Linklaters

June 2015

Technology Media and Telecommunication.

EU – Data protection authorities fight to regulate Facebook

Facebook's 1.44 billion active users make it custodian of the world's largest hoard of personal information. As a result, it is subject to fierce regulatory scrutiny by data protection authorities, who are increasingly keen to directly regulate its activities. The Belgian Privacy Commission recently decided it has jurisdiction over Facebook by virtue of Facebook's public affairs office in Brussels. We consider the background to this decision and the wider implications, particularly for US organisations operating in the EU.

Updating privacy policies – A high risk activity?

In November 2014, Facebook announced an update to its data protection policies, effective 1 January 2015. The changes affected, in particular, the way Facebook users are followed outside Facebook's own website. Unlike previous changes to Facebook's policies, no vote by the Facebook users' community was foreseen.

Updating your privacy policy is a risky business as demonstrated by Google's ill-fated update to its privacy policy in 2012. Facebook's 2015 update resulted in multiple questions to the Belgian Privacy Commission (the "**Commission**") from users, media and public authorities.

The Commission launched a major investigation. It consulted with other data protection authorities, instructed two Belgian universities to produce a joint report and enrolled leading experts in the field. Moreover, the report on the basis of which the Commission adopted the Recommendation was drafted jointly by its President and its Vice-President, further underlining the importance of the matter in the Commission's eyes.

Following this investigation, heavy correspondence and a hearing with Facebook, the Commission issued Recommendation No. 04/2015 in May 2015. In this document, the Commission assumed jurisdiction over Facebook and found Facebook's tracking of users via social media plug-ins does not comply with Belgian data protection law.

While the Commission cannot itself impose fines or enforce orders, it can refer the matter to the courts and its recommendations carry authority, especially when they contain such a direct allegation of potential violations to

Contents

EU – Data protection authorities fight to regulate Facebook 1

EU – Digital Single Market Strategy: Difficult choices on the road ahead 5

Australia – Your "metadata" as personal information 9

Belgium – Court rejects copyright levy on ISPs 12

Belgium – Final cookie rules released 14

Belgium/Luxembourg – Creation of a more unified mobile market 17

Singapore - Guidance on managing data breaches: Three key takeaways..... 18

Poland – New mandatory privacy audits..... 21

UK - *Google v Vidal-Hall*: A green light for compensation claims? 23

UK – The Information Commissioner cracks down on direct marketing 26

Belgian data protection law. The Commission also announced further steps, including a second recommendation to be released later this year.

As the dust settles, it is worth looking into the reasoning of the Commission and the wider implications, in particular regarding its territorial competence.

"One stop shop" regulation under the Directive

The territorial issues focus on the validity of the "single EU controller" model put forward by Facebook and other organisations, particularly US tech companies. In summary, Facebook has adopted a structure along the following lines:

> it has one single establishment in the EU in the sense of the data protection laws, namely Facebook Ireland Limited. Other entities in the EU, such as the one in Belgium, do not process user data and so Facebook does not consider them relevant from a data protection perspective. Any use of equipment by Facebook Ireland Limited in other Member States, e.g. cookies, is also irrelevant because of the existence of an EU establishment (thus excluding the operation of article 4(1)(c) of the Directive);

> Facebook Ireland Limited is the data controller for personal data about EU -ased users, with whom users enter into an agreement when joining the site; and

> Facebook, Inc. in the US acts as a data processor, processing EU personal data on behalf of Facebook Ireland Limited.

The advantage of the "single EU controller" model is that Facebook, in theory, becomes subject solely to Irish data protection laws and that the Irish data protection authority is the only competent regulator in the EU. This has two significant advantages:

> Facebook effectively obtains a "one-stop-shop" approach, a concept currently discussed in the context of the overhaul of the EU data protection rules. Facebook can focus its compliance efforts and resources on one national law and deal with one single regulator for all its activities in the EU; and

> while, in theory, all Member States should have similar data protection laws as a result of implementing the Data Protection Directive, Ireland is seen as having a very pragmatic data protection regime. Indeed, some other data protection authorities have concerns it is too pragmatic.

Attack on the "single EU controller model"

The Recommendation contains two key arguments against Facebook's single EU controller structure.

First, the Commission challenges the qualification of Facebook Ireland Limited as a data controller. For that purpose, the Commission refers to reports filed by Facebook, Inc. with the US Securities and Exchange

Commission as well as other factual elements, underlining the fact that Facebook acts as a group and that the Irish entity does not have any effective decision-making power or autonomy vis-à-vis the US parent company.

Secondly, the Commission relies heavily on the European Court of Justice decision of 13 May 2014 in *Google Spain* (Case C-131/12), which specifically addressed the concept of establishment.

In that decision, the ECJ found an establishment in one jurisdiction whose activities "are inextricably linked" to the activities of a data controller in a second jurisdiction, is sufficient to trigger the application of the relevant national law of the first establishment to the processing of the data controller in the second jurisdiction. This applies regardless of whether that first establishment itself is involved in the processing of personal data (see paras 52 and 56).

Accordingly, the Commission found Facebook's establishment in Belgium engages in activities which are inextricably linked to Facebook, Inc. in the US and that the Belgian data protection law applies as a result.

This is a significant extension to the principles in *Google Spain*. Google's establishment in Spain was actively involved in the selling of advertising space, activities intimately linked with Google's core business. In contrast, Facebook's establishment in Belgium is essentially a public affairs office, a much less core activity.

Beware the long arm of European privacy laws

Facebook is not the only organisation to adopt a "single EU controller" structure. However, for it to work, there must be an establishment in the EU acting as an actual data controller in the sense of the Data Protection Directive 95/46/EC. The Commission's decision makes it clear this must involve real decision-making powers rather than being a manufactured construct.

The Commission has also taken a very expansive view of what constitutes a linked establishment beyond the already broad interpretation of the ECJ in the *Google Spain* case. If a public affairs office can be qualified as an establishment triggering the application of the law, it seems possible that any presence in an Member State will potentially trigger the application of the local data protection law to other members of the group.

This appears to stretch the Data Protection Directive to a breaking point, given it was only intended to apply to data processing operations when they are "carried out in the context of the activities" of the establishment of a data controller.

Substantive findings – "Like" button unliked

The Commission's substantive analysis focused on tracking performed by Facebook outside its social networking website using so-called "social media plug-ins", i.e. the "Facebook" buttons present on numerous websites. These plug-ins are used by Facebook to place third party cookies on the computers

of both Facebook users and non-users. They allow Facebook to follow what users are doing outside the social network's own pages.

