dirt road' internet. There is also a concern that speeding up some services may prevent innovative new services developing if new or start-up companies cannot afford to pay for such prioritisation. Finally there are privacy fears: fears that traffic is being manipulated and restricted without users' knowledge.

We have set out ten facts below which help to reset the debate by explaining why many of these fears are unfounded and how networks actually work.

Net neutrality could slow down the internet

The internet operates by providing the best service possible to customers - by proactively prioritising and optimising traffic based on where end users are, what device they are using and what type of traffic they request. Internet service providers use various techniques to optimise the performance of their networks - by compressing video data, for example, so it takes up less space (and costs customers less to use), by adjusting the video content so that it takes account of the size of screen and handset being used, and by only downloading what is being used, not entire files. But the net neutrality proposals only allow traffic management where there is temporary and exceptional congestion - which would mean in practice that videos and streamed content would buffer and quality would go down.

Specialised services can improve the quality of internet access services

A fundamental principle of the internet is that it involves the sharing of scarce resources and everybody gets to use the same infrastructure. There is an understandable concern that this means some people will lose out if others are favoured. The net neutrality answer to this is to build a separate network for special and faster services, which would be

disproportionately expensive and difficult to do in practice. The better answer is to build bigger networks, which can be shared - even if some services have priority at certain times as general internet users will benefit from using the spare capacity as well. Costs, and therefore prices, will be lower for everybody. Requiring internet access providers to operate logically separate networks means significantly higher costs, duplication of infrastructure and unused capacity.

Regulators want to incentivise operators to invest in new high speed, high capacity broadband infrastructure

If operators can charge application and services providers for higher quality, this produces more revenue which then drives more investment. Otherwise operators will be faced with the challenge of building networks, sharing them with new entrants at regulated prices and making them available for free to application providers that compete with them.

Net neutrality can reduce customer choice - and cause harm as a result

The idea that no websites can be blocked is incompatible with controls which allow parents to block over 18 content on their laptops and mobiles so that their children cannot access this content. It also does not allow internet access providers to continue with their voluntary approach of blocking child abuse material via the lists produced by the Internet Watch Foundation and others - which is collated based on reports by the public.

Everyone pays for video

Sandvine recently released a report on internet traffic called 'Global Internet Phenomena Report 1H2014' stating that Netflix alone now constitutes over 34% of downloading traffic in the evening in North America[1]. Usage patterns on the internet are undergoing a fundamental change. Net neutrality requirements would mean that consumers who wish to use the internet for very light applications (e.g. social networking) will have to subsidise internet users who are using bandwidth heavy services such as video, since there is limited possibility to create innovative new business models for these services.

Net neutrality will not enable innovation - it will reduce it

Networks - and software used on those networks - are constantly evolving. For example, there is a new technology that has been developed which moves content around to use 'dark spaces' or empty gaps in the network. Users cannot necessarily see this service but it makes a huge difference to their experience. In addition, innovative services such as remote health monitors, IPTV and high quality voice services, which rely on a guaranteed quality of service, will not be possible without building separate networks, which is likely to be prohibitively expensive.

Net neutrality can distort competition

The net neutrality arguments fail to recognise that traffic management takes place at every level of the internet. Providers of handsets, browsers, virtual marketplaces and other services such as Google, Microsoft, Nokia and others use traffic management to improve the delivery of their pages on the internet and to optimise third party content - using the same methods as internet access providers. Optimisation, caching, intelligent traffic management and providers of Content Delivery Networks have a business model based on obtaining revenues by improving quality of experience for end-users. The net neutrality proposals only address part of the value chain and if we are to ensure harm is prevented, any restrictions must apply equally to any company that can block access to websites or prioritise content.

The proposals will put EU companies at a disadvantage

The proposals are more restrictive than any existing net neutrality laws imposed in Europe or the US. This is particularly true in the mobile space - which should be a key driver of growth in Europe, but which is being held back through overregulation and uncertainty. The Navigant report published in 2013[2] highlighted that the EU mobile wireless market was falling behind the US: US speeds are 75% faster than the EU average, US consumers use nearly twice as much data and the level of wireless capex in the US has grown by over 70% since 2007, while declining in the EU. The proposed EU approach will stifle innovation in relation to performance and quality and hold back Europe even further. The internet is global and the innovation will move to parts of the world with more innovation friendly regulatory environments.

Net neutrality is almost impossible to implement

In practice, the net neutrality proposals, wherever they have been implemented, have been very difficult to interpret and enforce. In the US, they have struggled to define specialised services - despite setting up a joint industry and government committee to do so. In the Federal Communications Commission (FCC) Open Internet Advisory Committee report

entitled 'Specialised Services: Summary of Findings and Conclusions' they state that defining specialised services has 'proved difficult,' not least because of the multitude of ways in which the FCC itself has used the term. In the Netherlands, one year after the implementation of net neutrality legislation, a consultation on the definition of specialised services was launched and we are still awaiting the outcome. Regulators have struggled in particular with services where data is offered for free - while these appear to discriminate against other services, they are also clearly advantageous to the consumer and also mean that there is more data within a capped bundle to be used for third party services.

