Linklaters

September 2011

Technology Media and Telecommunications.

Data Protection

Should you care what the Article 29 Working Party says?

> *"soft law - rules of conduct which, in principle, have no legally binding force but which nevertheless may have practical effects"*[1]

The Article 29 Working Party performs an important function helping with the development and interpretation of European data protection law. Its main output is soft law opinions which are not legally binding. This article considers the extent to which these opinions have hard law effects either through adoption by the courts and national regulators or by other means. It also considers the future of the Working Party and whether people ought to start listening to the Working Party more carefully.

Article 29

The Working Party was, unsurprisingly, established under Article 29 of the Data Protection Directive. It is an independent advisory body composed of representatives from the European Commission, the European Data Protection Supervisor and each national regulatory body. The Working Party elects a chairman, currently Jacob Kohnstamm (who is also the chairman of the Dutch Data Protection Authority).

The Working Party has around five full meetings a year and carries out a range of tasks allocated to it under the Data Protection Directive. While its main output is opinions, working documents and recommendations on the interpretation and implementation of the Directive (referred to generically as "opinions" in this article), it also has a number of other functions. This includes advising the European Commission on the adequacy of data protection legislation in third countries as part of the recognition process and preparing an annual report on the status of European data protection. It also conducts investigations into particular issues, such as its investigation last year into the activities of search engines.

[1] Francis Snyder, "The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques" (1993) MLR 19, 32

Soft or hard law

The Working Party's most important function is issuing opinions. This is the primary means by which it exercises its influence. It has issued 187 opinions to date covering a wide range of subjects, including the meaning of consent, the data protection implications of smart meters and the protection of children's personal data. These opinions emerge as "soft law". They are persuasive but not binding on the European Commission, national regulators, European or national courts.

To what extent do these opinions have hard law effects? The answer is mixed. These opinions are only rarely referred to by the European Court of Justice. The only decision which refers extensively to the opinions of the Working Party is *Promusicae v Telefónica de España SAU* (Case C-275/06), the question in that case being whether IP addresses are personal data. However, this may in part reflect the limited number of decisions by the Court of Justice on data protection matters.

The picture is less clear at a national level, though it appears to be broadly similar. The English courts will treat the Working Party's opinions as persuasive but also only rarely refer in practice. One notable recent exception is *British Telecommunications, R v Business, Innovation and Skills* [2011] EWHC 1021, again on the question of whether IP addresses are personal data. Similarly, the Working Party's opinions are not binding on the Spanish courts and are not generally referred to in practice.

Unsurprisingly, the Working Party has a much greater influence on national data protection regulators. While there is generally no legal obligation on regulators to adopt the positions of the Working Party, most regulators' guidance and other working practices do so in practice. Some examples of this are set out below.

Binding corporate rules

The development of binding corporate rules (Working Papers 74 & others) a means to justify transborder dataflows is one of the Working Party's more impressive accomplishments. There is no statutory basis for binding corporate rules in the Data Protection Directive but the Working Party has, through a range of soft law opinions, produced a detailed framework including criteria for determining a lead regulator, standard application forms and a summary of national filing requirements for binding corporate rules.

These changes have also had a real practical effect. For example, the majority of the national regulators are now part of a mutual recognition club under which an approval by a lead regulator and two co-lead regulators will automatically lead to approval by the other members of the mutual recognition club. This work by the Working Party has greatly increased the attractiveness of binding corporate rules.

The upcoming amendments to the Directive are likely to put binding corporate rules on a statutory footing. This shows the benefit of using flexible soft law

instruments such as this to test a new concept. If the concept is successful, it can then be morphed into hard law.

Whistle-blowing

Another notable success is the Working Party's opinion on whistle-blowing hotlines (Working Paper 117). The US Sarbanes-Oxley Act of 2002 introduced an obligation on US listed companies to implement whistle-blowing or ethical hotlines for employees to report accounting irregularities. The use of these hotlines is controversial in many European jurisdictions, partly because of their historical connotations, and there were a number of challenges to their use, such as the CNIL's action against McDonalds in France. Other national data protection authorities also raised objections though not necessarily on the same grounds.

This caused significant concern to many US companies who felt trapped between US securities law and the many different data protection laws of the European Member States. However, the Working Party's opinion on whistle-blowing hotlines was hugely helpful in resolving this issue.

This opinion provided a detailed analysis of the data protection issues together with a pragmatic and achievable compliance solution. It resulted in many national data protection authorities taking a harmonised approach to this issue whilst, because it is a soft law instrument, allowing some to take a slightly different approach reflecting their own cultural and legal requirements. For example, the Spanish and Belgian regulators restricting the use of anonymous whistleblowing hotlines.

Limits on soft law

There are, however, limits on the power of the Working Party and not all of its opinions have had the same impact.

One example is the opinion on the concept of personal data (Working Paper 136) which concluded that almost any information had the potential to be personal data. While this position has been adopted in many Member States, it has had limited effect in others. For example, the UK Information Commissioner produced guidance that broadly followed the Working Party's opinion but both that guidance and the opinion have been generally disregarded as they conflict with the decision of the Court of Appeal in *Durant v Financial Services Authority* [2003] EWCA Civ 1746. The hard law of that court takes precedence over the soft law opinion. Any change to this position would either require a binding decision by a higher court or a change in the law, which is entirely possible given the European Commission's continuing scrutiny of UK data protection laws.

Similarly, some opinions do not seem to have much effect on national regulators' working practices. For example, the Working Party considers that placing a cookie on a user's computer constitutes a "use of equipment" (Working Paper 56) which could result in an undertaking outside the European Union becoming subject to European data protection laws. This is a long held position, first adopted in 2002, but there is limited evidence of regulators

actually taking enforcement action on this basis, for example by asserting jurisdiction over a US company solely because of its use of cookies in Europe.

The future of the Working Party

The Working Party's opinions are, therefore, a classic example of soft law instruments. Like most such instruments, they provide a number of benefits. The most obvious is flexibility, which allows experimentation and adjustment and permits national variations which might otherwise lead Member States to block the use of hard law instruments. Equally, there are disadvantages in the use of such opinions such as the Working Party's lack of democratic mandate, the risk of scope creep and the lack of clarity in some of their opinions (though equally the use of examples and other explanations makes some opinions clearer than legislation).

These are issues that are likely to come under increased scrutiny given the impending amendments to the Data Protection Directive. The European Commission is proposing to strengthen the Working Party's role to ensure a more uniform approach to data protection legislation at a national level. Any such move should also address some of the problems set out above, for example improving the accountability of the Working Party by making it more transparent or including representatives from industry and consumer interest groups more closely in its workings and its decision making processes. There has been industry involvement in some of its opinions, such as the search engine opinion (Working Paper 148) where Google and Yahoo! were consulted, but this is the exception and not the rule and any involvement is limited.

Until any such revisions to the Directive are made, the Working Party's role is persuasive but limited. Its opinions do require consideration but will rarely require urgent action or a complete review of current compliance procedures.

By Peter Church, London

EU - Three hurdles to Europe-wide cookie compliance

Linklaters LLP has partnered with Magus (www.magus.co.uk) to offer an integrated technical and legal cookie review service. This article sets out some of the challenges raised by a Europe-wide legal review and the compliance solutions that might be adopted.

