Linklaters

July 2013

Technology, Media and Telecommunications.

EU – Advocate General considers if Google is subject to European privacy laws

Google's relationship with European privacy regulators is currently fairly fractious, but it will take some comfort from a positive opinion from the Advocate General in a crucial case currently before the European Court, *Google v AEPD* (C-131/12).

The case arose out of an individual's request that information about him be removed from Google's search engine. It poses three important questions. What is the territorial scope of the European privacy laws? Do they apply to "intermediaries" such as Google? Do they provide a "right to be forgotten"?

The key finding is that, while US-based Google Inc. is subject to European data protection laws, it is only partly responsible – i.e. only partly a data controller – in respect of personal data contained in, or referenced by, its search engine. This conclusion appears to be driven by policy considerations and the difficulties in reconciling the broad and antiquated European data protection laws with the modern world of the internet. It raises uncomfortable questions about whether the Data Protection Directive is still fit for purpose.

The Advocate General's opinion is not binding on the European Court of Justice but is often followed in practice. The court is expected to give its ruling either later this year or early next year.

Forgetting the past

The dispute dates to a newspaper report in 1998 about the financial difficulties of a Mr Mario Gonzales. An electronic copy of the report was subsequently placed on the newspaper's website and indexed by Google's search engine.

In 2009, Mr Gonzales asked the newspaper to remove the publication as it was old and irrelevant. The newspaper refused to do so, so Mr Gonzales asked Google to remove that publication from its search engine. When Google also refused, he complained to the Spanish data protection authority, the *Agencia Española de Protección de Datos* ("**AEPD**").

The AEPD found that the report was part of the public record and so the newspaper did not have to remove it from its site. However, the AEPD

Contents

ordered Google to remove a link to the publication from its search engine. Google appealed to the national courts who, in turn, referred the matter to the European Court of Justice.

The reference just relates to Google's acquisition and indexation of personal data from the internet. It does not relate to the processing of personal data about users of Google's search engine and other services, though, given the current enforcement action by French and UK data protection authorities and others, these issues may also come before the European Court of Justice in due course.

What is the territorial scope of EU privacy laws?

The first question relates to the territorial scope of European data protection laws, an increasingly important issue given the transnational delivery of services across the internet, particularly by large US-based technology companies. In general terms, a data controller will be subject to the data protection laws of a particular Member State if it is either established in that state or is not established in the EU but uses equipment in that Member State.

The analysis here was complicated by the fact that Google's search engine is operated solely by Californian-based Google Inc. The only presence Google has in Spain is a subsidiary, Google Spain SL, which is only involved in promoting and selling advertising space on the search engine.

The opinion considered this was sufficient to make Google Inc. subject to Spanish data protection laws (article 4(1)(a) of the Directive). Google Inc. and Google Spain SL were an "*economic operator [that] must be considered as a single economic unit*". This conclusion is possible in light of other European jurisprudence on the concept of establishment, though one might normally expect greater analysis of the application of these principles in this case, for example, some analysis of the scope of operations of the Spanish subsidiary or its ability to act independently from Google Inc.

In addition, while data protection laws apply to an establishment in a Member State, this is limited to personal data processed in the "context of the activities of [that] establishment". Given that the only processing conducted by Google in Spain was limited to sales and marketing, it is not immediately clear why other processing conducted outside of that territory, i.e. the operation of the search engine itself, should also be caught.

In addition, while data protection laws apply to an establishment in a Member State, this is limited to personal data processed in the "*context of the activities of [that] establishment*". Given that the only processing conducted by Google in Spain was limited to sales and marketing, it is not immediately clear why other processing conducted outside of that territory, i.e. the operation of the search engine itself, should also be caught.

It is hard to avoid the conclusion this finding is based partly on policy considerations, as in other areas of the opinion. It is also arguably unnecessary. Google does in fact have data centres in Belgium and Finland.

This constitutes use of equipment in those jurisdictions and would appear to make Google's search engine subject to Belgian and Finnish data protection laws. It is not clear why Mr Gonzales could not simply make his complaint under those laws rather than have to rely on Spanish data protection law.

In any event, if the opinion is followed by the European Court of Justice, it raises a range of interesting questions about the country of origin principle in the Directive. Are parent companies generally subject to dual establishment in all of the jurisdictions in which they have subsidiaries? For example, might that parent have to comply with multiple, and potentially conflicting, national data protection laws and also make local notifications?

It could also undermine the approach taken by other US tech companies which have established themselves in European Member States with "business friendly" privacy laws. For example, Facebook established its main EU operations in Ireland, in part, so it would only have to consider Irish data protection law. However, Facebook also has local sales and marketing operations around Europe, so its main EU operations could presumably also have multiple establishments across the EU for data protection purposes.

Finally, these difficulties provide some context for the extra-territorial provisions in the General Data Protection Regulation. These would clearly capture US internet businesses providing goods or services into the EU or monitoring consumer behaviour, regardless of whether or not those businesses have a EU-based subsidiary. The position in the draft regulation has been pushed for by many privacy advocates out of fear that internet businesses such as Google search were not caught by the current Directive. If that is no longer the case - at least in the case of Google and its ilk - one key driver for the need for the new Regulation may no longer exist.

Are search engines subject to data protection laws?

Having found that Google Inc. was within the territorial scope of Spanish data protection laws, the next question was whether it was within the substantive scope of those laws. The question is essentially whether search engines such as Google Inc. are responsible – i.e. data controllers – in respect of personal data in their search engine.

Before answering that question, the Advocate General made some wider observations about European data protection laws. His conclusions, though perhaps not surprising, create significant uncertainty about the operation of the law. He concludes:

> when the Directive was passed in 1995 use of the internet was limited and search engines were in a nascent state. The development of the internet into "*a comprehensive global stock of information which is universally accessible and searchable was not foreseen by the Community legislator*";

> the Directive was given a wide scope of application when it was enacted to capture the range of technological developments at that time. However, its potential scope of application is now "*surprisingly*

wide" and will potentially apply to "*anyone today reading a newspaper on a tablet computer or following social media on a smartphone*" to the extent that it applies outside their purely private capacity; and

> this broad scope requires the European Court of Justice to "*apply a rule of reason … the principle of proportionality, in interpreting the scope of the Directive in order to avoid unreasonable and excessive legal consequences*".

With these factors in mind, the Advocate General had to evaluate whether Google is a data controller on the basis that it determines "the purposes and means of the processing of personal data" in its search engine (article 2(d) of the Directive).

The opinion considers that Google is not a data controller in respect of the personal data it refers to on third party websites provided it takes certain minimum steps in respect of that data such as regularly updating cached content in its servers and not indexing content from sites with search engine exclusion codes. This is on the basis that Google is not "*aware*" of the actual personal data on those third party websites, nor is it intending to process that personal data in any "*semantically relevant way*". In coming to this conclusion the opinion warns the Court against the "*irrational nature of the blind literal interpretation of the Directive*" which makes "*virtually everybody owning a smartphone or a tablet"* a data controller. It also states that making Google a data controller of this information would mean it would be impossible for it to comply with data protection laws because of the restrictions on processing sensitive personal data (which would inevitably be included in some third party websites).

However, Google is a data controller in respect of the "index of the search engine". Google's processing of the index is compatible with the Directive because it constitutes the pursuit of a legitimate interest (article 7(f) of the Directive) and its data quality duties in respect of accuracy, excessiveness etc. (article 6 of the Directive) are limited to accurately reflecting the content of the underlying website. In this respect, the processing should be seen as the "*provision of information location services*" and "*not an issue relating to the content of the source websites*".

This approach is pragmatic but, as a piece of judicial law making, raises a number of concerns. Firstly, the Advocate General suggests his approach is not consistent with the literal interpretation of the Directive. Neither is it likely to be consistent with the purposive interpretation given that the Directive was deliberately drafted to be as wide as possible. Instead, it appears to be an attempt to rewrite the laws on pure policy grounds through the creation of a new exemption for intermediaries such as Google that perform "*entirely passive and intermediary functions*".

Secondly, Google's search index is effectively a distillation of the information from those third party websites so, substantively, will contain nearly all of the same personal data. Some of that personal data in the index will also be sensitive, so what is the justification under the Directive for its processing by

Google? If Google might struggle to establish grounds for processing sensitive personal data in its cache of website pages, it will equally struggle to do so in respect of its index.