Consumers are more interested in their service working well than in understanding how it works

All telecoms operators are already required to disclose how they manage traffic to their customers. Simply adding to the existing requirements is likely to be counterproductive, as consumers are overwhelmed with more and more information. In September 2013, Ofcom published research which showed that despite most consumers understanding the traffic management information provided, there was a general lack of awareness of traffic management, with one in 10 internet consumers familiar with the term and only one per cent claiming to have considered this when choosing their broadband service[3]. What is needed is clear information about the speeds consumers can expect, any restrictions on what can be accessed and how to opt in and out of solutions such as parental controls and spam filters.

The FCC rules

The proposals are more restrictive than any existing net neutrality laws imposed in Europe or the US. This is particularly true in the mobile space

Faced with these issues, 'good' net neutrality rules seem almost impossible to define. However, it is worth looking at the proposals introduced by the FCC in the United States, in their new Notice of Proposed Rulemaking ('NPRM') published on 15 May 2014.

The FCC focuses on three main areas: transparency, no blocking and commercially reasonable agreements. In relation to transparency, the proposals build on the requirements previously set out in the law - sensibly extending information requirements to speeds, data caps and point of sale disclosure requirements as well as traffic management. The no blocking requirements are the same as the previous law - prohibiting fixed broadband providers from blocking lawful content and mobile providers from blocking competing services. The FCC also addresses the thorny issue of what a minimum level of access looks like, suggesting that this might be 'the typical speed' received by users. Broadband providers would be allowed to negotiate a 'better than typical' speed but prohibited from delivering 'worse than typical' service in the form of degradation or outright blocking. Finally, the FCC also creates a new mechanism to allow commercial differentiation, provided operators' conduct is commercially reasonable.

While the FCC requirements are not perfect, they do prevent discrimination whilst allowing differentiation. If implemented, they will encourage innovation in the US - at the same time as it is being stifled in Europe, despite the fact that there is less competition amongst internet service providers in the US. It is difficult to predict the right answers, but at least the FCC is asking the right questions.

Lisa Felton Head of Consumer Policy and Content Standards
Vodafone Group Services Limited
Contact via editorial team

1. https://www.sandvine.com/trends/global-internet-phenomena/
2. http://www.gsmamobilewirelessperformance.com/GSMA_Mobile_Wireless_Performance_May2013.pdf
3. http://stakeholders.ofcom.org.uk/binaries/research/broadband-research/1145655/traffic-research.pdf

The Consumer Contracts Regulations and online sales

The law is changing for online businesses selling to consumers. Businesses need to review their terms and conditions and purchase flow to take into account the new rules in the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013, which come into force on 13 June 2014 and replace the existing Consumer Protection (Distance Selling) Regulations 2000. Doris Myles, Helen Brown and Julia Hemmings of Baker & McKenzie LLP, discuss the new Consumer Contracts Regulations in detail and guidance published by the Department for Business, Innovation & Skills (BIS) to help businesses understand the changes.

Digital content

The Consumer Contracts Regulations include a new category of 'digital content' which is intended to fill the gap that previously existed for the sale of downloaded or streamed digital content which does not easily fit into the traditional categories of goods or services.

Why is the law changing?

The Consumer Contracts Regulations implement the majority of the EU Consumer Rights Directive (2011/83/EU) ('Consumer Rights Directive') which is intended to standardise distance selling requirements across the EU. The previous law was based on a minimum harmonisation approach which led to very different national laws, creating problems for businesses selling to consumers across the EU. The new Consumer Rights Directive is a maximum harmonisation directive which means that EU Member States must ensure that their national laws do not go further than the terms of the Directive.

What will change?

The Consumer Contracts Regulations cover three key areas:

- A requirement to provide more information to a consumer before and after a sale, either as part of the purchase flow or in the terms and conditions.
- Increased cancellation rights.
- Prohibition on hidden costs.

Information as part of the purchase flow

One of the most important requirements of the Consumer Contracts Regulations is that the consumer has an opportunity to fully read and understand the main elements of the contract before buying. This obligation will require businesses to amend their websites to ensure that a consumer is provided with certain information at the right stage of the sales process. As a result, some information must be expressly set out in a clear and prominent manner directly before the consumer places the order and not just included in the terms and conditions.

Another change to the purchase flow is that online businesses must make it absolutely clear to the consumer that there is an obligation to pay, by using a button or similar function labelled 'order with an obligation to pay' or a corresponding unambiguous formulation. The BIS Guidance suggests that 'pay now' would be a suitable alternative formulation. It seems critical that the word(s) on the button must clearly indicate that the consumer is required to make a payment and businesses should no longer be using words on the button such as 'subscribe' or 'confirm.'

Information that must be provided before a sale

The Consumer Contracts Regulations contain a list of information that needs to be provided to consumers before a sale. Much of this information is not new as the existing Distance Selling Regulations included information requirements; however, there are some specific new requirements.