European states were supposed to introduce new cookie rules by 25 May 2011 and yet, months after this implementation date, the law is still in a state of confusion. There are three major problems:

> not all Member States have actually implemented the new cookie laws;

> of those that have implemented these laws, few have provided meaningful guidance on what they mean in practice; and

> fewer still have provided any guidance about how these laws will be enforced and whether any grace period will apply.

As a result, a pan-European cookie compliance programme is more a matter of risk assessment than legal analysis, requiring a trade off between regulatory risk, website usability and business impact.

A quick recap

Cookies are small text files stored on your computer. They are sent by a website to your computer the first time you visit that website and allow the website to recognise your computer on subsequent visits. While there are a number of legitimate uses for cookies, there is also a concern they can be used in a way that infringes users' privacy.

Accordingly, the ePrivacy Directive was amended in November 2009 to require consent from users for the use of cookies unless the cookie is strictly necessary for the provision of services to the user. However, this obligation needs to be read in light of the recitals to the amending Directive, which states that consent can be obtained from web browser settings.

These provisions have caused considerable confusion, with a number of conflicting views on how they should be interpreted in practice. This causes particular difficulties when trying to implement a pan-European compliance programme as there is potential for different approaches in different Member **States. Three major problems arise.**

1 - Failure to implement national laws

The first issue is Member States' failure to implement the new law. Whilst accurate information about the implementation status of this Directive is hard to come by, it appears that only Estonia, Finland, France, Ireland, Latvia, Malta, Sweden and the UK have introduced these new cookie laws.

The remaining Member States, including major jurisdictions such as Germany and Spain, are still considering this new law, though most have draft legislation under discussion. This has led to enforcement action by the European Commission, which has started legal action against these states.

2 - Lack of guidance

Even where the laws have been implemented, there is still likely to be significant uncertainty about the meaning of those laws and the critical question of what constitutes "consent". Does it have to be "prior" consent? Is it possible to rely on browser settings?

For example, Sweden, like many other Member States, has ducked the issue and simply copied out the wording of the Directive. It has a series of Questions & Answers on the new law but this contains little help in determining what consent means or how to obtain it in practice, though the IAB in Sweden is working on industry guidelines that may help to clarify things.

Even where Member States do more than just copy out the wording of the Directive, those additional provisions may be of limited use. Many commentators have focused on whether national legislation includes an express reference to browser settings but the significance of its inclusion is questionable as:

> just because browser settings are *capable* of demonstrating consent does not mean that current browsers are actually sufficient for this purpose. This is the case in the UK, where the Information Commissioner has expressly stated that current browser settings are not sufficient to provide consent despite an express reference in UK legislation; and

> similarly, just because browser settings are not referred to in national legislation does not mean they cannot provide consent.

A more relevant issue is whether national legislation contains an express requirement for "prior" consent. The Article 29 Working Party considers this is already implicit in the amendments to the ePrivacy Directive (see Working Paper 187) but there is no reference to "prior" consent in the Directive and the UK, at least, has clearly indicated this is not necessary.

What is really needed is clear guidance. That issued by the UK and Irish data protection regulators goes some way toward this goal, though still leaves a number of unanswered questions such as the extent to which consent can be implied through suitable website notices.

3 - Clarity over enforcement

Finally, how will these new laws be enforced, when will they be enforced and will they be enforced?

The first question is largely answered by the implementing law, which should determine the sanctions available for breach of that law. For example, in the UK these provisions have been implemented through amendments to the Privacy and Electronic Communication Regulations 2003, which can be enforced in a range of ways, including the issue of a cease and desist order (Enforcement Notice). It is also theoretically possible that a fine of up to £500,000 (Monetary Penalty Notice) could be issued, though in practice it is very unlikely that the threshold criteria for a fine would ever be met.

The next question is whether the law will be enforced immediately or whether there will be a grace period. Again, the UK has provided clarity on this issue and stated that there will be no enforcement action for 12 months so that organisations can put compliance measures in place and/or take a risk based approach to compliance based on the steps taken by their peer group.

Finally, will these laws be enforced in any meaningful way? Some regulators are likely to see this as a priority, such as the German data protection authorities who have been historically opposed to the use of some cookies, such as Google Analytics cookies. However, for other regulators, it is unlikely this will be a priority with some privately indicating that they do not believe these laws address any real privacy concerns.

A risk based compliance strategy

This lack of clarity means that any European-wide compliance programme will be driven more by the trade off between regulatory risk and other factors such as the ease of implementation, the effect on website usability and any reduction in the value of the website. This is best illustrated by considering some of the more obvious compliance options.

Option	Regulatory Compliance	Impact on Usability	Business Impact	Comments
Remove all non-essential cookies	Very High	Variable	High	It may be possible to remove all cookies from a website other than those strictly necessary for the provision of services to the user. However, this might require significant redesign work and reduce its value (e.g. if the owner is no longer able to get accurate information on website usage and visitor habits).
Pop Up Windows	High	High	High/ Medium	A pop up window is presented to the user. Non-essential cookies are only used if the user clicks "Accept". This is an intrusive and annoying option (not least because those refusing cookies will get the pop-up again and again). Many users may also decide not to accept cookies (see below). Partial acceptance of cookies may make tracking information meaningless.
Banner Tick Box	High	Medium	High/ Medium	A banner is placed at the top of the page allowing users to click to accept cookies. This is the option selected by the UK Information Commissioner. In practice, very few people click to accept cookies (see statistics here). Partial acceptance of cookies may make tracking information meaningless.
Acceptance of T&C's	Medium	Medium	Low	Users give consent to cookies when they accept the terms of use of a website. This only works if users are expressly required to agree to those terms of use in order to use the website.
Website Notes	Low	Low	Low	A prominent notice is provided indicating that cookies are used, linking to details of each cookie. This is the option taken by the UK Department of Culture, Media and Sport who are responsible for implementing the new cookies laws in the UK.

Selecting an option from that list will require consideration and assessment of a range of factors including:

> which jurisdictions' laws are you subject to? This is not a straightforward issue. The jurisdictional reach of these laws is unclear but may include the jurisdictions in which you operate or direct your activities. How clear are the requirements in those jurisdictions (or key jurisdictions) and how will they be enforced?

> how long and how much would it cost to amend your website? For example, can you carry out this work now? If you adopt a low level of compliance, how quickly could you adopt a more compliant solution if the risk of enforcement increases?

> how long will it be before consent can be provided through privacy-enhanced settings on browsers, for example by forcing users to make a decision on the use of cookies rather than allowing them by default? Is it worth waiting for these new browsers to be released (or waiting for IPv6)? If you do wait, how do you deal with legacy browsers such as IE6?

> how intrusive are cookies in practice? The more intrusive, the greater the need to show consent and the higher the risk of enforcement action.

> how important are cookies to your website? What would the impact be if you were unable to place non-essential cookies on your users' browsers?

> what steps have your peers and other organisations taken to comply with the new rules (including the steps taken by regulators and other government bodies)?