This tracking requires consent and the Commission considered such consent was not sufficiently free, specific, informed and unambiguous.

The Commission also considered the position of others affected by these social media plug-ins recommending that:

> website operators who include social media plug-ins on their website should put in place mechanisms to limit the tracking which can be made using such plug-ins; and

> end users should take measures to protect themselves against tracking by using browser add-ons and activating the "private" mode of their browsers.

Addressing the recommendations to local website operators follows a trend common to many issues that arise on the internet. Those actors closer to home find themselves under the spotlight when the ultimate source of the problem is harder to reach. It recently emerged that German consumers' advocates successfully pressured a number of companies, including well-known skin-cream producer Nivea, to remove the Facebook thumbs-up button from their German web pages.

Conclusion

While the Recommendation remains a non-binding instrument, it is a first step in an escalating discussion between EU data protection authorities and Facebook. It is also a symptom of a wider debate over the simultaneous application of data protection laws in several jurisdictions and companies' attempts to streamline their compliance.

Facebook and other US tech companies should prepare for increasingly tougher questions in the coming months as the debate heats up.

The Recommendation is available in French and Dutch.

The report from the two Belgian universities is available here.

By Tanguy Van Overstraeten and Guillaume Couneson, Brussels

EU – Digital Single Market Strategy: Difficult choices on the road ahead

The development of a single market for digital activities in the EU is hampered by cross-border barriers and differences in national telecoms, spectrum, copyright, e-commerce, data protection and consumer law regimes. The Commission's Digital Single Market Strategy is intended to overcome these barriers but, in many areas, will require the resolution of difficult regulatory and policy issues.

The Commission's Digital Single Market Strategy

In May 2015, the European Commission released its Digital Single Market Strategy as a first step towards remedying the fragmentation of the single market and the dampening effect this has on commercial opportunities and consumer welfare. The Strategy describes a digital single market as:

"one in which the free movement of goods, persons, services and capital is ensured and where citizens, individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence"

The Commission anticipates that a unified digital landscape would boost economic growth, potentially bringing about an increase of EUR 415 billion in European GDP in total. The Strategy has three pillars:

> Better access for consumers and businesses to online goods and services across Europe.

> Creating the right conditions for digital networks and services to flourish.

> Maximising the growth potential of the European Digital Economy.

For each of these pillars, the Strategy identifies a series of actions (sixteen in total) to be undertaken during 2015 and 2016. Several of the core actions are described below.

Better access for consumers and businesses

E-commerce rules – By the end of 2015, the Commission will propose harmonised EU rules for online purchases of digital content and a set of core EU contractual rights for online sales of tangible goods domestically and internationally. Sellers could rely upon their national laws but key rights and obligations, including guarantee periods and remedies for non-performance, would be standardised throughout the EU. To enforce these standards, the Commission also plans to bolster co-ordination of consumer protection by enforcement authorities and to create an online dispute resolution platform for the EU in 2016.

Copyright harmonisation - National copyright regimes are also a focus of the Commission's strategies. In late 2015, the Commission will issue legislative proposals to reduce the disparities between different countries' copyright

regimes. It will also review the Satellite and Cable Directive by 2016. As the Strategy explains, a balance must be struck between improving cross-border access to content and preserving content creators' rights. Key priorities include allowing educational institutions to use copyright-protected material more readily (particularly via cross-border text and data mining), and promoting a fair civil enforcement regime which incentivises content creation but does not unjustifiably restrict the use of copyright material. How these priorities will be balanced in practice remains unclear.

Prevention of "unjustified" geo-blocking - European consumers are often prevented from purchasing content from a Member State other than their own and may be unable to access content they have purchased in their home country when they travel elsewhere in the EU. The Commission has identified "unjustified" geo-blocking as a form of territorial segmentation and therefore an obstacle to a single digital market.

Little detail is provided to differentiate "justified" and "unjustified" geo-blocking – the Commission evidently considers geo-blocking in order to comply with legislation justifiable but makes few decisions with regard to the other possible rationales canvassed in its Working Document. By way of action, the Commission will consider whether to amend the e-Commerce framework or the provisions of Article 20 of the Services Directive, as well as conducting a Competition Sector Inquiry which will assess the interaction of competition law and e-commerce.

There may be significant specific carve-outs to supplement "justified" geo-blocking. For example, a working group has been formed from four of Europe's key film industry organisations to put forward an alternative proposal for better film access and distribution throughout Europe that would avoid the need for geo-blocking rules. The group's conclusions should be released in September.

Allowing digital networks and services to flourish

Telecoms regulation - The Strategy advocates a stronger single market approach to telecoms regulation and the radio spectrum. The Commission will propose strategies to achieve a more consistent, standardised approach to spectrum assignment and management at an EU-wide level. Building on the planned Telecoms Single Market package, the Commission will also recommend changes to existing legislation in order to foster regulatory consistency and create a more competitive market with fewer barriers to entry.

Online platforms and intermediaries - The Commission will assess the role of online platforms and intermediaries. It will consider the widely-discussed issues of transparency (including in paid advertising), platforms' use of the vast quantity of data they accrue and measures taken by intermediaries to reduce or remove illegal content. It will evaluate the extent to which intermediaries such as internet service providers should be responsible for removing illegal content and how such a responsibility might interact with their

rights under the e-Commerce Directive, particularly the exemptions from liability they are afforded.

The review of platforms and intermediaries has proven one of the Strategy's most controversial proposals. Some commentators characterise it primarily as an attack on the market power wielded by US-based platforms such as Google and Facebook. Others go as far as to suggest that in its most extreme form it may pose a threat to free speech – for instance, if platforms are to be required to review and censor user content before it goes online. To its credit, the Commission suggests no extreme measures of that kind in the Strategy and acknowledges the importance of free speech, asserting that decisions will be made "with due regard to their impact on the fundamental right to freedom of expression and information".

Cybersecurity and data protection - The Strategy notes that only 22% of Europeans trust search engines, social networking sites, email services and similar companies completely, and that much of that distrust relates to the collection and use of personal data online. Reflecting this public concern, the Commission will establish a Public-Private Partnership on cybersecurity in early 2016.