- Cooling-off period - businesses must inform consumers of their no-fault right to cancel within 14 calendar days. Failure to provide information on the cooling-off period before a sale will extend the cooling-off period from 14 calendar days to 12 months.
- Cost of returns - businesses must inform consumers if they must bear the postage cost of returning goods to the business if the consumer decides to cancel the contract during the cooling-off period. Failure to do so will mean that the business has to bear the cost. Of course in many cases businesses provide a method for the consumer to return the goods free of charge.
- Model cancellation form - businesses must provide a model cancellation form which can be used by a consumer to cancel the contract during the cooling-off period. Importantly, although the form must be provided (e.g. by use of a link), the consumer is not required to use the form and can cancel the contract using any other method e.g. email.
- Digital content - businesses must provide information on the functionality of digital content, including applicable territorial restrictions and any relevant interoperability with hardware and software that the business could reasonably be expected to be aware of, for example that an e-book will only work on a device with a particular operating system.

The Consumer Contracts Regulations recognise that in some situations, there may be limited space or time to display all the pre-contractual information (e.g. a mobile phone screen). In those situations, businesses must supply some minimum information and refer the consumer to another source of information, for example a link to the business' webpage where the consumer can access the remaining information.

Information that must be provided after a sale

After a sale, a consumer must be provided with a copy of their concluded contract in a durable medium which allows the consumer to store and reproduce information in an unchanged format for so long as the consumer needs it. An email or a text message is a durable medium. However, information contained in a link to a website which may change is not a durable medium.

Cancellation rights

One of the most important rights that a consumer has when buying online is a no-fault right to cancel the contract and obtain a refund within a short period of time, often referred to as the 'cooling-off period.' The Consumer Contracts Regulations have made some important changes to cancellation rights which are further complicated by different rights that apply whether a business is selling goods, digital content or services.

- Goods - The cooling-off period has been extended to 14 calendar days from the receipt of the goods. The consumer may use the model withdrawal form to cancel the contract or any other unequivocal statement of intention to cancel the contract.
- Services - The cooling-off period is 14 days from the date of the contract but if the consumer wishes the services to start immediately then the business needs to obtain explicit consent from the consumer and acknowledgement that when the service has been fully performed, the consumer will have no right to cancel. If a consumer requests for the services to start but subsequently cancels then the consumer will need to pay for any services delivered until the point at which they cancel.
- Digital content - The consumer will lose the right to cancel if supply of digital content has begun within the 14 day cooling-off period but the consumer must have given prior express consent to start the supply and acknowledged that by doing so, the consumer loses his/her right to cancel.
- Refund - If a contract for goods is cancelled by a consumer during the cooling-off period, the business must refund all payments including the price and any standard delivery costs paid by the consumer. If a consumer has paid an additional amount for express delivery then only the standard delivery charge needs to be refunded. A business may withhold the refund until it has received the returned goods or proof of postage but once received, the business needs to make the refund within 14 days.
- Use and diminished value - A business can reduce the amount of refund for goods returned which show evidence of use leading to diminished value. Consumers can inspect the goods to see if they are as expected, for example, the normal type of inspection or handling that would occur if the consumer was buying the goods in a shop. Businesses cannot reduce the refund where a consumer has merely removed packaging to inspect the goods. In reality it will be difficult for businesses to ascertain how much of a reduction should be made to a refund for 'unreasonable' use of the goods and it will be interesting to see how many businesses reduce refunds based on any diminished value of the goods.

One of the most important requirements of the Consumer Contracts Regulations is that the consumer has an opportunity to fully read and understand the main elements of the contract before buying

Hidden costs

Businesses cannot impose hidden charges on a consumer and as a result a business must seek express consent from a consumer for any additional payment.

- Pre-ticked boxes - businesses cannot use pre-ticked boxes on a website where it results in a payment by the consumer (e.g. insurance when booking a flight).
- Telephone calls - businesses cannot use premium rate telephone helplines. A consumer may not be charged more than the basic rate to call a customer service helpline or to discuss an order or problem with the supplied product or service.

Summary

The provisions in the Consumer Contracts Regulations are mandatory and any attempt by a business to change these rights in their contract with the consumer which results in a direct or indirect restriction of the consumer's rights will not be binding on the consumer.

As a result, businesses selling to consumers online should review their terms of sale and websites to ensure they are compliant with these new provisions when they come into force on 13 June 2014.

Doris Myles Professional Support Lawyer
Helen Brown Senior Associate
Julia Hemmings Senior Associate
Baker & McKenzie LLP, London
doris.myles@bakermckenzie.com
helen.brown@bakermckenzie.com
julia.hemmings@bakermckenzie.com

US Big Data Report focuses on use rather than collection

Kurt Wimmer, US Chair of Covington & Burling LLP's Privacy and Data Security Practice and Jeffrey Kosseff, also of Covington & Burling LLP, Washington DC, examine the Big Data Report presented to President Obama on 1 May, which looks closely at the future capability of technology in the collection, use and analysis of big data and its ability to protect and threaten privacy.