Depending on the option selected, you may also need to keep a watching brief and be prepared to move to a more compliant solution if the risk of enforcement increases.

By Marly Didizian and Peter Church, London

Belgium - Criminal proceedings for Street View Wi-Fi data capture

The fall-out from the collection of Wi-Fi data by Google's Street View cars continues. The latest update is the Belgian Federal Public Prosecutor's action against Google, discussed below.

Street View

Google's well-known Street View service offers panoramic street-level views of the streets in over 30 countries. The service originally raised privacy concerns in several jurisdictions, now largely resolved by number of privacy guarantees given by Google, such as the blurring of the faces of people captured on Street View. In light of these guarantees, Google was allowed to proceed with the development of this product in Belgium.

Following an enquiry from the German data protection authority for Hamburg, it emerged, however, that the Google Street View cars were also recording data from Wi-Fi networks. On 17 May 2010, Google admitted this had taken place and later confirmed that the data collected might contain personal data, such as email addresses and passwords. Google has always claimed that the data collection was unintentional.

Data protection authorities throughout the EU reacted to this, finding that Google's action infringed the privacy of data subjects. In a number of cases they imposed fines or ordered Google to delete the collected data.

Enforcement in Belgium

The Belgian Privacy Commission does not have the power to impose fines on data controllers for a breach of the Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data (the "**Privacy Law**"). However, it may report criminal offences to the Public Prosecutor.

The Privacy Law indeed can result in criminal sanctions for breach of most provisions. Penalties range from EUR 550 to EUR 550,000 and include, in specific cases, imprisonment of up to two years. The publication of the judgment may also be ordered, together with other measures such as confiscation of the media on which data is stored, an order to erase the data and/or a prohibition on using the personal data for up to two years.

When details of the Wi-Fi data capture emerged last year, the Privacy Commission asked the Belgian Federal Public Prosecutor's office ("*parquet fédéral*" / "*federaal parket*") to investigate Google's actions.

Action by Federal Prosecutor

On 18 August 2011, the Federal Prosecutor's office announced it had offered Google a deal. Google can pay EUR 150,000, in return for which the Federal Prosecutor will drop the charges against it - i.e. charges for what the Federal Prosecutor considered to be criminal offences committed by Google under the Privacy Law.

If Google does not take the deal, the Federal Prosecutor could decide to bring the case before the criminal courts. Google spokesman Anthony House told Bloomberg: "*(w)e have received an offer of extra-judicial settlement from the Belgian federal prosecutor and we have to study it carefully*". Google will have to choose between the proposed settlement and the risk of facing a full-fledged criminal prosecution on grounds of a breach of the Privacy Law.

By Guillaume Couneson, Brussels

Belgium - Privacy Commission's consultation suggests practical solutions to employee monitoring

Employee monitoring raises difficult legal issues in Belgium, as it does in many other jurisdictions. Following numerous enquires from employers, employees, trade unions and law practitioners on the topic of employee monitoring, the Privacy Commission decided to re-examine the issue.

On 13 July 2011, it issued a comprehensive set of documents including an explanatory text, an extensive legal report and a number of recommendations and practical guidelines.

Legal Framework

The Privacy Commission's review starts with a summary of the current legal framework applicable to employers when monitoring employees. This legal framework is very complex, as it consists of provisions from no less than seven different legal texts from different fields of law, which have to be combined and applied jointly.

However, the Privacy Commission's review has been underlined by a determination to provide practical solutions, as illustrated by its statements is that it "*is opposed … to an interpretation of the ensemble of applicable rules which would result in making [monitoring] by the employer impossible/illegitimate*".

Main Findings

The Privacy Commission's findings provide useful guidance. Compared to the rather uncompromising opinions issued by the Privacy Commission in the past, it is now suggesting a number of solutions, and demonstrating a more flexible approach. In doing so it is seeking to balance the legitimate interest of the employer to organise and monitor the activities of its employees, on the one hand, and the privacy-related interests of those employees, on the other.

The main conclusion of the Privacy Commission is that a distinction should be made by employers between the use of email for private purposes and its use for professional purposes. It suggests employers should:

> clarify in their policies that their professional email system can only be used for professional purposes; and

> allow employees to access their private email accounts at work for private correspondence.

If the employer's email system has been reserved for professional purposes in this way, the Privacy Commission considers the employer can access the email account and the content of the messages to ensure the continuity of service and the proper functioning of the company.

Another interesting conclusion is that the Privacy Commission strongly opposes reliance upon consent in an employment context as it considers it very unlikely such consent could be freely given. This is in line with the Article 29 Working Party's recent opinion on the definition of consent. This position contrasts with the consent-based solutions currently relied upon by many employers.

The Privacy Commission considers that the employer should be able to rely on other legal grounds in place of consent, such as the necessity of the processing for the performance of a contract, in this case, the employment contract. It is, however, still important for the employer to properly inform its employees of any monitoring.

Recommendations

The Privacy Commission also recommends that companies start by implementing rules and procedures to avoid the need for accessing the personal data of employees in the first place. This includes the separation of public and private email accounts (see above), but also the use of preventive software such as email and web filters rather than more invasive '*a posteriori*' controls.

In addition, the Privacy Commission makes other recommendations, aimed at employers who are not capable of excluding, or are not willing to exclude, mixed use (private and professional use) of their email system.

These documents are subject to a public consultation which is open until 30 November 2011. On 16 December, the Privacy Commission will present the first results and a preliminary draft opinion for a final recommendation during a conference on this topic.

By Bastiaan Bruyndonckx and Guillaume Couneson, Brussels

France – An update on the CNIL and data protection enforcement

The last months have seen a number of changes to the data protection landscape in France. This includes new enforcement activity and changes to the governance and powers of the French Data Protection Authority (the "**CNIL**"). This article provides a short refresher on these changes.

CNIL's new enforcement strategy

As part of its investigation programme for 2011, the CNIL indicated that it will greatly increase the number of audits it conducts.

This includes working much more closely with the General Directorate for Competition Policy, Consumer Affairs and Fraud Control (*Direction générale de la concurrence, de la consommation et de la répression des fraudes*). The two agencies signed a cooperation agreement on 6 January 2011 under which the DGCCRF will inform the CNIL of any personal data related offence it becomes aware of. This should significantly increase the CNIL's reach.

The CNIL annual audit program, adopted in March 2011, also reveals its strategy for the coming year. Its investigations have already trebled from 2005 and 2010 (100 inspections were held in 2005, whereas 300 in 2010), and its goal is to conduct even more audits, with 400 audits planned in 2011. In the medium term, the CNIL would like to increase this further to 800 audits per year. The audit program highlights five priority areas:

> *International Data Transfers* - The CNIL plans to investigate companies located in France as well as those located abroad receiving data about French nationals. It intends, amongst other things, to audit U.S. firms operating under the Safe Harbor programme.

> *Health Data* - The CNIL will continue to audit this sector with a particular focus on firms who store and process health data as well as firms who conduct medical research. This will include insurance companies, data hosts and health care service professionals.