Given the Strategy's timeframe and aims, the Commission describes the adoption of the General Data Protection Regulation by the co-legislator as an "urgent priority". Once that adoption has happened, the Commission will consider whether the e-Privacy Directive adequately protects data subjects and whether it treats various entities in the market equally.

Maximising growth

Building a data economy - The final pillar of the Strategy looks to the future and new initiatives to build a unified digital economy in Europe. The Commission envisions the free movement of data within Europe, including the development of a "European Cloud" to encourage greater provision and uptake of cloud services in Europe. Specifically, the Commission will need to consider certification, cloud contracts, users' ability to change providers and the possible creation of "a research open science cloud".

E-government - The Commission will also produce an "e-Government Action Plan 2016-2020". The Plan's objectives will include:

> linking business registers across Europe by 2017;

> testing the "Once-Only" principle, according to which individuals would only need to supply information once to public authorities;

> working towards a "Single Digital Gateway" which would consolidate contact points between public authorities, businesses and citizens; and

> assisting Member States to move more quickly towards full public e-procurement (currently scheduled for completion in October 2018).

The Commission claims that these changes should assist European startups to rapidly scale up their operations: "*any established company should be able*

to expand its operations cross-border online and be pan-European within a month".

Interoperability and standardisation - While the third pillar is largely innovative, like its counterparts, it emphasises standardisation. By the end of 2015, the Commission will adopt a "Priority ICT Standards Plan" for the standardisation of key technologies and domains, with a specific focus on the areas of transportation, health, energy and the environment. As a complementary measure, the existing European Interoperability Framework detailing the standards required for interoperability between Member States will also be extended.

Next steps and likely impact of the Strategy

The Strategy is ambitious both in scope and its aim of removing "provincialism" in Member States' digital markets. In addition, many of the actions it outlines are contingent on potentially lengthy planning, proposal and implementation processes. Some actions, especially those relating to copyright, geo-blocking and online platforms, are likely to face regulatory and political obstacles.

Given these challenges the full support of the European Council and Parliament will prove crucial. The European Council will consider the Strategy at its meeting on 25 and 26 June 2015 and the Parliament is developing an own-initiative report on the digital market. But support from the wider digital market is also needed. There is little point in optimising the theoretical conditions for the digital single market to flourish if providers are, in practice, unwilling to enter that market in the number and scale required.

The Commission's Communication on a Digital Single Market is available here

By Stephanie Essey, London

Australia – Your "metadata" as personal information

In May, the Australian Privacy Commissioner clarified that 'metadata' may be personal information where an organisation has the capacity and resources to link that information to an individual. We report on the Commissioner's determination, which found that Telstra breached the Privacy Act by failing to provide an individual with access to his metadata.

The facts

On 15 June 2013, Ben Grubb requested access under the *Privacy Act 1988 (Cth)* to all metadata Telstra stored about him in relation to his mobile phone service. His request included cell tower logs, inbound call and text details, duration of data sessions and telephone calls, and the URLs of websites visited. His request acknowledged that Telstra may charge him a fee.

Telstra's initial response notified him that he could access information on his outbound mobile call details and the length of his data usage sessions via online billing, but that his inbound call, text metadata and other metadata would not be released.

Mr Grubb lodged a complaint against Telstra in August 2013 with the Office of the Australian Information Commissioner, of which the Privacy Commissioner (the "**Commissioner**") is part. He sought a declaration that Telstra meet its access obligations under the Privacy Act.

Between the lodging of the complaint and the time of the Commissioner's decision, Telstra's policy on customer access to metadata changed, allowing customers to access the same metadata about them that Telstra would provide to law enforcement agencies on request. Telstra's new policy aligns with upcoming changes to the *Telecommunications (Interception and Access) Act 1979 (Cth)* ("**TIA**") that will require service providers to retain specified metadata and treat such metadata as 'personal information' that is subject to the Privacy Act. Telstra then released much of the requested metadata to Mr Grubb. However, Telstra continued to refuse access to:

> IP address information;

> URL information; and

> cell tower location information beyond that which Telstra retains for billing purposes.

The determination

The Commissioner found that IP address information, URL information and cell tower location information relating to Mr Grubb's use of his mobile phone service was his 'personal information' under the Privacy Act. There was also a question of whether inbound call information could be accessed; the Commissioner ultimately found that this information could not be released because it would compromise the privacy of other individuals.

The Commissioner declared under section 52(1)(b) of the Privacy Act that Telstra:

> had breached NPP 6.1 (now APP 12.1) of the Privacy Act by failing to provide Mr Grubb with access to personal information that Telstra held on him;

> must provide Mr Grubb with access to his personal information in the form of IP address, URL and cell tower location information (to the extent it had not already done so); and

> must provide Mr Grubb with access to the above information free of charge given that resolution of the matter had been drawn out by Telstra maintaining that metadata sought by Mr Grubb was not personal information.

The basis for the determination

The Australian Privacy Principles ("**APPs**") came into effect on 12 March 2014 and replace the National Privacy Principles ("**NPPs**"). The Commissioner's determination on this matter, however, was made under the NPPs because the matter related to events that occurred prior to 12 March 2014.

The Commissioner first assessed whether the metadata was information about Mr Grubb and found that it was because the relevant URLs, IP address and cell tower location information could be linked to Mr Grubb.

The identity of Mr Grubb was reasonably ascertainable. In making his determination, the Commissioner broke his consideration of 'reasonably ascertainable' into two parts:

> is it possible for the identity of the individual to be ascertained? and

> if it is possible, is the process of ascertaining the identity of the individual reasonable in the circumstances?

The Commissioner found that it was not only possible for Telstra to ascertain an individual's identity through inquiries and cross-matching against different network and records managements systems, but that it already had processes in place to do so in order to allow it to respond to requests from law enforcement agencies.

The Commissioner rejected Telstra's arguments that the processes involved in retrieving such information were not reasonable given the complexity, time and cost required. He instead found that such processes are not '*beyond what is reasonable relative to the resources [Telstra] has at its disposal and its existing operational capacities*.'

It is unlikely that the Commissioner's analysis would be any different under the new definition of 'personal information' that was introduced on 12 March 2014. The new definition would require the Commissioner to assess whether the metadata is information about an individual who is 'reasonably identifiable'. The narrower definition of personal information, which applied prior to 12 March 2014, was applied in this case, with the Commissioner concluding that the metadata in question amounted to information from which the individual's identity can be 'reasonably ascertained'. This finding suggests

that metadata becomes personal information by its association with other personal information of the individual, such as their name. If anything, the grounds for such metadata being personal information have strengthened under the new definition, which only requires such metadata to be information about an individual who is 'reasonably identifiable', and not information from which the individual's identity can be 'reasonably ascertained'.