Thirdly, there is a great deal of uncertainty about the new concept of "awareness" and "intention" in determining if someone is a data controller and it is not clear if they are really needed. The concepts assist the Advocate General to conclude Google is not a data controller in respect of personal data referenced on third party websites. It might be easier to conclude Google is not a data controller on the simple basis that it has no control over their content, or the purpose for which it is processed.

Is there a "right to be forgotten"?

The final question is whether the Data Protection Directive already contains a "right to be forgotten" based on the right to erasure and blocking of data under article 12(b) and the right to object to processing under article 14(a).

The Advocate General's opinion is no. The right to erasure and blocking of data under article 12(b) is more relevant to incomplete or inaccurate data, and there was no suggestion in this case that the newspaper report on Mr Gonzales was not entirely true and accurate. Moreover, the right to object under article 14(a) arises where there are compelling legitimate grounds. The desire of a data subject to restrict or terminate the dissemination of true and accurate public information on the grounds that it is harmful or contrary to his interests does not satisfy this condition.

This conclusion is supported – in the Advocate General's view - by the presence in the proposed General Data Protection Regulation of an express right to be forgotten. That right has met considerable resistance and arguably has been so watered down in the latest versions of the Regulation as to have little practical effect. Still – in the Advocate General's view – it is more than a codification of existing law and instead is a legal "innovation".

The Advocate General took comfort from his view that the Charter of Fundamental Rights did not require the creation of any such right to be forgotten either. While Article 8 of the Charter guarantees a right to the protection of personal data, this must be balanced against the rights of freedom of expression and freedom of information in Article 11 of the Charter.

Finally, the opinion warns against trying to deal with this issue on a case-by-case basis. Search engines could not be expected to carry out any substantive review of every individual request to remove material from its results so would be likely to automatically withdraw that material instead. This would result in the suppression of legitimate and legal information which would conflict with, amongst other things, the important educational and historical value of this information (as recognised by the European Court of Human Rights in cases such as *Times Newspaper v UK*, Applications 3002/03 and 23676/03).

There are powerful arguments that a right to be forgotten risks the "falsification of history" but it is also important to note that this was not a borderline case. For example:

> there was no question the information about Mr Gonzales was correct;

> the underlying publisher was subject to Spanish data protection law. The AEPD had reviewed the matter and concluded that the newspaper was not required to remove the material from its website as it was part of the public record; and

> the information was not particularly personal. For example, it did not reveal any sensitive personal information about Mr Gonzales.

At the other extreme, it is easy to imagine a situation in which false, or deeply sensitive, personal information is hosted on a server based in a territory which has little respect for privacy rights and where the only real remedy of the affected individual is for links to that information to be removed from the search engines. Ultimately, the conclusion may still be that freedom of expression trumps protection of privacy, but the matter should be tested against a more challenging scenario.

Is the Data Protection Directive fit for purpose?

The issues of territoriality, material application and the right to be forgotten are all interesting. The Advocate General's opinion on these points is not binding on the European Court of Justice, and, while it is normally followed in practice, there are reasons why the court might not want to do so in this case. For example, the Court might:

> conclude Google's search engine is not "established" in Spain and not otherwise subject to Spanish data protection laws. This finding could also provide fresh impetus to finalise the General Data Protection Regulation which contains express extra-territorial provisions that would apply to Google's search engine; or

> find that Google is a data controller in respect of both its search index and the contents of the information referenced by that search index – i.e. reject the opinion's suggestion that Google is, in part, not a data controller because it is not "aware" of and does not "intend" to process personal data referenced by its searches. This would not suddenly require Google to remove the publication about Mr Gonzales' given the opinion's recommendation there should be no "right to be forgotten" in these circumstances. It would raise the question of how Google justifies its processing of sensitive personal data but this is a problem affecting all data controllers, and it is not clear why this case justifies redefining core concepts such as that of a data controller.

A more important question raised by the opinion is whether the Data Protection Directive is still fit for purpose. It was intentionally drafted in broad terms with concepts such as "personal data" capturing almost any information about identifiable individuals and "processing" capturing almost any conceivable operation of personal data.

This sits uneasily with the internet age, in which most individuals have access to computers, smartphones, the internet and social media. The opinion suggests we have a law that is so broad and all encompassing that it can no longer provide sensible conclusions on the basis of either a literal or, possibly, a purposive interpretation and instead must be interpreted on some form of "super purposive" basis using broad policy consideration. It is difficult to see how organisations can be expected to comply with these laws where their interpretation is necessarily driven by unpredictable and subjective policy-based considerations. The opinion itself states in relation to the jurisdictional question: "*it is no wonder that data protection experts have had considerable difficulty in interpreting [the Directive] in relation to the internet*".

One of the consequences of "super-purposive" interpretation is that it moves so far from the original text – drafted and negotiated painstakingly by legislators - it risks unintended consequences. For example, if the concepts of "awareness" and "intention" from the opinion are adopted they will create new problems determining if someone is a data controller. Maybe other organisations, besides Google, that store large amounts of personal data but have no intention of looking at it themselves might also no longer be data controllers, no longer subject to data security obligations or fair use requirements – ISPs capturing email traffic for government authorities for example?

Many would agree with Advocate General's obvious distrust of the current Directive. But if we have learnt anything in privacy over the last few years, it is that law made in haste makes matters worse. The opinion suggests we need a fresh approach to European privacy laws, but more than anything what we need is a fresh approach that will stand the test of time.

By Richard Cumbley and Peter Church, Linklaters LLP, London

An extended version of this article will appear in the July 2013 edition of World Data Protected Report. See http://www.bna.com/world-data-protection-p6718/ for further details

EU – Money, money, money. It's a Bitcoin world

The online currency known as Bitcoin has been steadily building momentum, most recently through the Winklevoss twins' (previously of Facebook fame) launch of an exchange-traded product to track the dollar price of Bitcoins. We consider what Bitcoins are, why they are used and whether they are more than a digital fool's gold.

How Bitcoins work

Bitcoin is in an internet-based payment system, whose unit of currency is also called the "Bitcoin". Whilst traditional currency uses central banks to issue currency and print cash, Bitcoin uses an open source algorithm run over a peer-to-peer network. That network is made up of Bitcoin users' computers and controls, monitors and verifies both the creation of new Bitcoins and the transfer of Bitcoins between users.

The network hosts a shared public ledger, the "block chain", which is collectively maintained to record all Bitcoin transactions. Each new transaction is broadcast across the Bitcoin network. Participating computers then communicate with each other to validate the transaction, this checks the block chain to confirm that the transaction has not already occurred and thereby preventing double spending, and updates the block chain appropriately. This process is computationally intensive, and is in fact the same process used to create new Bitcoins.

The Bitcoins themselves are mathematically generated at regular intervals, currently around 25 Bitcoins are created every 10 minutes. This is done through "Bitcoin mining" - using computers to execute increasingly difficult number-crunching tasks. The Bitcoin algorithm is designed so that it becomes more and more difficult to "mine" Bitcoins with the number of new Bitcoins generated slowly decreasing (it is halved every 4 years) until the year 2140, when this number will round down to zero. At that time the total number of Bitcoins will have reached its maximum of 21 million. At the time of writing, there are approximately 11 million in circulation.

Once mined, Bitcoins become tradable and can either be bought or sold on third party exchanges for real money or transferred directly across the internet to another user, for example as payment for goods and services.

A growing Bitcoin market

Bitcoin is in a relatively early state of development, and its adoption is still nowhere near as widespread as other internet-based payment systems such as PayPal, let alone any traditional currencies.

However, Bitcoin is growing rapidly. A number of service providers have been launched to enable online merchants to accept Bitcoins just as easily as they accept payments from Visa, MasterCard, or PayPal, such as BitPay, which was signing up around 100 to 120 merchants per day in April 2013. Bitcoin is also accepted as payment by a number of retailers, such as Etsy, Wordpress and OKCupid, and there are bars in London, Cambridge and New York which now accept Bitcoins. Further afield, one Finnish software developer has

offered to pay its employees in Bitcoin, and the world's first "Bitcoin baby" (i.e. a baby whose parents funded the IVF treatment through Bitcoins) has been born in Los Angeles.

So why has Bitcoin become more popular and what are its relative strengths and weaknesses compared to other payment systems?