Not all uses of data are the same

That was the key message of a 79-page report from the White House Big Data Working Group. The report, released on 1 May 2014, outlines a number of recommendations and observations regarding the regulation of big data in both the private sector and government.

Although the report does not create any binding law or regulations, it shines a light on the administration's key priorities in privacy and data security in the era of big data and renews a call for Congress to consider privacy legislation. The Working Group was led by John Podesta, a top White House advisor and former chief of staff to President Clinton.

Collection vs. use

A key theme that emerged throughout the report is that regulators should focus on how companies and government agencies use big data, and regulate accordingly.

While such an approach may sound like common sense, it is at odds with how US lawmakers and regulators have addressed privacy for decades. Regulators have long focused on the methods of collection of data from individuals. This approach has long been the subject of criticism from consumer advocates and industry alike who argue that regulators should be more concerned about how the data is used after it is collected. As Craig Mundie, Senior Adviser to the CEO of Microsoft Corp., wrote in a recent Foreign Affairs article that was cited in the White House report, '[t]he time has come for a new approach: shifting the focus from limiting the collection and retention of data to controlling data at the most important point - the moment when it is used.' The White House report supports this approach, concluding that data that is 'socially beneficial in one scenario can cause significant harm in another.'

This approach also recognises, as the White House report puts it, that 'we live in a world of near-ubiquitous data collection.' There is no indication that this data collection will slow down, particularly as companies continue to devise new, in-demand technology such as appliances that are connected to the internet. The report recognises that it is possible to take advantage of the exponential growth in potential benefits of big data without compromising individual privacy.

Sensitive uses

In line with its focus on use rather than collection, the Working Group concentrated on particularly sensitive uses of data, including healthcare and education.

The Working Group recognised the tremendous potential benefits of big data for healthcare. The report recognises that big data can help identify preventative measures and potential treatments that may not be immediately evident. But the Working Group recognised that such use 'requires advanced analytical models to ingest multiple kinds of lifestyle, genomic, medical, and financial data.' The report questions whether existing health privacy laws, which were created before the age of big data, adequately address these uses. The Working Group concluded that modernising these laws 'will require careful negotiation between the many parties involved in delivering healthcare and insurance to Americans, but the potential economic and health benefits make it well worth the effort.'

Similarly, the Working Group recognised that big data provides numerous potential benefits for K-12 and university education, creating new ways for teachers to communicate with students and to better understand whether students understand the class material. But the Working Group also stated that 'some of the information revealed when a user interacts with a digital education platform can be very personal, including aptitude for particular types of learning and performance relative to other students.' The Working Group stated that the students' personal information must be 'protected from inappropriate uses, especially when it is gathered in an educational context.' This view, which the Education Department echoed in a February 2014 report, could pose challenges for companies that provide free, advertising based cloud services and software to schools.

No discrimination

Among the most pernicious forms of data use, according to the report, is discrimination based on race, socio-economic status, and other impermissible factors. The White House Working Group writes that such discrimination 'can be the inadvertent outcome of the way big data technologies are structured and used. It can also be the result of intent to prey on

vulnerable classes.' Big data provides companies and government agencies with 'the ability to segment the population and to stratify consumer experiences so seamlessly as to be almost undetectable,' the Working Group wrote.

For instance, the White House report cites a City of Boston program that allowed residents to use their smartphones' accelerometers and GPS functions to provide the city with information about potholes and other road conditions. Because low income residents are less likely to own smartphones, the Working Group wrote, the program could 'have the effect of systematically directing city services to wealthier neighborhoods populated by smartphone users.' (The report did compliment the City on finding ways to overcome that result, particularly by ensuring that road crews and inspectors focusing on less prosperous areas used the technology to discover road problems in those communities.)

At the federal level, the E-Verify program enables employers to confirm whether new hires are legally permitted to work in the United States. According to a 2009 report, the program had a much higher error rate for non-citizens. The Working Group concluded that 'technical issues like this could create higher barriers to employment or other critical needs for certain individuals and groups, making imperative the importance of accuracy, transparency, and redress in big data systems.' Such a conclusion is likely familiar to those who follow European privacy issues. One of seven principles of the EU Data Protection Directive is 'access,' meaning that individuals have a right to see all data that is collected about them, and to correct inaccurate information. Although the United States provides a limited right of access to such information in some circumstances, this report suggests that some believe the access right should be broader.

In addition to challenging the common US practice of focusing on data collection, the White House report questions whether the notice-and-consent approach to privacy is adequate in the age of big data

Notice and consent

In addition to challenging the common US practice of focusing on data collection, the White House report questions whether the notice-and-consent approach to privacy is adequate in the age of big data. Under this model, organisations describe their privacy practices in lengthy privacy policies, and consumers provide their 'consent' by clicking a button. The Working Group noted that the trend toward ubiquitous data collection and the difficulty of remaining anonymous 'may require us to look closely at the notice and consent framework that has been a central pillar of how privacy practices have been organized for more than four decades.'