Watch this space

Telstra has already announced that it will appeal the Commissioner's determination. It is supported by the Communications Alliance, a telecommunications industry body that represents the communications industry. The Communications Alliance has described the Commissioner's decision as a *'stark example of regulatory overreach'*, and flagged that this decision will only increase the cost burden for telecommunication companies already facing the burden of hundreds of millions of dollars in additional costs due to the incoming mandatory data-retention scheme.

The Communications Alliance has also pointed out that law enforcement agencies are likely to use the Commissioner's determination as grounds for seeking broader access rights to metadata than those currently provided for under the new mandatory data retention scheme which is being introduced through amendments to the TIA.

The incoming amendments to the TIA (here), restrict the types of metadata that service providers (telecommunications carriers, carriage service providers and internet service providers) are required to retain for the purposes outlined in the TIA. This limited data set is deemed personal information for the purposes of the Privacy Act, and service providers must disclose this retained data to the person to whom it relates.

The Commissioner's determination that URLs also fall within metadata that an individual has rights to access, goes beyond what was envisaged as metadata in the amendments to the TIA. Retention of URLs had been purposely excluded from the new mandatory data retention scheme to ensure that only data that does not go to the content of a communication is retained for the mandatory two-year period.

The determination is available here.

By Michael Pattison, Priyanka Nair and Leah Wickman, Allens, Melbourne

Belgium – Court rejects copyright levy on ISPs

The internet has created significant challenges for rights holders seeking to prevent, or at least obtain some compensation for, the infringement of their works online. The Belgian courts have now rejected the latest innovation, i.e. to impose a copyright levy directly on internet service providers.

SABAM: From filtering to copyright levy

SABAM is one of the major Belgian authors' rights collecting societies. It was previously in the headlines for its failed attempt to force ISPs to implement general filtering on their network to prevent copyright infringement (see *Scarlet Extended SA v SABAM* C-70/10, discussed here).

SABAM's new approach was to send internet service providers a letter requesting the payment of a levy of 3.4% of the annual subscription fees for each internet user. This levy would be due in return for authorising the communication to the public of the protected works in SABAM's catalogue by those internet service providers.

However, the Belgian Ministry of Economy, which oversees SABAM, considered this to overstep Belgian copyright law. It sought an injunction against SABAM to suspend this initiative; a move supported by the main Belgian internet service providers.

Is there a communication to the public?

The decision hinged on whether the activities of internet service providers can be qualified as a "communication to the public" within the meaning of Belgian and European copyright law.

SABAM argued the internet service providers' activities amount to a communication to the public which is different from the original communication to the public by the originator of the communication, e.g. either another internet user or service providers such as Youtube or Spotify.

In contrast, the Belgian State and the internet service providers considered that the internet service providers only have a technical and passive role in the communication to the public and that SABAM's distinction is artificial. In reality, there is only one single communication to the public by the originator of the communication.

Decision of the Court

In March 2015, the President of the Brussels Court of First Instance rejected SABAM's arguments. In relation to:

> *the uploading of protected works*, the court considered that the transmission of content from a user's computer to an internet service provider does not qualify as a communication to the public. Internet service providers cannot be considered as a "public" as defined under EU and Belgian copyright law (i.e. "public" means an indeterminate number of potential recipients and implies, moreover, a fairly large number of persons).

> *the downloading of protected works*, the court considered that internet service providers only act as technical intermediaries and do not initiate a communication to the public distinct from the original communication.

Accordingly, SABAM's payment request violates Belgian copyright law as there is no legal basis for such request absent a communication to the public.

Conclusion

The Brussels Court of First Instance recognises the collection of royalties directly with the internet service providers would be convenient from a technical perspective, but this alone is not sufficient. It also points SABAM to the originators of the communications to the public as the persons owing royalties, acknowledging that to collect those royalties remains very challenging.

By Guillaume Couneson and Clément Legrand, Brussels

Belgium – Final cookie rules released

The Belgian Privacy Commission (the "**Commission**") has now completed its consultation on the use of cookies (see here) and issued a final opinion. Amongst other things, it contains guidance on how to obtain consent to the use of cookies and the responsibilities of the various players in the online value chain.

Guidance on consent

The final opinion (the "**Opinion**") confirms that, in principle, consent has to be obtained prior to placing or accessing of cookies on a user's computer. The Commission however accepts that consent can be inferred if a user continues to surf on a website after having been informed about the use of cookies in certain circumstances.

The Opinion provides further practical guidance in relation to obtaining appropriate consent. The main recommendations are to:

> enable the user to give consent via a positive action, such as the ticking of a box;

> refrain from using mechanisms that solely request unconditional consent, without any room for choice by the user;

> refrain from imposing negative consequences (such as website access restrictions) as a result of a refusal to accept cookies;

> refrain from using classic pop-ups to get consent as most of them are automatically blocked by browsers and can be intrusive;

> instead use a banner on the homepage (on the side, top or bottom) to notify the user about the use of cookies, as these are most likely to attract attention. Another possibility is a banner shown before allowing access to the website; and

> ask users to pre-set their preferences with regard to cookies upon registration.

Specific recommendations for the online value chain

In addition to the above general guidance, the Opinion also contains practical recommendations for each person in the online value chain. The main ones are summarised below.

The owner of the website – They are considered by the Commission as ultimately responsible as data controller for the use of cookies on the website. They should:

> provide the publisher and administrator of the website with clear instructions on the use of cookies, e.g. via a specific security policy, more general working regulations or individual statements, declarations or contracts imposing binding obligations on the publisher and administrator in this respect;

> inform the visitors about the use of cookies and provide instructions on how to erase their tracks. The Opinion suggest this should be done using a cookie policy, which should be made easily accessible to visitors on the homepage; and

> make advertising space available only when there is a binding agreement with the advertiser under which transferred data is subject to the Belgian Data Protection Act. If not, the owner risks liability in case of violation of the rules by the advertiser.