> *Video Surveillance* - France adopted a National Security Act on 14 March 2011 (*La Loi d'orientation et de programmation pour la performance de la sécurité intérieure*) which regulates public authorities' video surveillance powers with respect to both public and private areas. This law gives the CNIL authority to inspect CCTV devices. The CNIL plans to perform 150 such inspections.

> *Private Detectives and Collection Agencies* - The CNIL consider there is a need to look more closely at this sector, in which breaches to data protection seem to happen frequently.

> *Marketing* - The CNIL intends to review this expanding area of business. Its review should encompass devices used to measure viewership (advertisement devices, direct marketing by electronic means) and behavioural analysis (social networks, websites, etc.).

Practical examples of enforcement

In July 2011, the CNIL indicated that it imposed a €50,000 fine to a company which denied individuals their right to object to the collection of personal data. The company had been collecting personal data on individuals who wanted to benefit from their gift certificates but had not notified the individuals of their right to object to the collection of such data. This violation of data laws allowed the company to compile a significant prospect database. The identity of the company has not been published.

In March 2011, the CNIL was the first data protection authority to formally sanction Google for the collection of Wi-Fi data by its Google Street View cars. The CNIL held a series of on-site audits to verify whether Google's practice was in compliance with the French Data Protection Act. This revealed Google had collected Wi-Fi data without the knowledge of the data subjects and recorded important information such as IDs, email exchanges, passwords, etc. As a result and after an attempt to cooperate with Google, the CNIL fined Google €100,000. The CNIL stated that Google: "*didn't give us all the information we asked for … and were not always very transparent*".

Amendments to the CNIL's powers and governance

The CNIL investigatory powers have recently been modified by the Law no. 2011-334 of 29 March 2011 (*Loi relative au Défenseurs des droits*) amending the French Data Protection Act. There are four key points arising from these amendments.

Firstly, amendments to the French Data Protection Act have been made to comply with the basic right to privacy and the right to a fair trial as laid out in Articles 6 and 8 of the European Convention on Human Rights (see *TMT News: France - Enforcement authorities must be mindful of human rights*). For instance, the proprietor of the companies' premises has a right to object to an audit by the CNIL and, where such an objection is made, the CNIL must obtain prior authorisation of a judge to the audit. The amendments now require the CNIL to clearly inform the proprietor of his right to object prior to conducting the audit. However, the CNIL may nevertheless conduct an inspection without giving the proprietor the right to object in cases where the emergency, the gravity of the facts at issue or the risk of destruction or dissimulation of documents justify the authorisation of the judge.

Secondly, the new provisions also prevent members of the CNIL with powers to impose sanctions from holding any prosecuting or investigative powers (i.e. to separate its role as a tribunal from its investigative role). Therefore, the composition of the Restricted Committee (*Formation Restreinte*), which is in charge of sanctions, will be modified so that the President and Vice-Presidents of the CNIL are no longer allowed to sit on such Committee.

Thirdly, the Restricted Committee is now authorised to publish the sanctions it imposes and may request their publication in newspapers and the like at cost of the infringing data controller.

Finally, under the new rules, the CNIL's President will be barred from any professional activity or holding any elected national office from 1st September 2012. This rule intends to guarantee the independence of the CNIL, as it has the status of an Independent Administrative Authority (*Autorité Administrative Indépendante*). The current President is a Senator, so he indicated that he will resign at the end of September 2011.

By Sylvie Rousseau, Pierre-Olivier Ally and Flore Colnet, Paris

India – Welcome clarification on sensitive personal data rules

India recently issued data security rules which caused confusion and some concern for those outsourcing services to India, particularly the suggestion that they require companies outside of India to obtain consent from individuals for such processing. The Indian Government has now issued a clarification which largely allays these fears, though a number of questions still remain.

Sensitive personal data rules

The Indian Government issued the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**Sensitive Personal Data Rules**") in April 2011. Rather ironically, they were intended to clarify the obligations on body corporates under the Information Technology Act, 2000 (see *TMT News: India - New data security laws and rules for sensitive personal information*).

However, there was significant ambiguity over the interpretation of the Sensitive Personal Data Rules, particularly their effect on companies outsourcing to India. As a result, NASSCOM, the association which represents the Indian information technology and business process outsourcing industry, raised a number of concerns to the Ministry of Information Technology.

Accordingly, on 24 August 2011, the Ministry issued a press release ("**Press Note**") in an attempt to clarify some of the provisions of the Sensitive Personal Data Rules.

Jurisdiction limited to India

Significantly, the Ministry has clarified that the Sensitive Personal Data Rules apply only to body corporates or persons located within India. This should help to address the concerns raised by the information technology and outsourcing industry in India, including that the Sensitive Personal Data Rules impose a higher burden on entities located outside India beyond what their local laws require of them.

The Press Note also confirms that the Sensitive Personal Data Rules only apply to "sensitive personal data or information" as the term is defined in those Rules.

Consent requirements have limited effect on Indian outsourcing

The other key clarification relates to Rules 5 and 6 of the Sensitive Personal Data Rules which set out the restrictions on a body corporate when collecting and disclosing sensitive personal data or information. This includes the requirement to obtain the consent of the "provider of information".

The Press Note clarifies that the term "provider of information", as used in the Sensitive Personal Data Rules, means individuals - i.e. natural persons who provide the information to the body corporate. It further clarifies that

> the data collection and consent requirements do not apply to Indian outsourced service providers receiving sensitive personal data under a contract with any legal entity (other than a provider of information)

located within or outside India. The Press Note also implies that this is the position regardless of whether the outsourced service provider receives sensitive personal data directly from the provider of information or via the legal entity with which it has a contract. This means that non-Indian companies outsourcing to India should not have to worry about the Sensitive Personal Data Rules. They are not subject to these rules (see comments above on jurisdiction) and neither should their service provider; and

> body corporates in India that obtain information from direct contact with individuals when providing services under a direct contract with such individuals are subject to the data collection and consent rules regardless of whether the individual is located inside or outside India.

Finally, the Press Note clarifies that "consent" includes consent given by any mode of electronic communication.

Other issues

The clarifications in the Press Note appear to resolve the immediate concerns of the information technology and business process outsourcing industry in India. However, the Ministry of Information Technology has not used this opportunity to clarify other general issues that persist under the Sensitive Personal Data Rules. Some examples are set out below.

Onward transfers

Rule 7 specifies that a body corporate may not transfer sensitive personal data or information to any other body corporate in India or outside unless such other body corporate ensures the same level of data protection that the body corporate transferring the information is required to adhere to under the Sensitive Personal Data Rules.

Such transfer may be allowed only if it is necessary for the performance of a lawful contract between the body corporate and provider of information or where such person consented to the data transfer. However, body corporates located in India are often required to transfer sensitive personal data or information relating to their employees to data centres or their parent companies located outside India for processing of the information. The data centres or the parent company could be in a jurisdiction which does not provide an adequate level of protection as contemplated in the Sensitive Personal Data Rules.