Recommendations

In light of these conclusions about big data, the Working Group made the following policy recommendations:

- Enact legislation that codifies the Privacy Bill of Rights: In 2012, the White House released a Consumer Privacy Bill of Rights, which calls for six general privacy principles, such as security and transparency. The Working Group calls on the Commerce Department to draft legislation that would codify these principles into law.
- Pass National Data Breach Legislation: Currently, 47 states have enacted laws that require companies to notify consumers if certain types of personal information are compromised in data breaches. The Working Group calls on Congress to pass a single nationwide notification standard.
- Protect the privacy of non-US persons: The Working Group concludes that the Privacy Act of 1974, which regulates government collection and use of personal information, should, when practicable, extend to non-US persons.
- Limit data that is collected in schools to educational uses: Recognising the sensitivity of student data, the Working Group seeks to prevent the use of this information for commercial purposes.
- Prevent big data-based discrimination: The Working Group calls on anti-discrimination agencies and consumer protection regulators to ensure that big data is not used to discriminate against individuals.
- Amend the Electronic Communications Privacy Act (ECPA): This statute, which was passed in 1986, protects the privacy of phone and email communications. A wide range of critics agree that the law is outdated and must be updated for the digital age, and the Working Group agrees.

In sum, although the Working Group's report does not create new law, it does provide a clear and comprehensive picture of the administration's privacy priorities over the next few years. The report is particularly noteworthy for its focus on data use, rather than the traditional US focus on collection and notice.

Kurt Wimmer Partner
Jeffrey Kosseff Associate
Covington & Burling LLP, Washington DC
kwimmer@cov.com
jkosseff@cov.com

European VAT moves to a destination principle of taxation

New EU rules on VAT, coming into effect on 1 January 2015, will mean that business-to-consumer supplies of electronic, telephone and broadcasting services will be subject to VAT based on the jurisdiction the consumer is in, rather than the supplier. This will have implications for e-commerce services, such as online auction sites and app stores. Chris Hutley-Hurst of Skadden, Arps, Slate, Meagher & Flom LLP (UK) discusses the forthcoming VAT changes and their impact.

Introduction

From 1 January 2015, new EU VAT rules will apply to cross-border business-to-consumer (B2C) supplies of electronic, telephone and broadcasting services, where the supplier and the recipient are located in different Member States. Broadly, the new rules will mean that the service is subjected to VAT in the jurisdiction of the end consumer rather than the jurisdiction of the supplier. This 'destination principle' of taxation (i.e. tax in the jurisdiction of the consumer) reflects the fact that VAT is a tax on consumption. The new rules will also mean that EU businesses are put on the same footing as non-EU businesses.

Whilst the new rules apply to electronic, telephone and broadcasting services, this article will focus only on electronic services (e-services) being provided to non-business end consumers, which include video streaming, music and video downloads, app downloads, e-books, gaming, software and online auctions. Further, these new rules do not apply to cross-border business-to-business services (B2B), which as a general matter are subjected to VAT in the jurisdiction of the recipient, who accounts for the VAT (subject to certain overrides).

Current rules

Under the current rules, the VAT treatment of e-services to EU-based consumers differs, depending on whether the supplier is established outside the EU (non-EU suppliers), or inside the EU (EU suppliers):

- E-services supplied by non-EU suppliers are treated as taking place in the recipient's Member State; and
- E-services supplied by EU suppliers are treated as taking place in the supplier's Member State.

Non-EU suppliers are therefore obliged to register and account for VAT in each Member State in which an end consumer is based (subject to any local thresholds). EU suppliers, however, are only obliged to register and account for VAT in the Member State in which they are established.

EU suppliers located in a low-VAT Member State can therefore have a competitive advantage over non-EU suppliers, as non-EU suppliers charge the consumer VAT at the rate applicable in the consumer's home Member State, which can be higher.

Further, EU suppliers only have to account for VAT in their home Member State, whereas non-EU suppliers face a higher compliance burden of accounting for VAT in multiple jurisdictions, although this burden is eased by the VAT on E-Services (VoES) Scheme, which (subject to certain conditions) broadly allows a non-EU supplier the option of registering for VAT in a single Member State of its choosing, and accounting to that Member State for the VAT that it charges EU consumers (at their relevant domestic rates). Under VoES, the non-EU supplier submits a single quarterly electronic VAT return to the Member State of registration, with the return setting out the amount of, for e.g., UK VAT, Spanish VAT, French VAT, etc. The Member State then distributes the various VAT revenues to the other Member States in which the services are consumed.

This differing treatment between EU and non-EU suppliers has led to a practice where international businesses establish a supplier entity in a low-VAT jurisdiction, such as Luxembourg, so that consumers throughout the EU are charged the lowest VAT rate possible on supplies of e-services, and so as to reduce the business's compliance burdens.

New rules

From 1 January 2015 EU suppliers of B2C e-services will, broadly, be treated in the same way as non-EU suppliers, so that the supply will attract VAT in the consumer's home jurisdiction.