The publisher of the website – They are responsible for putting in place the actual data processing mechanisms when creating the website's content, including cookies. They should inform the owner of their use of cookies and act in accordance with the latter's instructions. The publisher should:

> ensure that the cookie policy is easily accessible via the homepage (the Opinion recommends a link at the bottom of the page with a clear reference);

> make sure that cookies which are subject to consent, such as social network buttons and advertising banners, do not appear automatically on the homepage (see also in this respect the recent Facebook recommendation of the Commission, here);

> in order to obtain consent, make use of either a special menu in which the visitor can select the purposes for which it allows cookies or provide a general consent button (if only one type of cookies is used); and

> erase cookies containing personal data immediately at the end of the session.

The advertiser – They are data controller of the data provided by the visited website. The advertiser should ensure that a written agreement is put in place setting out the purposes and conditions for the reuse of the collected personal data. This will enable the publisher of the website to obtain informed consent from visitors

The website administrator – They act as a data processor, should only act upon instruction of the owner of the website and will be responsible for any actions undertaken outside of such instructions, which can derive from an employment or service agreement. The administrator should check whether personal data are anonymised and erased in a timely manner from the server.

The host of the website – They act as data processor on behalf of the owner of the website, but may also act as data controller in relation to additional data processed in order to enable the proper functioning of the services (e.g. information regarding activity on the website such as statistics or logs). A data processing agreement should be in place in relation to the processing performed on behalf of the website owner.

The visitor or user – Finally, the Commission recommends that the visitor of the website (data subject) should only give his/her consent for the use of cookies when he/she is properly informed about the possible consequences of his/her consent, e.g. when a cookie policy is made available.

Conclusion

The Opinion is important as it constitutes official guidance on the use of cookies in Belgium. The detailed recommendations to the different entities in the value chain is useful and should enable them to verify whether their current cookie related compliance mechanisms are in line with the Commission's guidance.

By Guillaume Couneson and Emma Ottoy, Brussels

Belgium/Luxembourg – Creation of a more unified mobile market

In April 2015, the Belgian and Luxembourg telecom regulators announced an agreement to create a more unified telecoms market. Mobile operators will be able to offer consumers in Belgium and Luxembourg the chance to call, text and surf at their usual national rate in both countries, effectively removing roaming charges.

Background

Technically, the agreement (the "**Agreement**") entered into by the Belgian and Luxembourg telecom regulators will make it possible to combine a Belgian mobile number with a Luxembourg international mobile subscriber identity or "IMSI" number, i.e. the unique number enabling the authentication of a mobile phone on mobile networks. The regulators also announced a Ministerial Decision to allow extraterritorial use of IMSI numbers for that purpose.

This technical solution was agreed on the basis of a principle of reciprocity. As a result, Luxembourg and Belgian operators will enjoy the same rights and will be able to offer services in both countries without application of roaming charges.

First commercial offer

The regulator's joint press release indicates that Luxembourg-based JOIN Experience will be the first to develop a service offering on the basis of the Agreement. The regulators hope that other operators will follow and that this initiative will ultimately result in lower prices and a wider variety of services being made available to customers.

Significance for the EU telecoms market

This development comes at a time when the Council of the EU and the European Parliament are debating when to remove roaming charges in the EU altogether. The move towards a more unified telecoms market in the BeLux region will undoubtedly be closely monitored by regulators and mobile operators alike, as it provides a testing ground for the removal of roaming charges at EU level.

Moreover, if the experience proves successful and the removal of roaming charges is delayed at EU level, similar bilateral agreements between regulators may provide a way forward in the short term.

The Agreement is available here

By Guillaume Couneson, Brussels, and Olivier Reisch, Luxembourg

Singapore - Guidance on managing data breaches: Three key takeaways

In May 2015, Singapore's national privacy regulator issued new guidance on managing data breaches. We consider three key aspects; breach notification obligations, embedding a privacy culture and the cost of data breaches.

Overview of the Guide

The Personal Data Protection Act only came into force in July 2014 and so the privacy landscape is still relatively new in Singapore. The Personal Data Protection Commission which enforces the Act has therefore issued a range of guidance including a Guide to Managing Data Breaches.

The Guide provides some insight into the Commission's expectations with regard to the way organisations respond to and manage data breaches, and encourages organisations to pro-actively develop and implement a data breach management and response plan.

In summary, the Guide suggests that each organisation's data breach management and response plan should include the following sets of activities:

C ontaining the data breach	Certain key actions should be taken as soon as an organisation is aware that a data breach has occurred (e.g. shutting down the compromised system that led to the data breach)
A ssessing risks and impact	The affected individuals and data should be identified along with the causes of the breach, and the consequences should be assessed
R eporting the incident	Organisations should plan whom, what, how, and when notification should be made when a data breach occurs
E valuating the response and recovery to prevent future breaches	Evaluate whether existing protection and prevention measures are sufficient to prevent similar breaches from occurring

The Guide also recommends that a data breach management team is appointed and that its details be made known within the organisation. This will provide a clear command and reporting structure of key employees who would take charge and make time-critical decisions on steps to be taken to contain the breach and manage the incident.

We set out below three key takeaways from the Guide that may be useful to your organisation:

Takeaway 1: Notifying individuals and regulators

There is currently no mandatory notification requirement imposed on organisations involved in a data breach. However, the Guide states it is generally good practice to notify the following persons after a data breach has been discovered:

> the individuals whose personal data have been compromised;

> interested third parties where relevant, e.g. banks, credit card companies, etc.;

> the police and other authorities where relevant, e.g. the Monetary Authority of Singapore; and

> the Commission itself.

Where the data breach may cause public concern or where it involves sensitive personal data, the Guide recommends that notification should be given to these persons *immediately*. These persons should be informed of the details of the data breach, including what types of personal data were involved in the data breach, how the organisation will be responding to the data breach, and the contact details and how affected individuals can reach the organisation for further information or assistance.

The urgency of the situation should be considered in deciding how notification should be made, e.g. media releases, social media, emails, etc. Updates should also be given to affected individuals when the data breach is resolved.

While the lack of mandatory notification obligation may tempt some organisations not to notify the Commission, the Guide states that failure to do so will affect its decision on whether an organisation has complied with its obligation in the Act to protect personal data. Given this clear steer from the Commission, organisations should develop clear notification procedures internally in order to manage data breaches effectively in the future.

Takeaway 2: Embed a culture of data privacy

Human error features as one of the primary causes of data breaches in organisations. These human errors include:

> unauthorised or accidental disclosure of personal data to third parties; or

> improper disposal of documents and other items containing personal data.