Bitcoin's strengths

It is flexible, open and cheap - Fees for processing Bitcoin transactions are generally very low, as they are executed directly by the Bitcoin algorithm. Bitcoins can be transferred anywhere in the world at any time of day, and the transfers happen very quickly. There are no limits or safeguards as might exist in a traditional payment system (such as the need to prove your identity). These factors makes Bitcoin an attractive payment solution for a range of users, including developing economies, which might lack an accessible banking infrastructure or a stable currency.

It is decentralised – There are economic arguments for the use of Bitcoins as well. Milton Friedman proposed that central banking authorities should be replaced with an automated system which keeps the money supply growing at a steady, predictable rate. This would help spending and investment decisions to be made on a surer footing and prevent inflation. Due to the fixed nature of the algorithm creating Bitcoins, there is no way for a central authority to instigate Bitcoin quantitative easing, i.e. issuing a flood of new Bitcoins and devaluing those already in circulation. However, opponents argue that this steady release will result in deflation and an illiquid currency.The authorities also cannot freeze or block transfers of Bitcoins, so they are immune to the sorts of measures imposed in Cyprus earlier this year when the central bank froze many of the country's bank accounts.

It is relatively anonymous - Although all Bitcoin transactions are publicly recorded, they are not tied to a real world identity. Its users can therefore operate relatively anonymously. This might be useful for making payments which are intended to be private or to fund controversial causes (e.g. Wikileaks accepts Bitcoins). However, this anonymity also has a number of drawbacks, set out below.

Bitcoin's weaknesses

It can be used for criminal activities - The relative anonymity of Bitcoins means they can be used for criminal activities such as drug trading, tax evasion and money laundering. For example, there are websites that allow the trade in illegal drugs, such as the infamous Silk Road, that only accept Bitcoins. In this respect, Bitcoins are very similar to physical cash, though there are suggestions that law enforcement agencies are able to conduct complex statistical analysis to track down Bitcoin users.

It can be volatile - The price of Bitcoins can fluctuate wildly. For example, the price of 1 Bitcoin was $13 on 1 January 2013. In mid-April, it rose extremely quickly to about $266, before dropping to around $50 in two days. Supporters state that traditional currencies can be volatile as well.

It is too complicated to use – The software required to use Bitcoin is complex and will deter many users from adopting Bitcoin. However, that software may well become more user-friendly and similar criticisms were levelled at services such as PayPal when they were first launched.

It is susceptible to hacking or deletion - The core Bitcoin architecture is said to be extremely secure with little evidence of successful malicious attacks or exploitations to date. This is partly because the Bitcoin peer-to-peer network is distributed, meaning tens of thousands of servers would need to be hacked at once to disrupt its operation. *The Economist* even suggested it might be more secure than traditional banking architecture. The position for third party ancillary services is different, such as the exchanges on which Bitcoins can be bought and sold using traditional currency. For example, Mt. Gox, one of the largest Bitcoin exchanges, was subject to an number of "denial of service" attacks in April 2013 and was victim of a breach in information security where thousands of usernames and passwords were stolen.

Bitcoins can be lost - Like cash, Bitcoins can also be lost due to human error. They are normally stored using a "digital wallet", which is accessed via a password. If a user loses this password, the Bitcoins are also lost. Similarly, if the digital wallet is deleted (and not backed up) the Bitcoins will be irretrievably lost. For example Stefan Thomas had three copies of his wallet, yet inadvertently managed to erase two of them and lose his password for the third. He lost about 7,000 Bitcoins, at the time worth about $140,000.

It is a poor use of computing power – Bitcoins are mined using computers to execute increasingly difficult number-crunching tasks so "miners" often build extremely powerful computers, or even hijack other people's computers. As a result, the Bitcoin network is now considered by some to be the world's largest and most powerful. This has been criticised as both a poor use of computing power and as being extremely damaging for the environment, given the electricity consumed by Bitcoin rigs.

Regulatory impact

Unsurprisingly, the growth of Bitcoins has also attracted regulatory attention. In October 2012, the European Central Bank issued a report on virtual currency, which indicated that Bitcoin may become the subject of regulatory interest in the European Union.

The Global Forum on Law, Justice and Development organised a roundtable discussion held at the World Bank on 14 June 2013 to discuss legal and regulatory challenges associated with Bitcoins (and other virtual currencies), during which an ECB representative stated, that although Bitcoin is not yet regulated, it posed a "challenge for authorities" and did fall within central banks' responsibility.

In the UK, it has been recently reported that the Financial Conduct Authority has been petitioned by a number of Bitcoin exchanges to actively regulate Bitcoin and to licence Bitcoin exchanges. The rationale for this is that those Bitcoin exchanges believe that regulated status would help to build trust in the Bitcoin platform with the general public. However, at this time neither the

Financial Conduct Authority or the Prudential Regulation Authority licence such businesses and have not made any statements as to whether 'Bitcoins' should or could be classed as specified investments for the purposes of UK financial services legislation. However, given that Bitcoin exchanges handle funds, they are likely to be caught by the UK's anti-money laundering and sanctions regimes, which are broader in scope.

There has been similar interest in the US. For example, the Financial Crimes Enforcement Network (FinCEN), a bureau of the United States Department of the Treasury, recently issued a report regarding the legal status of centralised and decentralised "virtual currencies", such as Bitcoin. Amongst FinCEN's findings were that American Bitcoin miners might have to register, and become regulated, as money service businesses and that American Bitcoin exchanges should also be regulated and subject to, amongst other things, money laundering regulations.

California's Department of Financial Institutions has also issued a cease and desist letter to the Bitcoin Foundation. It accused the Foundation of engaging in money transmission without obtaining a licence or proper authorisation to do so under the California Financial Code.

What is clear is that at the present time, whilst showing significant interest in Bitcoin, regulators around the world have not yet reached any form of consensus about whether such virtual currencies fall within their regulatory remit. In many cases further legislation may ultimately be required to clarify the position, both for the Bitcoin market and for the regulators.

The future of Bitcoin

The Bitcoin economy is now estimated to be worth more than $1 billion so further attempts at regulation seem likely. That regulation could be damaging to Bitcoin by clamping down on its use, beneficial, by providing Bitcoins with greater legitimacy, or simply ineffectual given it operates through a decentralised peer-to-peer network.

In any event, the internet has produced many new and disruptive technologies over the past decade. Whether Bitcoin is the latest iteration, revolutionising our perception of money, or simply another passing fad, remains to be seen.

By Andrew Byrne and Will Hallatt, London

EU – Key factors when deciding on a data centre location

Data centres are a critical part of many organisations' infrastructure and are likely to require further investment given the rise of Big Data and the expectation in today's online society that real-time access to information will be available around the clock and around the world. However, building a data centre is a major investment that requires careful analysis.

One key issue is the location of the data centre. What will be the most appropriate location is influenced by a wide range of technical, economic, environmental and geopolitical factors. It is also influenced by legal and regulatory factors, including restrictions on data transfers in the jurisdiction in which the organisation is based and surveillance and disclosure laws in the jurisdiction in which the data centre is located, a point thrown into sharp focus by the recent revelations about the US PRISM program. We consider these factors in more detail below.

The Data Centre Risk Index

The Data Centre Risk Index is an annual report published by Cushman & Wakefield, hurleypalmerflatt and Source8. It highlights the main points influencing uptime and service continuity, acknowledging that data centre downtime can potentially lead to substantial negative impacts on revenues and customer services and thereby cause irreparable harm to a business' reputation.

The report ranks 30 countries, made up of a mix of established data centre locations, emerging markets and key regional centres. The ranking is based on the top risks likely to affect the successful operation of a data centre, weighted to reflect their relative importance. These are physical, economic and social risks, such as energy cost and availability, connectivity, labour cost, political stability, ease of doing business, water availability, sustainability and risk of natural disasters.

The 2013 edition suggests that the Nordic region is one of the best places to locate corporate data centres, largely due to the high percentage of energy coming from renewable resources, the availability of natural resources, the low risk of natural disasters, the political stability and the ease of doing business. Thanks to these factors, the region dominates the top 10, with Sweden ranked as the third safest location worldwide.

The US is still considered to be the lowest risk data centre location worldwide, due to low energy costs, international bandwidth and ease of doing business, with natural disasters being the most significant detraction. The UK maintains its position as the lowest risk data centre location in Europe and the second safest place worldwide, thanks to its level of connectivity and ease of doing business. However, rising energy costs and a heavy reliance on fossil fuels is raised as a concern for the future.