As worded, Rule 7 seems to prohibit any such transfer. Is this the purpose that Rule 7 aims to achieve? Can such information be transferred by the body corporate in India if the other body corporate contractually commits to provide the same level of protection that is afforded under the Sensitive Personal Data Rules? This would impose an additional indirect burden with respect to protection of data on the body corporate outside India. However, this would be no different from EU data protection legislation, which restricts transfers of personal data outside of the EU unless certain measures are taken, such as requiring the data importer to sign up to 'Model EU Clauses'. Questions remain

over whether this aspect of the Sensitive Personal Data Rules goes beyond their mandate under Section 43A of the Information Technology Act, 2000.

Government access to information

Rule 6 permits transfer of sensitive personal data or information without obtaining consent from a provider of information if such sensitive personal data or information is requested by *"Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences".*

However, it is not clear whether this exemption would apply to transfer of sensitive personal data or information by a body corporate in India pursuant to an investigation conducted by a governmental authority in another jurisdiction (i.e. one that does not afford the same level of protection as that required under the Sensitive Personal Data Rules) or whether this exemption applies only to government agencies established under Indian laws.

In the present times, it would not be unusual for government agencies undertaking investigations in other countries also to require sensitive personal data or information that has originated from India and the obligations of an Indian body corporate under the Sensitive Personal Data Rules in such an instance are not clear.

Conclusion

The Press Note has addressed immediate concerns raised by the information technology and business process outsourcing industry. However, the Government of India needs to provide more clarity on how the Sensitive Personal Data Rules are to be applied by body corporates' located in India generally.

The Press Note is available here.

By Deepa Christopher and Praveen Thomas, Talwar Thakore & Associates, Mumbai.

Talwar Thakore & Associates is a "best-friend" of Linklaters LLP

Spain – Proposals for new cookie laws

The Spanish Government has issued proposals to implement the amendments to the ePrivacy Directive. The implementation will be by way of a Bill of amendment of Spanish Law 32/2003, of 3 November, on General Telecommunications (the "**Bill**"). This includes a range of provisions to improve customers' rights, guarantee better access to the internet, protect data, promote the quality of services and competition between different service providers.

Cookies

One of the proposed amendments relates to cookies and amends article 22 of the Spanish Law 34/2002 on the Information Society and Electronic Commerce. The Bill would oblige service providers to inform users, clearly and specifically, of the purpose of the cookie and to obtain *prior* consent from the user to install the cookie. This amends the current position which merely requires certain information to be provided to the user.

The Bill also allows for the creation of voluntary codes of conduct, preferably in an international framework. Such codes of conduct would provide guidance, particularly about measures to guarantee that users receive information in a clear, specific and easy way and can easily accept or refuse the cookie. This may be possible through the development of standardised icons.

Browser settings must be expressly selected

As in the ePrivacy Directive, the amendments state that where it is technically possible and effective, in accordance with the relevant data privacy regulations, the user's consent may be expressed by using the appropriate settings of a browser or other application.

However, for this condition to apply the user must select those settings during the installation or update of the browser through their own action. Cookies cannot be accepted by default.

Remaining issues

As with many other Member States' implementations, or proposed implementations, of this new law, a number of questions remain:

> how should the service provider inform users of its use of cookies? How much detail is needed?

> how should the service provider obtain the user's consent?

> how should the service provider deal with a revocation of consent?

As this is only a bill, the final wording of the implementation of the new cookie laws is still not agreed. Additionally, there will be general elections in Spain in November, so it is possible that the Bill will not be approved by then and that implementation of the amendments to the ePrivacy Directive will start again from scratch in 2012.

By Carmen Burgos and Beatriz Pavón, Madrid

UK - The ICO's audit programme: Gold stars for some, continuing pain for others

> *"I simply can't understand why you wouldn't accept a free audit from the Information Commissioner … I think it is very short sighted of private companies not to engage with the Information Commissioner"*[2]

The Justice Committee's recent hearing on the workings of the Information Commissioner revealed that only a fifth of private companies approached by the Information Commissioner have agreed to a consensual audit. This article looks at his audit programme and considers why take up has been limited to date.

What is the ICO auditing?

One reason why the audit programme is so interesting is because it provides an insight into the issues that really matter to the Information Commissioner. Each audit normally focuses on four or five issues and a breakdown of the issues covered in the audits carried out in the last 12 months is set out below.

Data protection issue	Included in audit
Governance	100%
Training and awareness	79%
Security	75%
Subject access requests	50%
Records management	42%
Data sharing	29%
Other	4%

The two specific issues that feature most heavily in the audit programme are the familiar bugbears: data security and subject access requests. This is not surprising and correlates closely with other enforcement action taken by the Information Commissioner.

Of more interest is the consistent focus on more general compliance issues: governance, training and awareness, and records management. Whilst accountability is still not a formal part of the European data protection framework, these statistics show it is already part of the Information Commissioner's compliance expectations.

What is the outcome of an audit?

The audit will provide an overall rating for an organisation's compliance from High Assurance, Reasonable Assurance, Limited Assurance all the way down to a Very Limited Assurance finding. An executive summary of the audit will normally be published on the Information Commissioner's website, though an organisation can ask that it be withheld.

[2] The Information Commissioner, Evidence to the Justice Committee on The Workings of the Information Commissioner, 13 September 2011.

Whilst the majority of the audits led to a Reasonable Assurance rating (61%) there is a substantial minority of Limited Assurance findings (29%). Only three organisations received a coveted High Assurance rating. Two of these are from the private sector, GE Money Home Lending and Nationwide Building Society, and one was from the public sector, DEFRA. The GE Money audit covered governance, training and awareness, security and subject access requests. It concluded there was "*limited scope for improvement … and as such it is not anticipated that significant further action is required*".

For others, the audit process may have required further action. The Law Society and the Ministry of Defence both received a Reasonable Assurance rating. This is the grade below High Assurance so not a serious cause of concern but both have been subject to follow-up audits by the Information Commissioner. For them the audit was not a one-off process and additional work will no doubt have been required for those supplementary audits.

What does a full audit report look like?

The audit itself is not a superficial exercise, as it involves both an off-site review of policies and procedures and on-site interviews to confirm they have been complied with in practice. Whilst the Information Commissioner only publishes an Executive Summary of the audit reports, the full reports for some organisations have been made available and demonstrate the level of scrutiny an audit involves.

One example is the full audit report for Portsmouth City Council, which runs to 40 pages. The audit covered governance, training and awareness, security and subject access requests and, whilst the Council clearly had good compliance measures and structures in place, it only received a Reasonable Assurance on the basis of a number of, occasionally, minor failings. A selection of these failings are set out below. Some may be frighteningly familiar.

> *Policies* - The Council's policies and procedures do not show the date of production, date of last review and responsible owner. Some appeared to be out of date. The Council agreed to resolve this issue by purchasing software (Conform) to ensure all such policies are owned, dated and regularly reviewed.

> *Governance* - The Council collected very few statistics on data protection compliance and there was no reporting on these figures to function or group leaders. The Council agreed to resolve this issue by collating statistics quarterly as part of the Governance and Audit report.

> *Privacy Impact Assessments* - There was no requirement for departments to conduct a privacy impact assessment ("**PIA**"). The Council agreed to ensure that PIAs are conducted for all new projects.

> *Technology* - The Council allows staff to scan and upload documents from their desktop computer to the central Electronic Social Care Record system. However, this process does not automatically delete the copy of the document stored on the local desktop computer. The Council agreed

to amend its process to ensure that duplicates of documents are not stored locally in the future.