Robust sets of policies (e.g. security policies, social media policies, etc.) that employees are expected to adhere to are one way to mitigate this risk, but the risk is they remain as mere “paper tigers”.

A better way to combat human error is to embed a culture of data privacy among employees. In tandem with the internal policies mentioned above,

training sessions should be conducted to educate employees about the obligations of the Act, e.g. how to identify personal data, what can and cannot be done with personal data, and what to do in the event of a data breach. This should include practical examples in dealing with personal data that employees may face in the course of their employment.

Finally, the contact details of a key contact person within the organisation (e.g. the Data Protection Officer) should be made known to employees so they can defer any privacy-related queries they may have to him/her.

Takeaway 3: Fines are the tip of the liability iceberg

Organisations are often concerned about the possibility of incurring an administrative penalty issued by the Commission of up to S$1 million to ensure compliance with the obligations of the Act. However, the liabilities an organisation faces from a data breach are much wider than administrative penalties and include:

> *Costs of investigations*: The costs of investigating high profile data breaches to determine their cause and the exact data lost can be significant.

> *Costs of rectification*: New data security systems/policies may have to be implemented under directions by the Commission arising from its investigation of a breach. This may need to be done on an urgent basis and can incur significant costs.

> *Costs of civil litigation*: Significant class action suits may be brought by affected individuals and other third parties against organisations for data breaches of highly sensitive personal data.

> *Business opportunity costs*: The Commission has the power under the Act to suspend use of personal data while investigations are ongoing, and there may be costly ramifications for certain businesses (e.g. banks not being allowed to use personal data to process credit card payments).

Finally, the reputational damage to the organisation surfacing from a data breach may have long-term ramifications on its business operations.

A full copy of the Guide can be accessed here.

By Adrian Fisher, Laure de Panafieu and Joel Cheang, Singapore

Poland – New mandatory privacy audits

The new rules on mandatory internal data protection audits have now come into force. We consider their impact on Polish data controllers and potential loopholes in this new law.

Background

The recent amendments to the Polish Act on the Protection of Personal Data (the "**PPD**") came into force on 1 January 2015 (more details here). Among other things, they introduced mandatory internal data protection audits. The details of these audits obligations are set out in a separate Regulation which is effective as of 30 May 2015.

The audits are aimed at verifying compliance with the provisions of the PPD and should be carried out by that data controller's information security officer. However, curiously, the recent changes to the PPD do not make the appointment of an information security officer mandatory.

Internal audits – Scheduled and ad hoc

Under the Regulation, an information security officer must carry out:

> *scheduled audits* – These are to be carried out in accordance with an audit plan, which specifies the date of a particular audit, the subject matter thereof, as well as the scope of activities undertaken during the audit. The audit plan must cover a period of not less than one quarter and not more than one year, and at least one audit must be carried out during that period; and

> *ad hoc or unscheduled audits* – These must be carried out without delay after an information security officer receives information on a personal data breach or there is a reasonable suspicion of such a breach.

In addition, the information security officer is obliged to perform similar audits at the request of the GIODO (the Polish Data Protection Authority) and the GIODO itself might decide to carry out its own inspection.

Outcome of the audit

The information security officer must prepare a report once the audit is complete. The report should include information on the date, names and location, a list of activities undertaken by the information security officer and a list of persons covered by the checks. It must also set out any remedial action to be taken to ensure compliance with the PPD.

The report on scheduled and ad hoc audits must be provided to a data controller. A report on an audit carried out at the request of the GIODO must be provided to the GIODO.

Loopholes in these requirements?

The intention of the recent amendments to the PPD was to reduce the regulatory burden on entrepreneurs, but it is not clear if this is the effect in

practice. Instead, the Regulation imposes new and onerous obligations on information security officers and indirectly also data controllers who have appointed such a person.

The Regulation also fails to clearly describe which data controllers are subject to these audits. In particular, it is not clear if they apply to data controllers who have not appointed an information security officer. In practice, they may deter data controllers from making such an appointment given the potential additional audit obligations that will entail.

By *Ewa Kurowska-Tober* and *Lukasz Czynienik*, Warsaw

UK - *Google v Vidal-Hall*: A green light for compensation claims?

In March, Google experienced yet another setback in European courts. This time the English Court of Appeal found against Google on three key issues arising out of its so-called Safari cookie workaround (see *Google v Vidal-Hall* [2015] EWCA Civ 311).

The first finding was that the claimants can serve proceedings on Google in the United States for the misuse of their private information and for breach of the Data Protection Act 1998.

The second is that there is an arguable case that browser-generated information ("**BGI**"), such as cookies, constitutes 'personal data'. This brings a whole swathe of Google's online activities into the scope of European data protection laws.

Finally, the Court found that the claimants can claim for distress without having to prove pecuniary loss. This greatly increases the scope for compensation claims in the future given an invasion of privacy will rarely be accompanied by actual monetary loss.

This article considers the decision in greater detail before considering its wider implications and the barriers that remain for compensations claims for breach of UK data protection law.

Background to the claim against Google

The Wall Street Journal first published allegations that Google was circumventing the Safari browser's privacy settings in February 2012. Six months later, Google had agreed to pay a record $22.5 million penalty to the US Federal Trade Commission for misrepresenting to its users what it was doing. However, it wasn't required to make any admission of wrongdoing.

The following year, the three claimants sought to bring a claim against Google for the tort of misuse of their private information and for a breach of its statutory duties as a data controller under the Data Protection Act 1998. The claims arose because Google tracked and collated information relating to their internet usage on the Safari browser between mid-2011 and early 2012.

As Google is a registered corporation in Delaware with its principal place of business in California, the claimants were required to obtain permission from the Master under the Civil Procedure Rules to serve proceedings abroad, which they were successful in doing. Google appealed that decision to the High Court and then the Court of Appeal. Assuming Google does not make a further appeal to the Supreme Court, the substantive claim can now proceed.

The long arm of UK privacy law

The first point considered by the Court of Appeal was whether the claimants were entitled to serve proceedings on Google in the United States for the misuse of their private information. Under the Civil Procedure Rules, this is only possible if this misuse is characterised as a tort rather than as an equitable remedy.

The Court of Appeal was, unsurprisingly, unwilling to let the historical distinctions between equity and the common law frustrate the claimants action and so confirmed that the misuse of private information is a tort. Google had already conceded that breach of the Data Protection Act 1998 would be a tort for these purposes. As the damage from that tort was sustained in the UK, the claimants were able to serve their claim out of jurisdiction on Google Inc in the US.