Legal and regulatory framework

While commercial considerations will often be a key factor in deciding where a data centre is located, in addition to the factors considered in the Data

Centre Risk Index, the impact of the legal and regulatory framework on the location of any data centre must also be carefully considered.

Surveillance and disclosure laws

Although still ranked by the Data Centre Risk Index as the safest location worldwide to locate a data centre, the recent revelations about the US PRISM system – a system used by the U.S. National Security Agency to gain access to private communications of users of various popular internet services – may very well affect companies' attitudes to its suitability. However, the existence of national surveillance program,es is not a new feature, nor is it in any way isolated to the US or its government. Many other governments, including European governments, also have extensive powers to access data, e.g. through rights of interception of data and various disclosure requirements (for example, see our previous review of *Law Enforcement and Cloud Computing*, October 2011). It is also worth considering how regulatory enquiries for information from foreign authorities and disclosure requests issued by foreign courts will be handled.

The risk of government access has been a major factor in some companies' choice of data centre location, which, in some cases, has led to locations such as Switzerland being selected based on the strict protection given to information in that jurisdictions. However, it is not just a question of disclosures towards public authorities, as civil litigation disclosure can also be a risk in some jurisdictions. Although disclosure obligations are relatively common, the extent of those obligations varies and can be particularly wide in common law jurisdictions.

Restrictions on data transfers and other factors

It is also necessary to consider any legal barriers that prevent data from being freely transferred. Data privacy regulations are perhaps the best known restriction. For example, the countries within the EU are subject to the EU Data Protection Directive, which restricts transfers of personal data to countries outside the European Economic Area that are not considered to have an adequate level of protection for personal data. Many other jurisdictions have similar data privacy laws that restrict transfers of data to other jurisdictions. For the countries within the EU, it is normally possible to comply with these restrictions by putting appropriate compliance measures in place, such as the use of Model Clauses or registration within the US Safe Harbor scheme.

In addition to data privacy regulations, there are many other legislative schemes that may prevent transfers of data. For example, there may be regulatory requirements to retain material information onshore and, in some jurisdictions, certain transfers of data – even to another entity within the same country – may qualify as a breach of the applicable banking secrecy or professional secrecy rules.

In this context, the technical means to transfer or store data is also an important aspect. In some cases, the use of encryption technology can legitimise a transfer that would otherwise be prohibited under banking

secrecy or professional secrecy rules. However, in other cases the use of encryption might be prohibited or restricted, e.g. requiring a specific licence and deposit of security encryption keys.

Regulations around energy supplies are also an important factor, especially considering the increased awareness of the need for sustainable energy sources. Some countries allow for tax or investment incentives where sustainable energy sources are used, while there may be taxes or other penalties or limits on the use of non-renewable energy sources.

Mitigating the risks

In addition to the examples set out above, there may be other legal and regulatory issues that need to be considered. An assessment of the specific legal and regulatory framework that applies and whether it presents any obstacles will always need to be done on a case-by-case basis, taking account of the specific needs and requirements, as well as the factual circumstances applicable in each individual case.

By *Emma Linnér*, Stockholm

Asia - Developments in the scheme for cross-border data transfers

Three major developments over the last couple of months have brought the aim of free sharing of personal information around Asia significantly closer to being achieved. They are particularly important for anyone considering or using binding corporate solutions in the EU.

Recent developments

In June 2013, Japan became the third country to apply to join the pan-Asian scheme, endorsed by the Asia Pacific Economic Cooperation ("**APEC**") forum. This follows Mexico and the United States, which were approved as participants in January 2013 and July 2012 respectively.

The APEC committee responsible for the cross-border data scheme (known as the Cross-Border Privacy Rules, or "**CBPR**", system) also recently met for the first time with representatives of data protection authorities from the European Union to discuss the development of a system to enable multi-national organisations to transfer personal data more easily between their affiliated companies in Asia and Europe. Currently, companies in Europe may freely transfer personal information to affiliated companies located in Europe and, with an approved binding group privacy policy, to affiliated companies outside of Europe. Until the introduction of the CBPR system, no similar regional scheme existed in Asia.

A crucial final step in the successful implementation of CBPRs was achieved at the end of June when the first independent examiner in CBPRs was approved. For the first time, CBPR applications can now be made, examined and approved.

What is the CBPR system?

APEC, a forum comprising 21 nations from the Asia-Pacific region that focuses on fostering economic prosperity and free trade in the region, developed a privacy framework that was approved by its member nations in November 2004. The privacy framework establishes a number of guiding principles that member nations may follow when implementing domestic laws for the protection of personal information.

The framework recognises that, given the differences in social, cultural, economic and legal backgrounds of APEC member nations, there must be flexibility in how each member nation implements the privacy framework. Accordingly, and in line with APEC's co-operative rather than directive nature, the privacy framework does not create binding obligations on member nations. APEC member nations represent a diverse collection of countries, including the United States, China, Russia, Indonesia and Australia. Some of these economies already have robust privacy laws in place, while others have no comprehensive laws dealing with privacy.

The CBPR system was developed under APEC's privacy framework and endorsed by APEC member nations in 2011. The CBPR system allows for organisations in participating APEC nations to seek to have their group

privacy policies and practices certified against the privacy standards set out in the CBPR system. If an organisation's privacy policies and practices are certified under the CBPR system, they will become binding on and enforceable against that organisation. In practice, this should mean that the organisation may then transfer personal data collected in its home jurisdiction to affiliated companies in other APEC countries without contravening the domestic laws of its home jurisdiction.

Responsibility for certification of an organisation's privacy policies rests with "Accountability Agents" approved for the jurisdiction in which the organisation is based. The Accountability Agent could be a public agency (e.g. the country's data protection authority) or a private entity. The CBPR scheme also envisages the appointment of "Privacy Enforcement Authorities" in participating nations. The role of these authorities would be to enforce the CBPR scheme and coordinate and share information with other authorities in the region on enforcement issues.

The CBPR system is in the early stages of development, with the United States and now Mexico being the pilot participants. It is envisaged that more APEC member nations will sign up to the system in the coming years.

How does this compare with the EU system?

Under EU law, personal data generally may not be transferred to a country outside of the EU unless there is an assurance of adequate protection in that country. One way to ensure adequate protection for transfers of data between members of the same corporate group is for that group to adopt Binding Corporate Rules ("**BCRs**"). These BCRs must impose privacy obligations that meet the standards set by EU law and must be formally approved by the data protection authorities in the EU nations in which the group operates. Once approved, an organisation in the group may transfer personal data to its affiliated companies outside of the EU on the basis of the group's BCRs. Although the BCR system has been approved at the EU level and adopted by almost all EU nations, some EU nations do not recognise the adequacy of BCRs for cross-border data transfers. At the moment, over 40 organisations have obtained approval for their BCRs, including Linklaters and, in the healthcare industry, Novartis, Sanofi, Novo Nordisk and, on 10 June this year, GSK.

BCR and CBPRs have a number of key similarities that should, in theory, make them inter-operable. Both solutions are based on groups of entities adopting – and making binding upon themselves – standards and policies for looking after personal information. Once an organisation has obtained approval of its group privacy policies, it may freely transfer personal data between its group members without fear of contravening the laws of its home jurisdiction.

There are, however, some differences between the two systems. In the EU, approval of an organisation's BCRs means that the organisation may transfer personal information collected in the EU to group members located outside the EU without contravening EU law. In contrast, the CBPR system is

intended to enable organisations to more easily transfer personal information to group members within the APEC region only. Certification of an organisation's privacy policy under the CBPR system will not of itself mean the organisation may freely transfer personal data to group members located outside of the APEC region (e.g. to European nations). In addition, the process for applications is different. In the BCR system, applications are made to a lead regulator in the EU who then examines the application and either co-ordinates the consideration of the application by other EU regulators or, more often, examines the application on behalf of multiple member states under the "mutual recognition procedure". In contrast, CBPR applications will be considered by independent, certified, accountability agents from the private sector. Crucially the first accountability agent capable of receiving, examining and approving CBPR applications was approved on June 25 this year.