Mini One-Stop-Shop (MOSS)

To ease the administrative burden of EU suppliers having to register and account for VAT in multiple Member States, EU suppliers will have the option to use the MOSS scheme, which is similar to the VoES scheme currently available to non-EU suppliers in that it involves the EU supplier electronically filing a single VAT return to its home Member State, but accounting for the VAT due in the various Member States of its customers. EU suppliers can register for MOSS from October 2014.

Ascertaining the supplier

EU suppliers of B2C e-services will be liable to account for the VAT on their supplies, it is important to ascertain the identity of the supplier for VAT purposes. EU suppliers that supply e-services via online portals, marketplaces, or

gateways ('gateways') will need to consider whether they are making their supply through the gateways, in which case their supply is B2C, or to the gateways, in which case their supply is B2B. Where the EU supplier is making a B2B supply to the gateway, it is not treated as making supplies to end consumers, and the B2C rules should therefore apply to the gateway instead. Whether an EU supplier is making a supply to or through the gateway will be both a question of fact and a question of the terms of the contract between the EU supplier and the gateway. Typically, if the gateway sets the general terms and conditions of the supply to the consumer, authorises payment or delivery, or does not clearly state the EU supplier's name on the receipt or invoice issued to the consumer, then it is likely that the gateway will be treated as making the B2C supply, even if it is only acting as an agent.

Ascertaining a consumer's home Member State

EU suppliers must be able to identify the Member State where their customer is 'established' for VAT purposes, as this will be the Member State in which the supply of e-services is treated as taking place. For individuals, this home Member State is typically where they have their permanent address or where they usually reside.

For e-services, the customer's home Member State will depend on the consumer location as follows[1]. If the service is supplied:

- through a Wi-Fi hot spot, the consumer location will be where the Wi-Fi hotspot is located;
- on board transport travelling between different EU Member States (for example, by boat or train), the consumer location will be the place of departure for the journey;
- through an individual consumer's telephone landline, the consumer location will be the place where the landline is located; and
- through a mobile phone, the consumer location will be the country code of the SIM card.

It is entirely possible for a consumer to mask the location from which they are actually accessing the internet, and so an EU supplier may believe that a customer is physically accessing the e-service from a different Member State than is actually the case

Where one of the above applies, the EU supplier is only required to retain evidence showing the relevant place set out above. However, practical difficulties can arise from the above. A consumer that accesses e-services whilst travelling outside his/her home Member State could end up paying differing rates of VAT. Further, some e-services suppliers don't look to the geographic area from which the customer is accessing the e-services at any particular time, but instead look to the customer's home address (typically the address at which the payment card is registered). Finally, in order to access geographic-specific content, it is entirely possible for a consumer to mask the location from which they are actually accessing the internet, and so an EU supplier may believe that a customer is physically accessing the e-service from a different Member State than is actually the case.

To deal with these, and various other, practical issues arising from the above rules, an EU supplier can use alternate evidence to ascertain the customer's home Member State. To do so, the EU supplier must obtain two pieces of non-contradictory evidence supporting the home Member State. The evidence can include:

- customer billing address;
- customer IP address;
- location of customer bank;
- country code of SIM card in customer's phone;
- location of the customer's fixed land line through which the service is supplied to him/her; and
- other commercially relevant information.

Therefore, it is (quite rightly) open to EU suppliers to ascertain the customer's home Member State by use of billing address and bank location, such that the customer is charged VAT at that Member State's applicable rate, irrespective of whether the customer is travelling when he/she accesses the relevant e-service.

Conclusion

The new rules will bring the VAT treatment of EU suppliers into line with the current treatment of non-EU suppliers. The application of the 'destination principle' of VAT to intra-EU B2C supplies of e-services will also mean that VAT applies like the consumption tax that it is meant to be. EU suppliers will suffer an increased compliance burden, as they will have to apply differing VAT rates to their supplies, depending on the customer's home Member State. However, the MOSS is meant to minimise this burden. Consumers may also see a price increase where the EU supplier passes on any increase in the VAT rate chargeable as the place of supply switches from a low-VAT to a higher-VAT Member State.

Chris Hutley-Hurst European Counsel
Skadden, Arps, Slate, Meagher & Flom LLP, London
Chris.Hutley-Hurst@skadden.com

The views in this article are the author's own, and do not necessary reflect those of Skadden, Arps, Slate, Meagher & Flom LLP.

1. Note that other rules apply in relation to telephone and broadcasting services.

Eight pointers for protecting personal data while processing

In May this year the UK Information Commissioner's Office published its report 'Protecting data in online services,' which details eight computer security issues that may pose a threat to the protection of personal data processed by computer systems. Philip James, a Partner at Sheridans, analyses each of the issues highlighted in the ICO's report and examines what can be done to mitigate the risk to personal data in each of the eight areas.