Browser-generated information as personal data

The second point arose from Google's argument that BGI was anonymous information. Accordingly, Google argued there was no serious issue to be tried that BGI is 'personal data' within the meaning of the Data Protection Act 1998.

The Court of Appeal had to consider a range of arguments. The first was whether the BGI identified an individual by itself. The Court of Appeal was satisfied it was seriously arguable. In focusing on the Opinion issued by the Working Party 29 on the concept of personal data, and the decision of the European Court of Justice in *Lindqvist*, it said the correct approach may be to consider whether the data "individuates" the individual, such that the individual is able to be differentiated from others. It is not necessary for the data to reveal information such as the actual name of the individual.

As the BGI told Google such information as the claimants' unique IP addresses, the websites they were visiting, and even their rough geographic location, Google knew their 'virtual address' and when they were at their 'virtual home'. Therefore, the Court of Appeal stated that it is likely that the individuals were sufficiently individuated and that the BGI on its own constitutes 'personal data'.

The Court of Appeal also considered two subsidiary points. Google argued that while it might be able to identify the claimants by aggregating their BGI with other information it holds about them, it would not do so in practice and therefore that potential combination should be ignored in determining if the BGI is personal data. The Court suggested Google was wrong on this point though did not make any definitive findings.

Equally, Google argued that BGI could not be deemed personal data because third parties might see targeted adverts on the claimants, computer based on that BGI. The Court of Appeal considered this point was neither clear-cut nor straightforward. Moreover, it was unnecessary for it to make any findings, given its earlier conclusion that there was a serious issue BGI might be personal on the basis set out above.

Claims for distress alone possible

Section 13(2) of the Data Protection Act 1998 states that an individual who suffers distress arising from a breach of the Act is entitled to compensation only if the individual "also suffers damage" (or the processing be for the so-called "special purposes"; journalistic, literary or artistic purposes).

This damage had previously been interpreted as meaning pecuniary loss. The need for claimants to prove pecuniary loss as a prerequisite to claiming for distress has required significant evidential contortions in the past, e.g. such as the Doctor and the second breakfast, see *Johnson v MDU* [2006] EWHC 321.

The Court of Appeal decided this was incompatible with the right to an effective remedy under Article 47 of the EU Charter of Fundamental Rights. What was needed was "*the disapplication of section 13(2), no more and no less*." In reaching its decision, the Court of Appeal held: "[s]*ince what the [Data Protection] Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage)".*

Will the floodgates open?

The fact litigants need no longer prove pecuniary loss in order to claim for distress, has to lead some commentators to suggest the opening of the proverbial floodgates to litigation. However, there are a number of factors that suggest this might not come to pass. Claims for breach of the Data Protection Act 1998 are potentially difficult given the complexity of the law in this area.

Moreover, compensation awards are typically small and may not provide sufficient incentive to bring such a claim. While we are still a long way from determining the level of compensation available in *Vidal-Hall,* it is likely to be dwarfed by the legal fees. Google's trial costs alone are estimated to be £1.2 million (though the Court did describe this figure as "extremely high").

This is less of an issue for many individual claims which can be brought though the small claims process and so escape any adverse cost orders. However, it will remain a significant deterrent to larger group actions; as will the "opt-in" nature of group litigation in the UK and the need for damage and distress to be assessed on a case by case basis, rather than by a global award.

By *Greg Palmer*, London

UK – The Information Commissioner cracks down on direct marketing

The last year has seen the Information Commissioner issue a series of fines to marketers who deliberately flout the UK's direct marketing rules. Changes to the enforcement regime are likely to lead to more fines in the future. He is also applying greater scrutiny to borderline activities, such as the recent undertaking from the Universities and Colleges Admissions Service not to "bundle" consent with other services. We consider the implications.

A sharp uptick in fines

One of the Information Commission's strongest sanctions is to fine an organisation. This is often seen as a weapon of last resort to be used only where the breach is so serious it needs to be sanctioned with a fine or a deterrent is needed against further breaches.

The increasing number of fines for breach of the direct marketing rules over the last year (see table below) shows the Information Commissioner believes that both sanction or deterrence are increasingly necessary. This is unsurprising given the increasing problem of spam text and nuisance calls - the Information Commissioner receives around 15,000 complaints per month for these breaches, peaking with 19,683 complaints in July 2014.

Three of these fines, known as monetary penalty notices, demonstrate not only the Information Commissioner's increased activity in this area but also the difficulties under the previous regime of making them stick.

Spam texts: Neibel – In June 2014, an Upper Tribunal overturned a fine of £300,000 against Christopher Niebel, director of Tetrus Telecoms, for sending spam texts. At the time, to issue an fine the Information Commissioner had to prove:

> a serious contravention of the direct marketing rules in the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**") had occurred;

> such breach was of a kind likely to have caused substantial damage or distress to the recipients; and

> the breach was deliberate or reckless.

The second requirement was most problematic. The Upper Tier Tribunal acknowledged Tetrus Telecoms has clearly breached PECR by sending hundreds of thousands of spam texts relating to PPI mis-selling and accident claims, without making any effort to ensure recipients had consented. However, the Information Commissioner could only bring forward evidence from 286 complainants who had received the spam texts in support of the contravention. The Upper Tier Tribunal found this evidence insufficient to show substantial damage or distress and dismissed the fine.

Breach of do not call register: Amber UPVC – The Information Commissioner has been more successful in more recent cases. In January 2015, the First Tier Tribunal upheld the £50,000 fine on Amber UPVC Fabrications Limited.

Under PECR, organisations may only carry out telemarketing to recipients enrolled in the Telephone Preference Service ("**TPS**") if they have the recipient's consent. The Information Commissioner brought evidence of over 500 complaints during a two year period from individuals subscribed to the TPS who had received unsolicited marketing calls from Amber. The First Tier Tribunal agreed Amber's conduct was not only a serious breach of PECR but also caused substantial distress to the recipients and merited the fine.

Breach of do not call register: Reactiv Media – This was followed by a First Tier Tribunal decision against Reactiv Media. The Information Commissioner's original £50,000 fine was not only upheld but increased to £75,000. Again, the Information Commissioner presented evidence that Reactiv Media was engaging in widespread unsolicited telemarketing to recipients listed on the TPS. Influenced by the decision in *Amber*, the First Tier Tribunal agreed the fine was justified. It argued (amongst other things) Reactiv Media showed a conscious disregard for its obligations under PECR when carrying out its business.