Despite that progress, the CBPR system still requires the participation of a critical mass of APEC member nations which regulate personal data exports before it becomes a truly effective system. Currently, only the United States, Mexico and Japan are participants in the program, and of these only Mexico specifically regulates the export of personal data in a way that CBPRs solve. This means that a multi-national organisation headquartered in Mexico which has had its privacy policy certified under the CBPR system may transfer personal information collected in Mexico to another APEC member nation in compliance with Mexican law. However, an affiliate of that organisation located in another APEC member nation (e.g. Russia) will not be able to transfer personal information collected in that nation to the United States under the CBPR system until Russia signs up to the system. This is in contrast to the BCR scheme in Europe which has been adopted by all but two member nations of the EU. In our view, CBPRs need at least two other APEC member states which regulate personal data exports to join the CBPR scheme for it to reach critical mass.

Benefits and challenges of co-operation between the EU and APEC

There are clear benefits for cooperation and alignment of the BCR system in Europe and the CBPR system in Asia. As more and more organisations focus on business opportunities in the Asia-Pacific region, the free flow of personal information between affiliated companies in different countries will allow businesses greater room to grow without burdensome compliance obligations. Lower cost service-based nations, which sometimes do not have robust privacy laws, will also benefit if it becomes easier for multi-national companies to outsource personal data processing to their affiliates in these nations from higher cost jurisdictions (such as the United States and Australia).

A further benefit of co-operation between the EU and APEC lies in the ability of data protection authorities to share information with each other, helping to ensure a consistent approach to the enforcement of the various international schemes relating to cross-border data transfers.

A key challenge to the development of a clear EU-Asian system remains that APEC is a co-operative forum that develops non-binding policy guidelines and objectives. Unlike the EU, APEC is not a formal union of nations that can create mandatory legal obligations. Rather, APEC is comprised of a selection of nations with varying and disparate interests. There is no guarantee that all or even most APEC nations will participate in the CBPR system or any co-operative system between the EU and APEC, which may undermine the effectiveness of these systems.

Conclusion

The pan-Asian CBPR scheme remains in the early stages of development and it may be some time before it is fully implemented by APEC member nations. However, with the approval of Mexico as a participating economy, the application by Japan to join the scheme, the recent collaboration meeting between APEC and EU data protection authorities and the approval of the first accountability agent, there are signs that the scheme is gaining momentum.

More APEC economies are expected to sign up to the CBPR scheme soon and the APEC and EU data protection working groups have committed to meet again later this year to continue their discussions. Given that momentum, it would be sensible for anyone considering international data transfer issues – and the EU's binding corporate rules in particular – to factor in an Asian CBPR dimension to their programme.

By Richard Cumbley, London, and Adrian Fisher, Shanghai

Belgium – More details needed when responding to subject access requests

In February 2013, the Belgian Supreme Court gave one of its first decisions on the transparency obligations contained in the Belgian Privacy Act. It ruled that a data controller must provide an individualised answer when responding to a subject access request, specifying the exact processing it carries out in respect of the individual making the request. It cannot just rely on the general processing details in its publicly available notification made to the Belgian data protection authority. The Supreme Court also emphasised that failure to comply with these obligations is criminally sanctioned.

Transparency obligations

Article 10 of the Privacy Act gives data subjects the right to make a subject access request – i.e. obtain information regarding the processing of their personal data from any data controller. In particular, the data subject should be informed by the controller about the personal data regarding him/her being processed by the controller within 45 days of receipt of such request.

Article 17 of the Privacy Act provides that data controllers must also file a notification with the Belgian data protection authority prior to the start of any automated processing of personal data. This notification mentions, amongst other things, the categories of personal data being processed.

Failure to observe either of these provisions is sanctioned by a criminal fine of up to EUR 600,000.

Background

On 19 May 2003, Mr D. submitted a subject access request to the French-speaking Community of Belgium (the "**Community**"). The Community failed to reply to his letter, so on 13 August 2003 Mr D. launched summary proceedings in order to force the Community to respond to his request.

During court proceedings, the Community sent a copy of the notification filed with the Belgian data protection authority to Mr D's counsel. In first instance, the judge dismissed Mr D's claim and failed to rule on whether the Community had properly answered Mr D's access request. In appeal, the court recognised that the first judge had omitted to address Mr D's access request, but considered the provision of the notification constituted a sufficient answer to the subject access request.

Decision of the Belgian Supreme Court

In its decision of 14 February 2013, the Supreme Court overturned the Court of Appeal's decision.

The Supreme Court drew a functional distinction between the notification requirement, which allows an *ex ante* control by the data protection authority on the intended processing, and the access request requirement, which obliges the data controller to provide the data subject with an individualised answer containing the information he/she is entitled to receive under the

Privacy Act. The Supreme Court reiterated that failure to do so is sanctioned by criminal penalties.

Conclusion

The Supreme Court's analysis of the Privacy Act offers guidance on compliance with transparency requirements. The functional distinction between the notification in the public register and the answer to an access request may seem somewhat artificial. However, the information contained in the notification is generic and does not inform the data subject specifically about which personal data the controller is processing about him/her. The Supreme Court emphasises that the data subject must receive an individualised answer to his/her request with specific information regarding the personal data being processed about him/her.

It is also interesting to note that the Supreme Court stressed the criminal sanctions for failure to fulfil an access request, which may be read as a reminder that enforcement action could be taken against data controllers failing to comply with their transparency obligations.

By Guillaume Couneson and Ronan Tigner, Brussels

Belgium – Further proposals to implement the EU Data Retention Directive

A draft bill has been introduced into the Belgian Parliament to modify the Electronic Communications Act of 13 June 2005 (the "**ECA**") to ensure the full implementation of the Data Retention Directive 2006/24 (the "**Directive**").

Current implementation status

The Directive has already been partially implemented through amendments to the ECA. This enables a Royal Decree to be issued setting out when and under which conditions operators should retain traffic and identification data regarding end-users for law enforcement purposes. The ECA also explicitly provides that, for telephone services, the retention period to be set by the Royal Decree must not be shorter than 12 months or longer than 36 months (this exceeds the maximum retention period of 24 months allowed by the Directive).

However, no such Royal Decree has been issued, leaving operators uncertain as to their retention obligations.

Proposed legislation

If adopted, the draft bill would provide some clarity about the implementation of the Directive into Belgian law, as set out below.

Persons subject to data retention obligations – The data retention obligations would apply to providers of publicly available fixed and mobile telephony services (including teleconferencing, voicemail, call forwarding and SMS), internet access providers, e-mail providers and voice-over-IP providers, as well as to the providers of the underlying electronic communications networks (the "**Providers**"). This amendment would bring the list in the ECA in line with the Directive, which explicitly limits the retention obligations to these categories of providers.

Data to be retained – The Providers must retain the so-called "meta-data" about the communications, but not the actual content (unless otherwise provided by law). The following meta-data must be retained: (i) traffic data; (ii) location data; and (iii) information allowing the identification of the end-user, the electronic communication service and the probable type of equipment used. A Royal Decree is still needed to specify the exact data to be retained, but the scope of that decree is limited to specifying the data to be retained depending on the type of service.

Retention period – The bill distinguishes between different types of meta-data. Traffic and location data must be retained for 12 months as of the date of the communication. Other meta-data must be retained "for as long as an incoming/outgoing communication is possible using the subscribed services and for 12 months as of the last recorded communication". This retention period can be extended by Royal Decree for a limited period of time for reasons of public health, safety or defence. Should this period exceed 24 months, the Minister of Economy must notify the EU Commission and other

EU Member States. These changes will bring the ECA into line with the retention period limits imposed by the Directive.

Purposes – The meta-data must be retained for the following purposes: (i) the exercise by the public prosecutor, the investigating magistrate and the Belgian secret services of their investigatory powers relating to electronic communication services; (ii) the prosecution of malicious calls to emergency services; and (iii) the identification by the Telecom Ombudsman of persons misusing an e-communication service or network. Providers must ensure that the meta-data is accessible to the competent authorities from anywhere in Belgium and can be disclosed to them upon request.

Technical and organisational measures – The draft bill explicitly qualifies Providers as data controllers under the Belgian Data Protection Act. Providers will have to (i) guarantee the quality of the meta-data; (ii) implement technical and organisational measures to protect such data; (iii) limit access to the data to only the competent personnel of the operator; and (iv) ensure the data is destroyed at the end of the retention period. Providers will also need to take into account the other obligations imposed by the Belgian Data Protection Act, such as the obligation to inform the end-users whose data is being collected.

By Guillaume Couneson and Ronan Tigner, Brussels

Belgium – New protocol to ease (and complicate) the use of Model Clauses?