These findings illustrate that the audit involves a deep dive with a detailed review of an organisation's systems, processes and technology. They also show that an audit can be used as a proxy for a wider accountability and compliance agenda, with organisations being expected to have strong compliance structures in place and adopt measures generally recommended by the Information Commissioner, such as Privacy Impact Assessments.

The Information Commissioner is clearly disappointed with the private sector's low level of engagement with his audit programme and indeed there are a number of advantages to agreeing to an audit (see TMT News: UK - Information Commissioner steps up his consensual audit programme). However, reviews of full audit reports made available to date demonstrate the relatively high level of scrutiny a consensual audit involves, that a good degree of compliance expected and the potentially detailed remedial measures that may be recommended by the Information Commissioner. Therefore, at the very least, it would seem sensible for an organisation to benchmark itself against these full audit reports before choosing to take part in the Information Commissioner's consensual audit programme.

Further statistics on the Information Commissioner's audit programme and the full audit reports for the Highways Agency, the Ministry of Justice and Portsmouth City Council are available from the authors on request.

By Georgina Kon and Sanjana Sagoo, London

An extended version of this article will appear in the November edition of Privacy Laws & Business. See www.privacylaws.com for further details

Telecoms and Media

Belgium – New code of conduct for Premium Rate Services

Following a significant increase in legal issues and disputes over the use of premium rate services, and particularly premium rate SMS, the Belgian legislator decided to impose stricter rules on these services. As a result, on 1 July 2011, the Royal Decree of 9 February 2011 concerning an Ethical Code on Telecommunications came into force in order to regulate premium rate services as well as to inform and protect consumers.

Background

After numerous cases of misuse of premium rates services, the legislator considered that the self-regulatory codes of conduct, including the GSM Operators Forum ("**GOF**") guidelines, offered inadequate protection to consumers. It therefore exercised its power under Article 134, §2 of the e-Communications Act of 13 June 2005, to issue a Royal Decree imposing a new, binding Ethical Code on Telecommunication.

This Ethical Code is an amalgamation of the self-regulatory codes, supplemented by additional provisions from the Mediator for Telecommunications, the Ministry of Economic Affairs, the Consumer Council, the Belgian telecom operators and GOF. Inspiration was also found abroad in certain provisions in international codes of conduct, especially the code of practice of the Irish premium rate regulator, RegTel. The codes of conduct applicable in the United Kingdom, Sweden, France and The Netherlands were also used to a lesser extent.

Scope

The new Ethical Code applies to any type of premium rate service, which is broadly defined by the Belgian legislator as "a service which through equipment connected to an electronic communications network allows the caller to obtain or send information, to contact other users of the information service, to access games or other benefits or to make payments for products or services provided during the communication or as a direct result thereof, on payment of a fee higher than the normal user-price for a communication to a standard geographic or mobile number".

The Ethical Code therefore applies to a wide range of services including premium rate voice, SMS, MMS and fax services.

New strict and binding rules

According to the new Ethical Code, the premium rate services should be fair and transparent, must not be misleading and should be up to date. In addition, strict rules on advertising apply. If any service is not suitable for minors, it must be clearly identified as such.

The service provider must also provide high-quality customer care and ensure that the general terms and conditions are available free of charge. The strict

information obligations on tariffs and consumption also illustrate the focus of the new Ethical Code on transparency.

Furthermore, the new Code sets out explicit rules for registration and deregistration of premium rate services providers, and confirms the double opt-in procedure as already required by the GOF guidelines.

Sanctions

The fines for breaching the Ethical Code have also been increased considerably in order to create an incentive for service providers to comply instead of simply treating fines as another business expense. The fines are administrative and have been increased from EUR 12,500 to EUR 125,000.

In addition, it is now possible to impose both a fine and suspension of operations, whereas under the previous regime only one or the other could be applied. Furthermore, operations can be suspended for 90 days instead of the previous 30 days.

Finally, for serious or repeated infringements, an infringing service provider can face an administrative fine from EUR 250 up to EUR 250,000, a suspension of operations for one year, and even the (permanent) removal of the service or a ban on new services.

By Didier Wallaert, Brussels

France - European Telecom Package finally implemented

On 26 August 2011, the long awaited French Ordinance no. 2011-2012 of 24 August 2011 on electronic communications, implementing EU Directives 2009/140/CE and 2009/139/CE, entered into force.

Overview

The Ordinance amends the French Consumer Protection Code, the French Penal Code, the French Postal and Electronic Communications Code as well as the French Data Protection Act. The driving principles of the Ordinance are to:

> ensure better regulation of the electronic communication sector;

> ensure more efficient spectrum management and to facilitate spectrum access; and

> reinforce consumers protection and data protection.

The Ordinance includes the following specific provisions.

Cookies

The Ordinance sets out the rules for the use of cookies requiring data controllers to:

> inform users about the purposes for which information is stored or is accessed on users' terminal equipment and about the means to prevent such storage or access (unless the users have already been informed); and

> obtain consent from users to such storage or access after having been provided with relevant information.

The law explicitly recognised that such consent may result from appropriate settings on a user's connection device or from any other applications placed under user's control. Such broad wording might allow consent to result from default browser settings, though this is uncertain and would contradict the Article 29 Working Party's position in its Opinion 2/2010 on online behavioural advertising.

User consent is not required where the cookie's sole purpose is to enable or facilitate the communication or it is strictly necessary to provide an online communication service requested by the user.

Data breach and security

Public network services providers should notify the French Data Protection Authority ("**CNIL**") without delay as soon as a personal data breach occurs in connection with the provision of electronic communication services. A personal data breach is defined as any security breach resulting accidentally or unlawfully in the destruction, loss, alteration, disclosure or unauthorised access to personal data.

Where such a personal data breach might impact a user or an individual's personal data or privacy, the service provider must also notify that person without delay, unless the CNIL determines that adequate protective measures have been implemented to render the data inaccessible by unauthorized persons (for example, as a result of encryption).

In cases where an operator fails to notify such breach, sanctions may be imposed of up to five years' imprisonment and fines up to €300,000. Operators must also maintain an inventory of data breaches, which must be provided to the CNIL on request.

There are also wider security obligations on electronic communications operators who must notify security and integrity breaches. The Minister in charge of electronic communications may also request a security audit of installations, networks and services provided by operators, at the operators' cost. A decree must still be adopted to appoint the person in charge of this audit process and fix the conditions for such an audit.

Other changes

The Ordinance will also introduce a number of other changes:

> *Increased power for the regulator* - The Ordinance will increase the independence of the French electronic communications regulator ("**ARCEP**"), extends its competences and increase its enforcement power.

> *Spectrum*: The Ordinance contains various provisions to facilitate use of spectrum including a right for ARCEP to impose a deadline for use of radio frequencies to ensure they are used effectively. New provisions have been included to enable the Minister in charge of electronic communications to allow spectrum trading.

> *Net neutrality*: In order to promote network neutrality, ARCEP's dispute resolution power has been extended to cover disputes between network operators and companies providing online public communication services. ARCEP also obtained additional enquiry powers with respect to companies providing online public communication services and it is entitled to impose minimum quality requirements.