The difference in the tribunals' approach between the decisions in *Niebel* and *Amber / Reactiv Media* is not immediately obvious. However, it can in part be attributed to the differing marketing channels. Whilst an SMS can be annoying, it may be ignored or deleted. In contrast a live telephone call requires direct human interaction and demands attention, making it more likely to cause substantial damage or distress.

Greater ability to fine

Despite the successes in *Amber* and *Reactiv Media*, the decision in *Niebel* highlights the difficulties under the previous regime. Even where an organisation is deliberating flouting these laws it has often been tough for the Information Commissioner to present enough evidence to meet the substantial damage or distress threshold.

After a long campaign to rectify this issue, the government announced it would make it easier for the Information Commissioner to fine companies making nuisance calls or sending spam texts and emails. From April 2015, there is no need to prove substantial damage or distress in these cases. To issue a fine the Information Commissioner only needs to demonstrate there has been a serious contravention that was committed deliberately or recklessly. This clearly shifts the focus to the action and intention of the offender, rather than the effect on the victim (which, in cases of nuisance calls and spam texts, may be no more than irritation).

Greater focus on legitimate marketers

The Information Commissioner's focus has extended not only to those who flout the law but also those on the boundaries of the law.

In March 2014, the Guardian newspaper published an article questioning the Universities and Colleges Admissions Service's ("**UCAS**") direct marketing activities. In particular, UCAS "bundled" consent to direct marketing into the wider application process such that applicants could not refuse third party

commercial offers without also opting out of receiving potentially important information about careers, education and health. In addition, the default option on the registration form was to provide that consent.

The Information Commissioner's subsequent investigation found that was a breach of the direct marketing rules and UCAS gave formal undertakings to remedy the situation. The findings touch on several key elements of the current UK marketing regime.

Unfair processing – Specific marketing rules apply depending on the channel used (e.g. post, email, SMS, telephone) but all forms of direct marketing are subject to the Data Protection Act 1998 and must be fair and lawful. UCAS breached the fairness requirements as its privacy documents were not sufficiently transparent. It did not properly explain the marketing purposes for which it collected data and third parties with whom the data would be shared.

"Bundled" consent invalid – Under PECR, organisations may only send direct marketing emails or texts if the marketing is for its own products and services as part of an existing commercial relationship or they the have consent. In UCAS' case, advertising third party products such as energy drinks and mobile phones clearly required consent.

Under the European Data Protection Directive, consent must be freely given, specific and informed. The Information Commissioner decided the mechanism used by UCAS did not satisfy these requirements. In particular, bundling consent meant it was neither specific nor freely given as students felt obliged to consent for fear of missing out on important career information. In addition, the Information Commissioner suggested that opting applicants into marketing by default also meant consent was not valid. This conclusion is likely to be influenced by the quasi-monopoly status of UCAS and the inexperience of some students. The Information Commissioner suggested it was questionable whether younger applicants, some of whom might only be 13, have the capacity to consent in any event.

The undertakings require UCAS to:

> split out marketing consents; and

> provide applicants with more detail on use and sharing of their information.

These are not unreasonable but tougher than expected given UCAS' privacy policy already contains a relatively clear explanation of how an applicant's information may be used (including for marketing purposes) and students were able to opt out of marketing at any point. Similarly, UCAS only sent out marketing material on behalf of other organisations, it did not share applicants' actual data.

Conclusions

The public interest in stemming the tide of spam and unwanted cold calls, coupled with the Information Commissioners increased ability to impose fines for serious breaches, means enforcement action is only likely to grow.

It will be interesting to see if the Information Commissioner continues to focus his attentions on the "bad guys" who deliberately flout the law or whether reputable organisations with bullish marketing practices will also be in the regulator's crosshairs.

The UCAS undertaking is available here

By Dominic Bilham, Alaister Johnson and Clare Zucker, London

Recent marketing fines

Date	Offender	Grounds for the fine	Penalty
March 2015	Direct Assist Ltd	Making unsolicited marketing calls to individuals registered with the TPS.	£80,000
Dec 2014	Parklife Manchester Ltd	Sending unsolicited marketing text messages by disguising the identity of the person on whose behalf the messages were sent.	£70,000
Sept 2014	EMC Advisory Services Ltd	Making unsolicited marketing calls to individuals registered with the TPS.	£70,000
Sept 2014	Kwik Fix Plumbers Ltd	Making unsolicited marketing calls to individuals registered with the TPS.	£90,000
July 2014	Reactiv Media Limited	Making unsolicited marketing calls to individuals registered with the TPS.	£50,000
April 2014	Amber UPVC Fab. Ltd	Making unsolicited marketing calls to individuals registered with the TPS.	£50,000

Author: Peter Church

This publication is intended merely to highlight issues and not to be comprehensive, nor to provide legal advice. Should you have any questions on issues reported here or on other areas of law, please contact one of your regular contacts, or contact the editors.

© Linklaters LLP. All Rights reserved 2014

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The term partner in relation to Linklaters LLP is used to refer to a member of Linklaters LLP or an employee or consultant of Linklaters LLP or any of its affiliated firms or entities with equivalent standing and qualifications. A list of the names of the members of Linklaters LLP together with a list of those non-members who are designated as partners and their professional qualifications is open to inspection at its registered office, One Silk Street, London EC2Y 8HQ or on www.linklaters.com and such persons are either solicitors, registered foreign lawyers or European lawyers.

Please refer to www.linklaters.com/regulation for important information on our regulatory position.

We currently hold your contact details, which we use to send you newsletters such as this and for other marketing and business communications.

We use your contact details for our own internal purposes only. This information is available to our offices worldwide and to those of our associated firms.

If any of your details are incorrect or have recently changed, or if you no longer wish to receive this newsletter or other marketing communications, please let us know by emailing us at marketing.database@linklaters.com.

Contacts

For further information please contact:

Tanguy Van Overstraeten
Partner

(+32) 2501 9405

tvanover@linklaters.com

Peter Church
Solicitor

(+44) 20 7456 4395

peter.church@linklaters.com

One Silk Street
London EC2Y 8HQ

Telephone (+44) 20 7456 2000
Facsimile (+44) 20 7456 2222

Linklaters.com

A20010485/0.3a/15 Jun 2015