On 25 June 2013, the Ministry of Justice (the "**MoJ**") and the data protection regulator (the "**Privacy Commission**") concluded a protocol to streamline the approval of transfers of personal data outside of the EEA based on contractual clauses. The protocol addresses both the use of the standard contractual clauses and ad hoc contractual clauses to legitimate such transfers.

Contractual clauses as a data transfer solution

European data protection laws prohibit the transfer of personal data to countries outside of the EEA which do not provide an adequate level of personal data protection, subject to certain limited exceptions. One such exception is the use of appropriate contractual clauses by the data exporter to ensure adequate safeguards for that personal data.

Different types of contractual clauses can be relied on, including, among others:

> *Standard contractual clauses (SCC)*: These are template agreements pre-approved by the EU Commission for party-to-party transfers outside the EEA. Transfers based on these clauses are usually subject to limited formalities. For example, prior to the adoption of the above protocol in Belgium, it was sufficient to indicate the use of SCC in the mandatory notification to the Privacy Commission. The disadvantage of SCC is that they do not offer much flexibility (as their provisions cannot be changed) and they normally only allow for bilateral transfers.

> *Binding Corporate Rules (BCR):* These are a set of binding compliance measures adopted by a corporate group that allow transfers of personal data within the group, wherever the individual corporate entities are located. Both the BCR themselves and the transfers based on such BCR are subject to extensive approval requirements, although there are ongoing efforts by EU privacy regulators to simplify this process. The disadvantage of BCR is that they do not cover transfers of personal data outside a group of companies.

> *Ad hoc contractual clauses (AHCC):* These are tailor-made contractual clauses for the transfer of personal data between one or more entities located inside the EEA to one or more entities located outside of the EEA. These entities do not need to be part of the same group of companies. In many EU Member States, such ad hoc contractual clauses and the transfers based on such clauses are subject to specific formalities, e.g. notification/approval by a regulator or other public authority. Under the Privacy Act, transfers based on AHCC must be approved by a Royal Decree, i.e. an act signed by the King, after having obtained advice from the Privacy Commission. This is a time-consuming and complex exercise. To simplify this process, the Belgian Ministry of Justice ("**MoJ**") and the Privacy Commission concluded a

protocol on 25 June 2013, similar to the protocol already in place for BCR.

The new protocol

The protocol applies to both SCC and AHCC. The protocol requires SCC to be submitted to the Privacy Commission for approval to allow it to verify that the SCC conform to the template adopted by the EU Commission. Given the direct applicability of the EU Commission's decisions in Belgium, no Royal Decree is required. Instead, the Privacy Commission will confirm by letter that the submitted clauses are SCC and thus the international transfer is authorised. A copy of the letter will be sent to the MoJ.

AHCC still require the adoption of an individual Royal Decree, a template of which is attached to the protocol. However, these Royal Decrees do not require a prior review by the Belgian Council of State or full publication of the approved contract in the Official Journal. This greatly simplifies the adoption process.

In practice, the protocol requires that the AHCC are submitted to the Privacy Commission, which reviews their adequacy from a data protection perspective and prepares an opinion for the MoJ. If the Privacy Commission renders a positive opinion, it prepares an individual Royal Decree based on the template. The Privacy Commission then sends its opinion and the completed Royal Decree to the MoJ for signature by the King. The MoJ publishes an extract of the signed Royal Decree in the Belgian State Gazette, thereby allowing the transfer of personal data outside the EEA based on the approved AHCC.

Conclusion

No single compliance solution provides a silver bullet for international data transfers. Entities wishing to transfer personal data outside of the EEA must choose a solution based on the circumstances of each transfer.

The adoption of the new protocol between the Privacy Commission and the MoJ provides data exporters with a more streamlined approach to validate transfers on the basis of AHCC as an alternative to SCC or BCR. However, it also introduces a new obligation for data exporters who rely on SCC. These now require prior submission to the Privacy Commission for verification of their conformity to the templates of the European Commission, whereas it used to be sufficient to merely notify the Privacy Commission of an international transfer of personal data based on SCC.

By Tanguy Van Overstraeten, Guillaume Couneson and Ronan Tigner, Brussels

Luxembourg – Draft laws to encourage paperless offices

In February this year, the Luxembourg government proposed a new draft law n° 6543 on electronic archiving. It aims to provide clear guidelines on the creation and storage of electronic copies of paper originals, ensure high fidelity and durability of such copies and recognise their legal value. This should, in the long run, allow companies to rely on electronic copies and destroy many of their original paper documents.

Current rules on electronic copies of paper documents

Under current Luxembourg law, it is already possible to create electronic copies of original paper documents that have a legal value. In order to do so, the copies have to be created in accordance with a number of criteria laid out in a Grand-Ducal Decree dating back to 1986. This is intended to ensure that the copies accurately reflect the contents of the original and can be preserved over time. It is no surprise that such Decree mainly caters for microfilm archives and no longer reflects current state-of-the art in office technology.

In any event, even though a proper electronic copy is admissible in court, its use can be challenged. Where such a challenge is made, the holder of the document has the burden of proof to demonstrate that the copy is identical to the original. In the event of a challenge between a paper document and an electronic copy, the original paper document would prevail.

As a result, while many companies choose to digitise their documents for efficiency reasons, there are significant risks in also destroying the paper originals.

Proposed changes under the draft law

The draft law proposes a number of changes to improve on the existing system. First of all, the criteria for electronic archiving have been updated to match the current technical environment, whilst remaining neutral from a technology point of view.

Furthermore, the draft law allows for certification as "*Prestataire de services de dematerialisation et de conservation*" ("**PSDC**"), meaning a specialised service provider in digitising and archiving. In order to get the PSDC certification, service providers will have to demonstrate to the Luxembourg authorities that they have implemented technical and organisational standards that will ensure that copies are created and subsequently archived in accordance with the conservation criteria laid out by the draft law. Any entity can obtain PSDC certification, even for its own archiving needs. For example, a bank could obtain PSDC status and then benefit from the favourable regime for its own electronic archives, without having recourse to any external service provider.

It is furthermore possible for service providers to obtain an additional status as "*Professionnel du Secteur Financier*" ("**PSF**"), meaning that they will submit themselves to the Luxembourg financial sector rules and therefore be entitled to archive confidential documents, subject to Luxembourg banking secrecy.

While electronic copies that are created by an entity without PSDC status still enjoy the same legal value as under the current legislation, the advantage of the PSDC certification is that it will trigger a reversal in the burden of proof in the event that a copy is challenged in court. PSDC created copies will be presumed to be an accurate copy of the original (whether it still exists or not) and a party challenging its content will have the burden to prove that it does not accurately reflect the original.

This change of approach with electronic copies could finally encourage companies to trust in the use of electronic copies and destroy any remaining paper originals. However, it is important to note that that the draft law specifically excludes authentic acts (e.g. notarial deeds, enforceable court decisions, etc.) so originals of these documents should be preserved.

It also should be noted that any service provider with PSDC certification will be subject to Luxembourg professionals secrecy rules when acting for third parties, meaning that documents archived by a PSDC are protected by a regime similar to Luxembourg banking secrecy.

Challenges and outlook

While the draft law is still in its early stages and some questions on how it will work in practice remain unsolved, the Luxembourg government has stated that with the new draft law, it intends to grab a leading role in the electronic archiving sector within Europe and to attract businesses that seek to centralise their archiving needs in a single European country.

The ambition of the Luxembourg government is backed by the fact that in June 2012 the European Commission presented a draft proposal for a European Regulation in relation to the recognition of the probative value of electronic documents and the mutual recognition of such copies within the European Union (COM (2012) 238).

By Olivier Reisch, Luxembourg

UK – Update on 4G

Ofcom has completed its auction of the 800 MHz and 2.6 GHz spectrum bands and issued licences for 4G mobile broadband services earlier this year on 1 March. The licences were awarded to the four main mobile players, Vodafone, EE, O_2 and Three, together with a fifth operator, Niche Spectrum Ventures, which is a subsidiary of BT. This marked the end of a difficult auction process for Ofcom, who had to deal with a number of competing commercial, regulatory and policy considerations.

The auction involved the sale of 250 MHz of spectrum, which is equivalent to three-quarters of the spectrum previously available for mobile use. It could therefore shake up the playing field for mobile services quite significantly, as could Ofcom's more recent announcement that it will liberalise all existing 2G and 3G licences to allow the use of 4G. However, many 4G services have yet to launch and currently EE operates the only 4G network in the UK.