> *Next generation networks*: In order to facilitate the development of next generation networks, the Ordinance set forth new rules to regulate access to physical infrastructure and cables from electronic communications operators. It also imposes specific deadlines on public authorities to answer operators' requests for access to the public domain.

> *Consumer protection*: Additional information must be provided to consumers. In addition, electronic communication service providers must offer to settle any disputes with its subscribers through an independent mediator.

> *Portability*: The deadline for operators to port numbers is reduced to one-business day.

Conclusions

There is little of surprise in the Ordinance as its contents are largely dictated by the European Telecom Package. It is good to see signs of an industry friendly approach with respect to the French implementation of the "cookies" rules. However, the security breach notification regime may raise concerns as there is no threshold trigger for the notification obligation. Hopefully the CNIL will issue guidance soon to avoid an explosion of notifications.

By Sylvie Rousseau and Ambre Fortune, Paris

UK - Website blocking: Do easy cases make bad law?

The war against online piracy is being waged on many fronts. In addition to enforcement action against suppliers and consumers of pirated materials, rights holders have now turned their sights on internet service providers.

One UK example is the successful application for an order requiring BT to block access to the pirate website Newzbin2 (see *Twentieth Century Fox & oths v British Telecommunications* [2011] EWHC 1981). However, there are concerns that this might lead to censorship of the internet and that it is technically ineffective in any event.

Newzbin2

The Newzbin2 website provides index files allowing its users to download copyright works from Usenet. It is well known for committing large-scale piracy. An injunction was issued against an earlier incarnation of the website, Newzbin1, after it was found to be: (a) authorising infringement by its users; (b) jointly liable for its users' infringements; and (c) a primary infringer by communicating infringing works to the public (*Twentieth Century Fox v Newzbin Ltd* [2010] EWHC 608). Shortly after that injunction Newzbin1 went into liquidation and the Newzbin2 website was set up.

The Newzbin2 site operates in essentially the same manner and under the same domain name. It has a substantial UK user base, requires payment in sterling and only uses the English language. The content indexed by the site includes movies, TV and music, the vast majority of which is pirated. The judge stated that it was "*quite hard to find any content of Newzbin2 that is not protected by copyright. BT's best shot was to point to a reference to the 1891 Lancashire census*".

The original owner of Newzbin1 denies any involvement in Newzbin2, which is operated by unknown persons, offshore and beyond the reach of the court.

Application to block access

The Newzbin2 website therefore presented the perfect target for an application to block access. Not only was it involved in large-scale piracy, its operations also appeared to have been deliberately moved out of jurisdiction to frustrate the earlier injunction against Newzbin1.

There was also no immediate technological obstacle to the injunction. BT already operates a system called Cleanfeed which uses a combination of IP address blocking and URL blocking using deep packet inspection (see below for details) to block access to child abuse sites notified to it by the Internet Watch Foundation. It would be relatively straightforward to add the Newzbin2 website to the list of blocked sites.

The rights holders therefore sought an injunction against BT to use the Cleanfeed technology to block access to Newzbin2. The content holders relied on section 97A of the Copyright, Designs and Patents Act 1988 and had to show that BT had "*actual knowledge of another person using their service to infringe copyright*". Section 97A implements art. 8(3) of the Information Society

Directive which states that rights holders should be "*in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe copyright*".

This was clearly a test case and other ISPs were informed in advance to see if they wished to intervene but none did so. However, despite the uphill battle facing it, BT chose to oppose the application on the basis of a number of points:

> *Was BT's service being used to infringe copyright?* BT argued that the users were using Newzbin2's services to infringe copyright, not its own. Moreover it was not an "intermediary" for the purposes of art. 8(3). However, Arnold J. said this argument was a false dichotomy. BT subscribers used both BT's services and Newzbin's services. Moreover, the European Court of Justice had already decided that internet service providers are intermediaries (*LSG v Tele2* C-555/07).

> *Did BT have actual knowledge of the infringements?* BT suggested that it was not sufficient that it should be aware Newzbin2 was generally infringing and instead must have knowledge of "*a particular infringement of a particular copyright by a particular identified or identifiable individual*". However, section 97A refers to the use of a service "to infringe" not to particular infringements so, while details of such infringements may be relevant, it is not essential to provide actual knowledge of a specific infringement of a specific copyright work by a specific individual. Similarly, the court had the jurisdiction to issue an injunction preventing general access to Newzbin2, not just to specific named works (see *L'Oréal v eBay* C-324/09).

> *Was BT subject to a general monitoring obligation?* Art. 15(1) of the E-Commerce Directive prevents ISPs from being subject to a general monitoring obligation. However, the court considered that measures requested by the rights holders were specific rather than general and were not active monitoring as Cleanfeed did not involve detailed inspection of the communications of its subscribers.

> *Would an order infringe BT's subscribers' freedom of expression?* There was no question that any interference with the subscribers' freedom of expression was potentially justified by the need to protect the rights of rights holders. However, BT relied on the Advocate-General's opinion in *Scarlet Extended* (C-70/10) to argue that section 97A was not sufficiently clear and did not provide the "quality of law" necessary to justify this measure. The court considered that section 97A was sufficiently clear and, while the European Court of Justice is yet to rule on *Scarlet Extended*, the facts of that case are sufficient to distinguish it in any event.

Accordingly, Arnold J. gave judgment to the rights holders and he will order BT to use Cleanfeed to block access to Newzbin2 once he has had further submissions on the nature of that order. However, this is not the end of the

matter. Questions remain about the extent to which this might lead to web censorship and whether the blocking is effective.

Censorship of the internet

The content holders stated that this was a test case and future injunctions will be sought, both against other ISPs and against other pirate websites. Indeed, a significant number of blocks would be required to cover the many pirate websites currently operating on the internet, and the pirate websites are likely to adapt their operations in a way that will require further blocks to be added in the future.

The potential for a flood of future requests was one of the concerns raised by BT when opposing the injunction. However, Arnold J. felt that the content holders would not undertake future applications lightly and did "*not anticipate a flood of such applications*". There are a number of reasons for this. Firstly an application would need to be supported by proper evidence to show that the website was, in fact, committing significant infringements. Secondly, the application would be costly and ISPs may be able to recover some of their costs in dealing with this application (see *Totalise v Motley Fool* [2001] EWCA Civ 1897). A third factor not considered in the judgment is timing. An application to block a website may take weeks to prepare and put in place. For particularly valuable content such as pre-release films or sporting events, it may be necessary to put a block in place within hours.

So it is likely that applications under section 97A will be limited and directed to the more egregious infringements. However, the real concern here is not websites being blocked following an open judicial process but the risk that many ISPs will want to avoid the time and expense of contesting future applications and instead block access on a voluntary basis. This process could sweep up not only egregious infringers like Newzbin2 but also other sites that might have a more tenuous link to piracy. Whilst *20CF v BT* may have been an easy case, it does not necessarily make good law.