Introduction

The UK Information Commissioner (ICO) has recently published a report that focusses on what it sees as the most significant threats to data protection in relation to personal data that is processed by computer systems. The report is of particular interest to organisations that are operating in an online environment. The report deals with eight computer security issues that have frequently come to the attention of the ICO during investigations of breaches of the Data Protection Act 1998 (DPA) and these are dealt with individually below. A key theme of the report is the importance of organisations staying up-to-date with advances in technology and being aware of new threats to cybersecurity before they occur. Any organisation operating within an IT environment must therefore ensure that it continually maintains and monitors the technical and organisational measures it has in place to protect personal data.

As in the case of any cybersecurity measures, it is important to remember that technological measures only form part of the solution. It is essential to have in place adequate, and equally robust, processes and organisational precautions (such as the promotion of security risk awareness and even an incentivised culture amongst a workforce) to meet the challenges posed by threats to information security. Some of the issues set out below will be obvious to even perhaps some of the least sophisticated companies and concerns. However, it is often the basic fundamentals that are ignored in favour of less obvious, but more high profile or attractive measures. If they do the fundamentals well, organisations will be a significant way down the track to developing a more secure environment.

1. Software security updates

No software is perfect and over time even the most secure and reliable software will develop bugs or errors. Attackers typically run automated scans across a range of online services searching for un-patched, out-dated or otherwise vulnerable software to attack. It is therefore important that any software used to process personal data is subject to an appropriate security updates policy. If there are a number of parties involved with the management of computer systems it is important that the parties have clearly set out who is responsible for maintaining software updates and that there are no gaps.

2. SQL injection

SQL injection affects applications that pass user input to databases in an insecure manner. Typically this can occur in a publicly available website that uses a database, in order to display information. Since SQL injection flaws are introduced in the source code of applications, it is important that the person responsible for maintaining the source code of any application used is clearly identified.

3. Unnecessary services

An important principle in network security is only to run the services that are absolutely necessary. This will then reduce the number of ways an attacker might compromise systems on the network. Where services are publicly accessible and are not being actively used, this unnecessarily exposes a range of potential avenues of attack. Which services a business considers as 'necessary' will inevitably be fact specific depending on the cost-benefit analysis of each service for any particular business. A classic example of this is a legacy communication line that is still active but is rarely used. There are however some general examples of services that are suitable for use within a trusted network, but which should not be made available to the internet. Typically, these services should be contained within the relevant local area network (LAN) by using correctly configured firewalls. Examples include direct database access, Universal Plug 'n' Play and Simple Network Management Protocol.

4. Decommissioning of software or services

Within large organisations that have been operating for a large number of years there may well be old computing services that are no longer needed. It is important that such systems that are no longer used are decommissioned thoroughly, otherwise they may continue to pose a risk. This risk could be direct, such as when a service is inadvertently left running and accessible. However, there may also be secondary risks resulting from failure to remove components such as binary executables or configuration files, which may help an attacker if they attempt a multi-layered attack. Where an organisation makes use

of temporary systems, for example as a test or pilot, a record of such systems should be made so that it is clear which systems will eventually need to be disabled.

5. Password storage

Although it may seem obvious, the fact that users' access credentials are particularly valuable to attackers is often overlooked by organisations. The secure handling of passwords is therefore of vital importance to reduce the adverse consequences of an otherwise successful attack which has defeated other security measures. Recent experience of the eBay password incident clearly indicates that it is not only the security of passwords that is of importance, but the deployment of an effective response and risk management plan should users' passwords be compromised. Techniques such as 'hashing' and 'salting' can be utilised to help improve the strength of password security (this uses encryption to reduce the likelihood of third parties reversing a hashed password to obtain the underlying real password).

As computing hardware becomes more sophisticated the ability to crack passwords also becomes more efficient. It is therefore important for organisations to periodically review the strength of any 'hashing' method that they use and that they stay up-to-date with advancements in computer power. Another simple method that organisations can use to improve the robustness of password storage is to ensure that users are educated in how to ensure they have a strong password (i.e. by using a wide range of letters and symbols and avoiding recognisable words).

6. Configuration of SSL or TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are closely related encryption schemes used for ensuring secure communications across the internet. Organisations should have a clear idea of which information needs to be encrypted and which does not, and thus apply the use of SSL or TLS appropriately. It may be most cost effective for an organisation to simply use SSL or TLS throughout the whole domain.

Organisations should change the default credentials (typically username and password) that are provided with software components as soon as possible, normally before development or testing begins, and certainly before the relevant software component is put into production

7. Inappropriate locations for processing data

The ICO has recognised that a large number of data breaches are caused by personal data being processed in an inappropriate location because of either poor security architecture or personal data being inadvertently stored in a publicly accessible location. With regards to security architecture the use of segmentation strategies and the application of policies according to network zone rather than individual systems can provide organisations with scalable approaches to increasing the strength of system security. Another common approach to improving security architecture is the use of on-site and off-site backups. In cases involving the storing of personal data in a widely-accessible location the ICO recognises that this is usually due to human error such as failure to realise that the storage place is widely accessible or failing to realise the personal nature of the data in the first place. There are, however, technical policies that can be put in place to help reduce these errors. For example, if an organisation needs to process particularly sensitive information, it may choose to set up a network which is isolated from any other network, to avoid an unintended data transfer. A similar effect could be achieved by using internal firewall policies.