History of the auction

The UK has historically led the way in the telecommunications sector – privatisation of the sector was undertaken much earlier in the UK than other countries and the UK was a leading player in the launch of 2G and 3G services. However, until late last year, the UK did not have a 4G network and lagged behind many other jurisdictions, including Germany, the US, Australia, Sweden and Estonia.

So why the lag in respect of 4G? Much of the answer comes from the difficult commercial, regulatory and policy considerations Ofcom faced when attempting to arrange the 4G auction. For example:

> the 2.6 GHz band became available in 2005 and Ofcom was ready to auction it off in 2008. However, this decision was challenged by some of the mobile operators because of the uncertainties at the time in relation to the re-farming of the 900 MHz 2G spectrum and its potential effect on the value of the new spectrum to be made available. Ofcom withdrew the auction in light of the Digital Britain Report and instead decided to implement the report's recommendations to hold a combined auction of the 2.6 GHz and 800 MHz bands, the latter spectrum being made available as a result of the digital dividend freed up in the switch from analogue to digital TV;

> the merger between Orange and T-Mobile also caused delay due to the potential impact of the European Commission's review into the competition issues raised by the merger. These operators where eventually required to divest part of their spectrum holdings and this needed to be taken into account by Ofcom in structuring the auction; and

> Three were unhappy with the initial auction plans, claiming that, without any safeguards to protect it from the larger players, it would be forced out of the UK market.

Perhaps in an attempt to make up lost ground, Ofcom decided to 'liberalise' EE's 1800 MHz 3G licence in September 2012 to allow it to be used with 4G technology. However, this liberalisation almost had the effect of stalling the auction, as other mobile operators claimed that the decision by Ofcom offered a competitive advantage to EE.

The Government eventually felt it had to get involved and a deal was brokered between the operators whereby the auction was brought forward by a couple of months and the operators agreed not to pursue a formal challenge to Ofcom's auction process.

Auction safeguards

The auction presented Ofcom with a number of competing and arguably inconsistent objectives. On the one hand, the Government was keen to raise as much money as possible through the auction, and on the other, Ofcom needed to maintain a relatively level playing field in the mobile space and ensure the wide availability of 4G services to the UK population. To achieve these objectives, Ofcom's auction rules included a number of safeguards.

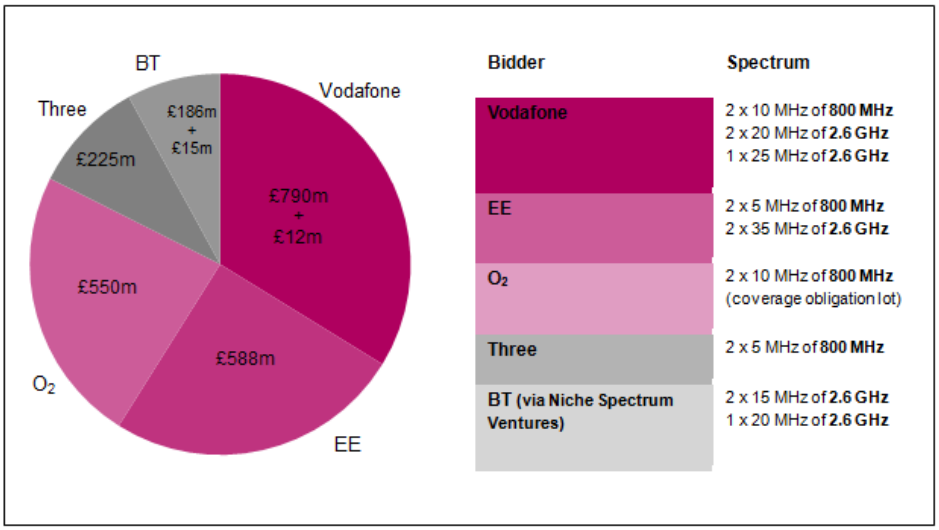
Firstly, Ofcom determined that, to preserve a competitive landscape, the market had to comprise at least four 'credible' national wholesalers. This meant that some spectrum was reserved for a fourth national wholesaler, which could be any operator *other than* Vodafone, EE or O_2. Three was not excluded from bidding for this reserved spectrum, which went a long way to allay its concerns that it would eventually be pushed out of the UK market if its spectrum holdings were not protected in some way.

Secondly, Ofcom placed caps on the amount of spectrum than an operator could be awarded. No one operator could hold more than 2 x 105 MHz of spectrum in aggregate nor more than 2 x 27.5 MHz in the bands below 1 GHz.

Finally, Ofcom imposed a minimum coverage obligation in one of the 800 MHz licences on offer to ensure that mobile broadband would be provided to a significant proportion of UK consumers. This obligation requires the licensee to achieve outdoor coverage to an area within which 99.5% of the UK population live and indoor reception to an area within which 98% of the UK population live. These coverage requirements are to be achieved by 17 December 2017.

The award

So who was awarded what in the auction? This is an overview of the licence fees paid and the spectrum awarded:



The five operators paid a total of £2.3 billion for the 250 MHz:

> Vodafone was awarded the largest slice of spectrum with a good range in each band, but it also paid the highest price. Vodafone acquired 2 x 10 MHz of the 800 MHz band and 2 x 20 MHz and an unpaired 25 MHz of the 2.6 GHz band for £790 million, representing more than one-third of the entire auction's proceeds. Vodafone also paid an additional £12 million for specific frequencies within the bands it bid for.

> EE paid the second highest price of £588 million for 2 x 5 MHz of the 800 MHz band and a very substantial section (2 x 35 MHz) of the 2.6 GHz band.

> O_2 was awarded 2 x 10 MHz in the 800 MHz band for £550 million. This spectrum lot was subject to the minimum coverage obligation.

> Three was awarded the spectrum reserved for the fourth national wholesaler, being 2 x 5 MHz of the 800 MHz band, for a modest £225 million. This was, in fact, the reserve price set by Ofcom prior to commencement of the auction.

> BT acquired 2 x 15 MHz and 20 MHz (unpaired) of the 2.6 GHz band for £186 million, paying an additional amount of £15 million for specific frequencies within the bands it bid for.

Ready to launch?

Following the auction, EE has the largest overall spectrum holding with 2 x 105 MHz of spectrum across the 800 MHz, 900 MHz, 1800 MHz, 2100 MHz and 2.6 GHz bands. This is equivalent to the overall cap imposed by Ofcom. In addition, it was able to launch its 4G services almost 10 months ago following the liberalisation of its 1800 MHz licence, whilst the other operators may not be ready to launch their 4G networks for another few months.

Vodafone is said to be ready to launch its services by the late summer. One of the reasons for this delay reportedly being because the current iPhone 5 is not compatible with a 4G network run on the 800 MHz band. O_2's 4G network is also expected to be launched this summer but no fixed date has yet been announced, presumably due to similar issues with the iPhone 5. Three has said that it is unlikely to launch its 4G service until the end of the year.

The operators also now have the option to use their existing spectrum holding for 4G following Ofcom's announcement on 9 July 2013 that it will liberalise all existing 2G and 3G licences to allow the use of 4G.

However, take-up of 4G services seems to be have been fairly cautious so far. That may be due to the price of 4G services, the absence of unlimited data offerings and the limited number of 4G compatible phones on the market. However, when the other operators launch their services that should inject some competition into the market, which may lead to a much more widespread take-up of 4G.

By *Melissa Fai* and *Gary Chu*, London

UK – Proposals to restrict IT suppliers withdrawing or altering supplies on customer insolvency

The Enterprise and Regulatory Reform Act 2013 (the "**Act**") gives the Government the power to introduce secondary legislation that voids terms in IT supply contracts that permit the IT supplier to terminate or alter their supply if their customer becomes insolvent. These powers seek to extend the protections given to insolvent companies under current insolvency law. The main aim of the reform is to support the rescue of viable insolvent businesses. The Government intends to issue a consultation on these powers in due course and bring them into force in April 2014. We consider the implications of the reform in practice.

The current framework

Currently, under section 233 of the Insolvency Act 1986, suppliers of "essential supplies" (gas, water, electricity and communications services) may seek a personal guarantee from an insolvency practitioner before continuing to supply an insolvent company, but may not demand payment of pre-insolvency debt as a condition of further supply.

Extending protection to the IT sector

The Government considers that IT supplies are now equally critical to the continuing operation of an ailing business as traditional utility supplies. It has therefore included section 92 in the Act to give it the power to extend the present list of essential supplies to include supplies "*for the purpose of enabling or facilitating anything to be done by electronic means*", i.e. IT supplies.

The Government will consult with interested parties in due course to determine exactly who will be caught by this extension. It specifically chose to use secondary legislation for this purpose and to give it the flexibility to update the scope of this legislation in light of changing market practices.

The Act also grants a power to extend the list of essential supplies to on-sellers of utilities and communications supplies. This reflects the way the utility and telecoms markets have evolved and been deregulated since current insolvency law was first enacted.

Further protections against termination of essential supplies

In addition, section 93 of the Act gives the Government the power to introduce secondary legislation to render void any contractual terms that allow providers of essential supplies to withdraw supply or alter terms of a supply contract (for example, by increasing charges) on account of certain insolvency circumstances.

This provision covers terms that allow a supplier to terminate the contract on account of a termination event that occurred before the insolvency, but which had not been exercised by the supplier by the time of the insolvency.

However, to ensure that the interests of suppliers are protected, a number of express safeguards must be included in any secondary legislation made under this power. The supplier must be given the right to:

> terminate the supply contract if the relevant insolvency practitioner or a court grants permission for such termination;

> terminate the supply contract if post-insolvency charges are not paid within 28 days of the date that they fall due; and

> request a personal guarantee for payment from the insolvency practitioner as a condition of continuing the supply (though there may be exceptions to this right).

Power is also given to include more safeguards as necessary.

Tricky questions for the IT sector

The intention is to support the rescue of insolvent companies by preventing providers of IT and utility supplies from withdrawing or altering the contractual terms of supply following an insolvency. If rescue is not possible, the reform should still deliver better outcomes for creditors as a whole in the insolvency. In particular, the changes protect against suppliers of essential supplies seeking 'ransom' payments (i.e. requiring fees up front or increasing fees) as a condition of continuing to supply in insolvency situations. The reform has been introduced following lobbying from The Association of Business Recovery Professionals.

The powers are expected to be brought into force by 6 April 2014. However, there are still a number of difficult questions to be answered.

For example, most "essential supplies", such as gas and water, are inevitably provided from within the UK. This is not the case with IT supplies, which are frequently provided by overseas suppliers under contracts that are subject to foreign laws and foreign jurisdiction. Moreover, with remotely provided services, such as cloud services, the supplier might not have any physical presence in the UK. Attempting to enforce these new provisions out of jurisdiction could be challenging.

Also, the powers only prevent the IT supplier from terminating or varying their contract. They do not appear to affect any non-alienation provisions in those contracts. IT suppliers will still presumably have a veto over any attempt to assign their contract to a third party, for example as part of pre-pack sale.

It will be interesting to see how the these issues are addressed once the consultation process begins. Further details about these changes are available here.

By Sanjana Sagoo, London

UK – Contractual duties of confidence are mainly … contractual

Confidentiality clauses are a staple ingredient of most commercial agreements. The Court of Appeal's decision in *Force One India v Aerolab* [2013] EWCA Civ 780 provides useful guidance on their interpretation, emphasising this is primarily a question of looking at the contract. The decision also considers damages for breach of confidence.

Aerodynamics testing and development

In April 2008 Aerolab entered into an exclusive contract to provide aerodynamic testing and development services to the Force One India Formula 1 team. The relationship between the parties broke down after Force One India failed to pay Aerolab for its work. Aerolab finally terminated the contract on 19 August 2009. However, before the contract with Force One India came to an end, Aerolab started to provide services to the competing Formula 1 team, Team Lotus.

Force One India alleged that Aerolab had entered into a concerted plan with Team Lotus to copy its aerodynamic system using confidential design files obtained by Aerolab whilst providing services to Force One India. It brought claims against Aerolab and Team Lotus for breach of confidence and copyright.

Force One India had little success at first instance. The claim against Team Lotus was dismissed. The claim against Aerolab was successful but the judge only found copyright infringement in relation to a small number of components and there was only limited misuse of Force One India's confidential information. In particular, he found that there was no attempt to replicate the overall aerodynamic system used in the Force One India car and Aerolab had instead just used the confidential design files to "short cut" the process of creating new aerodynamic components for the Team Lotus car.

Permission to appeal was given only in relation to claims for breach of confidence.

Interpreting express duties of confidence

The contractual confidentiality duties of Aerolab were set out in some detail in their agreement with Force One India. Amongst other things, Aerolab agreed not to disclose or use any "Information"; this term was defined widely to extend beyond trade secrets and even include information in the public domain. However, Aerolab benefited from a number of standard carve outs. For example, the duty did not apply to information in the public domain.

The key question for the Court of Appeal was the scope of Aerolab's confidentiality duty. It stated that this was primarily a matter of looking at the contract. In this particular case "*the parties have carefully balanced their respective rights and obligations [and] the court should be very slow to substitute its own perception of what is reasonable*".

In particular, the Court of Appeal was critical of the lengthy analysis of various authorities in the first instance judgment noting the analysis "*hardly refers to the wording of the contract at all*" and "*has little to do with answering the question: what does the express term mean*". In particular, there was little value reviewing implied duties of confidentially as there is nothing to prevent an express confidentiality term providing greater protection than that available under implied duty.

The use of general skill, knowledge and experience

It was equally unnecessary to review the law on implied duties of confidentiality to determine if Aerolab and its employees were entitled to rely on any general skill, knowledge or experience developed under that contract.

This is because the contract restricted the use or disclosure of "Information" so was clearly not relevant to the use of acquired "skill" or "experience". The position on "knowledge" is more difficult. However, the Court of Appeal advocated the approach taken by Roxburgh J in *Terrapin v Builders' Supply Company* [1967] RPC 375, who stated "information" needed to be traced back to a particular source and would not include something that had become so merged in the mind of the person informed that it was impossible to say from what quarter it was derived. However, the Court of Appeal was careful to also point out that "information" would not cease to be confidential just because it was memorable.

Public information

A subsidiary question was whether a claim for breach of confidence could subsist where the relevant information was in the public domain.

This was an issue as Force One India's car was on public display during the Formula 1 races. It was therefore possible, and in fact common practice, for teams to photograph each others' cars to study their design. This would have enabled Aerolab to get a great deal of information about the overall shape and configuration of the Force One India car even if it would not provide the exact dimensions.

However, the Court of Appeal confirmed it is no defence that a person in breach of confidence could have obtained the information elsewhere if they did not do so. That person should go to the public source and get the information or, at the very least not be in a better position than if they had gone to the public source. Moreover, as with all the other carve outs from the duty of confidence, the burden was on Aerolab to establish the exception applied and it had not, and could not do so.

Assessment of damages

With these factors in mind, the Court of Appeal concluded that Aerolab had breached its duty of confidence to Force One India, but felt bound by the first instance judge's findings on the facts that this did not involve copying of the whole aerodynamic system. Instead, with some minor exceptions, Aerolab had simply reused some of the information as a "short cut" to help create new designs for its work with Team Lotus.

This, in turn, influenced the damages due for that breach. Force One India had not suffered any loss as a result of the breach so damages were instead assessed on a *Wrotham Park* basis. In making its assessment, the Court of Appeal considered that:

> the information in question was not very special. For example, it did not include reuse of the aerodynamic system. Therefore, the appropriate measure of damages was the alternative means of obtaining that information from another source;

> there was no evidence that Aerolab intended to systematically re-use the whole library of components and therefore the damages were restricted to the information actually misused (if it had been shown that Aerolab was treating the whole library of components as its own, damages may have been greater: "*if A wrongfully retains B's dictionary, it does not matter that he only looked up a few definitions*" per Lewison LJ); and

> damages were therefore based on the time it would have taken for a third party consultant to replicate the misused information. On the basis of the evidence available, this was assessed to be Euro 25,000. To the extent the Enforcement Directive applies to a breach of confidence (a matter Lewison LJ was "sceptical" about) it was an "effective, proportionate and dissuasive" remedy, not least because it equates to almost all of the profit Aerolab made on its contract with Team Lotus.

The decision in *Force One India v Aerolab* [2013] EWCA Civ 780 is available here

By Ian Karet and Peter Church, London

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 2013

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