From a geographical perspective, it is essential for organisations therefore to determine early on in devising a solution or network where the appropriate forum is located to store and process certain categories of data.

8. Default credentials

Organisations should change the default credentials (typically username and password) that are provided with software components as soon as possible, normally before development or testing begins, and certainly before the relevant software component is put into production. Failure to do so means that any personal data processed using that system or service could be at risk from unauthorised access. Again, this may seem obvious, but many organisations are unaware of how easy it is for an attacker to access systems using default credentials that can be accessed with relative ease. When changing default credentials it is also important for organisations to follow good practice on strong password choice as outlined above.

Related guidelines

In a related set of guidance, organisations should also refer to recent guidance, issued by HM Government, known as 'Cyber Essentials'[1]. Again, the guidance is focussed on technical measures (as opposed to organisational precautions). Nonetheless, it is a very useful starting point and checklist for smaller to medium sized organisations.

Philip James Partner
Sheridans, London
pjames@sheridans.co.uk

1. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/301383/BIS-14-696_Cyber_Essentials_Requirements_scheme_basic_technical_protection_from_cyber_attacksV2.pdf for further details.

HOT TOPIC: Wearables

E-Commerce Law & Policy explores the opportunities and challenges presented by wearable technology, with perspectives from three jurisdictions around the world.

UK

Every footstep, heartbeat, ailment, location visited and event witnessed will be captured, stored and uploaded to the nefarious cloud - here lies the future of wearable tech. From Google Glass to elaborate health assessment clothing, wearable tech will be the next disruptive technology.

From a legal perspective, the potential problems are as vast as the opportunity is exciting. Intellectual property will be at greater risk of being copied and transferred, employers will need to be careful about employees covertly monitoring and recording every word and businesses will face the contradiction of having potential access to an array of data whilst having to address the ever increasing rise in laws to protect an individual's privacy.

Legislators including the court will find themselves facing situations where the law fails to move at the same speed as the technology it is attempting to assess. Needless to say, lawyers will be busy assessing and reassessing policies, data permissions and procedures in order to protect their clients' interests.

The development of wearable tech is exciting although we may all have to wait until the Cupertino giants at Apple introduce the iWatch before we all start craving for something without knowing why we really need it…

Garry Mackay Partner and Joint Chief Executive Officer
Ashfords LLP, Bristol
g.mackay@ashfords.co.uk

Belgium

Google Glass gives its users hands-free access to a variety of smartphone online features. In its current form, Google Glass can, among other uses, pull information from the web, take photographs, record videos and provide navigation services. Applying current European data protection laws to such wearable technology raises many legal challenges, even though most laws exempt processing for domestic, household and recreational purposes from their scope. Fears of ubiquitous surveillance of non-users by users, whether through such recordings or through other applications currently being developed, have been raised.

Users will therefore have to understand (via a clear privacy policy) how to use Google Glass and where the sensitivities lie, not only in respect of themselves but also any non-users being filmed and recorded. The data protection regulators in the US, EU, Australia, Canada, Mexico and New Zealand have already indicated that Google, as a data controller, will have to address such issues which, most notably, relate to the privacy safeguards put in place by Google and app developers, the extent of the information collected by Google and shared by third parties (e.g., marketers, users' employers, insurers and authorities), the ways in which and the purposes for which the information will be used, and sharing and security measures. Google has already indicated that it will not use the facial recognition function of Google Glass and that its privacy policy will address both users and non-users.

Karin Retzer Partner
Alja Poler De Zwart Associate
Morrison & Foerster, Brussels
KRetzer@mofo.com
APolerDeZwart@mofo.com

Spain

Wearables represent a business opportunity for e-commerce in the near future, but we should not lose track of the new challenges behind these devices.

On one hand, wearables can lead to the emergence of markets of new accessories to facilitate users' lives with a high degree of customisation and functionality. These devices can also lead to new forms of technical innovation as well as the creation of new markets, but also involve a list of legal challenges.

As an example, what about protecting these devices in terms of design, patent registering and software rights as well as ensuring the right law is applied depending on the country where the devices are sold?

In my opinion, there is another, special challenge in this regard: simply finding the balance between the benefit wearables represent to users in terms of control and improvement through the use of these devices to aspects of their life: for e.g., health status or walking or sports habits, and how manufacturers deal with all that priceless private data. In this very case, more information means more business too.

Big data is the future but, is there any limit between privacy and doing business with it? Nowadays, the world's legislation runs at a much slower rate compared to the speed markets move.

That is why we need lithe and fast international legal instruments in order to regulate these situations in days to come. Again, here we are with a new challenge.

Vanesa Alarcón Partner & Co-Manager
Avatic Abogados, Spain
valarcon@avaticabogados.com