Limited technical effect

A more significant problem for the rights holders is the ease by which these website blocking techniques can be avoided. These issues are considered in great detail in Ofcom's recent report, which was drafted to assist the UK Government in deciding whether to bring further website blocking powers under the Digital Economy Act 2010 into force. The report considers four main techniques to block access to sites:

> *Blocking IP addresses.* Computers on the internet communicate with one another using IP addresses. Those addresses are similar to telephone numbers on a normal telephone network save that they are often shared due to a shortage of available addresses. The IP address for Ofcom is 194.33.179.25. One technique is to block any access to IP addresses used by infringing websites.

> *Blocking DNS resolution.* Most users do not use IP addresses directly as they are hard to remember and can change. Instead, they type in a

domain name (such as www.ofcom.org.uk) and the domain name system returns an IP address (like 194.33.179.25). The DNS system is therefore like a giant internet telephone directory. DNS blocking acts to make certain domain names "ex-directory" by removing the IP address associated with that name.

> *URL blocking.* Resources on the internet are often accessed by not just specifying a domain name, but also specifying a particular file at that domain. One example might be www.ofcom.org.uk/piratedfilms. URL blocking acts at a more granular level by blocking particular URLs rather than entire domains. Thus it would be possible to block the previous URL whilst still providing access to www.ofcom.org.uk/consultations.

> *Packet inspection.* This looks at the content of the communication to determine if it is directed at an infringing website. For example, the BT Cleanfeed system inspects the URLs contained within packets of data sent by users to see if they are directed at a blocked website.

These solutions are all far from perfect. They can have a negative impact on the performance of an ISP's network due to the extra work involved in inspecting and filtering traffic. More importantly, there is a real risk of "over-blocking", particularly in case of IP address blocking, as this will also block access to any legitimate sites sharing that IP address.

There are also a range of measures users and website owners can take to evade these blocks. Some of the measures listed in Ofcom's report include:

> websites changing IP addresses. This is relatively simple to do. Indeed some websites, such as www.kickasstorrents.com, are set up to regularly cycle through a range of different IP addresses;

> websites changing their domain names. For example, changing www.ofcom.org.uk to www.ofcom.gov.uk. This again is not a difficult exercise;

> use of a proxy server. It is possible for users to connect to the internet via a proxy server. All of the user's traffic goes to the proxy server in the first instance and is forwarded on to its final destination. The ISP only knows the user is contacting the proxy server; it does not know what the final destination is;

> use of an alternative DNS service. Rather than using the DNS service provided by the ISPs (in which pirate websites may be "ex-directory"), it is relatively easy for users to specify an alternative DNS service, such as the Google Public DNS service. This avoids DNS blocking; and

> users encrypting their internet session to prevent packet inspection of their contents.

Following Ofcom's report, the Government decided not to bring new website blocking measures in the Digital Economy Act 2010 into force. The report was also made public after the judgment in *20CF v BT* but it appears that similar points were raised during the case and made little difference to the decision.

In particular, Arnold J. considered that even if website blocking only caused a limited increase in the cost and difficultly in accessing pirate websites that would at least narrow the gap with legitimate services. There is some truth in this. A user may now have to pay for: (a) access to Newzbin2; (b) a Usenet service; and (c) use of a proxy server, so may well prefer to opt for something simpler such as a subscription to LOVEFiLM®. In any event, Arnold J. considered the order would be justified "*even if it only prevented access to Newzbin2 by a minority of users*".

Conclusions

This is the first time rights holders have sought an injunction under section 97A, so the decision in *20CF v BT* provides a useful summary of its operation. However, there are a number of open questions about how website blocking will operate in practice. Will future sites be blocked as part of an open judicial process or as part of a private treaty between the rights holders and ISPs? How effective will these changes be in practice?

The decision is also an interesting prelude to the eagerly anticipated decision of the European Court of Justice's in *Scarlet Extended* which will consider the more ambitious proposition that ISPs ought to actively monitor and filter users' communications to prevent the exchange of infringing material.

By Muzaffar Shah, London

This article was first featured in the September issue of World Data Protection Report.

Outsourcing

UK - White-label agreements and disastrous exit periods

Of all the pillars of a contract, its term often appears the most straight-forward. However, as the Court of Appeal decision in *Interactive Investor Trading Ltd v City Index Ltd* [2011] EWCA Civ 837 demonstrates, this can be a serious pitfall if the interplay between the termination notice period, the exit assistance period and the overall term of a contract is not properly considered and clearly drafted.

Interactive v City Index also contains a health warning for companies using white-labelled products or services. A white-labelled arrangement will not necessarily result in a customer "belonging" to the company purchasing white-labelled services. This is despite the common assumption underpinning most white-label arrangements.

A "white-label" service

Interactive Investor Trading Ltd operates an interactive website which provides financial tools and information for its clients. It purchased a white-label service from City Index Ltd who operated an online trading platform which enabled trading in contracts for differences and spread betting. There were two white-label agreements, one in respect of contracts for differences and the other related to spread betting, under which Interactive introduced its clients to City Index's online trading services via a link on Interactive's website. Under the white-labelling arrangement, the trading services provided via Interactive's website all had Interactive's branding.

Once accepted by City Index, a client entered into a separate agreement with City Index. City Index then paid Interactive a share of the commission paid by clients on trades executed on the Interactive-branded platform.

Termination

Notice to terminate both agreements was served on 31 March 2010. The termination notice period under each agreement was three months, following which there was to be a "Wind Down Period". The Wind Down Period was defined in the agreements as "*the period of 6 months after termination of this agreement*". The term of the agreements was not specifically defined - the agreements were to continue until terminated by either party.

The agreements were not clearly drafted and the parties entered into a dispute over each other's respective rights and obligations before, during and at the end of the Wind Down Period. The dispute included Interactive's right to receive commission on trades executed during the Wind Down Period, and, more critically, the extent to which City Index could solicit clients during and after this period.

The wind down period

The agreements could be said to comprise three different phases:

> the business-as-usual service provision phase prior to termination of the agreement;

> the Wind Down Period; and

> the period after the end of the Wind Down Period.

Despite these more or less well-defined phases, the agreement contained a number of potentially ambiguous provisions. Rights and obligations were expressed to apply to a number of different time periods; "*for the duration of this agreement*", "*during this agreement*", "*on termination of this agreement*", "*on and following termination of this agreement*", "*during the Wind Down Period*" or "*after expiration of the Wind Down Period*".

In each case, it was not entirely clear how each expression of the different phases interacted or overlapped. Of particular importance was whether the Wind Down Period was, or was not, a continuation of the main term of the agreement.

Commission and solicitation

So, for instance, the link to City Index's online trading platform was to be maintained on Interactive's website "*during the Wind Down Period"* to allow City Link to deal with clients during this period. However, the obligation on City Index to pay Interactive a commission on trades executed by clients applied only "*during this agreement"*. The Court decided this meant that Interactive had to maintain the link to City Index's trading platform during the Wind Down Period but was no longer entitled to commission on any trades conducted.

The interplay of the various phases caused a similarly unpleasant result for Interactive in respect of the non-solicitation provisions in the agreements. City Index was not permitted to directly market to, or solicit, clients:

> "during the agreement"; and

> "after expiration of the Wind Down Period".

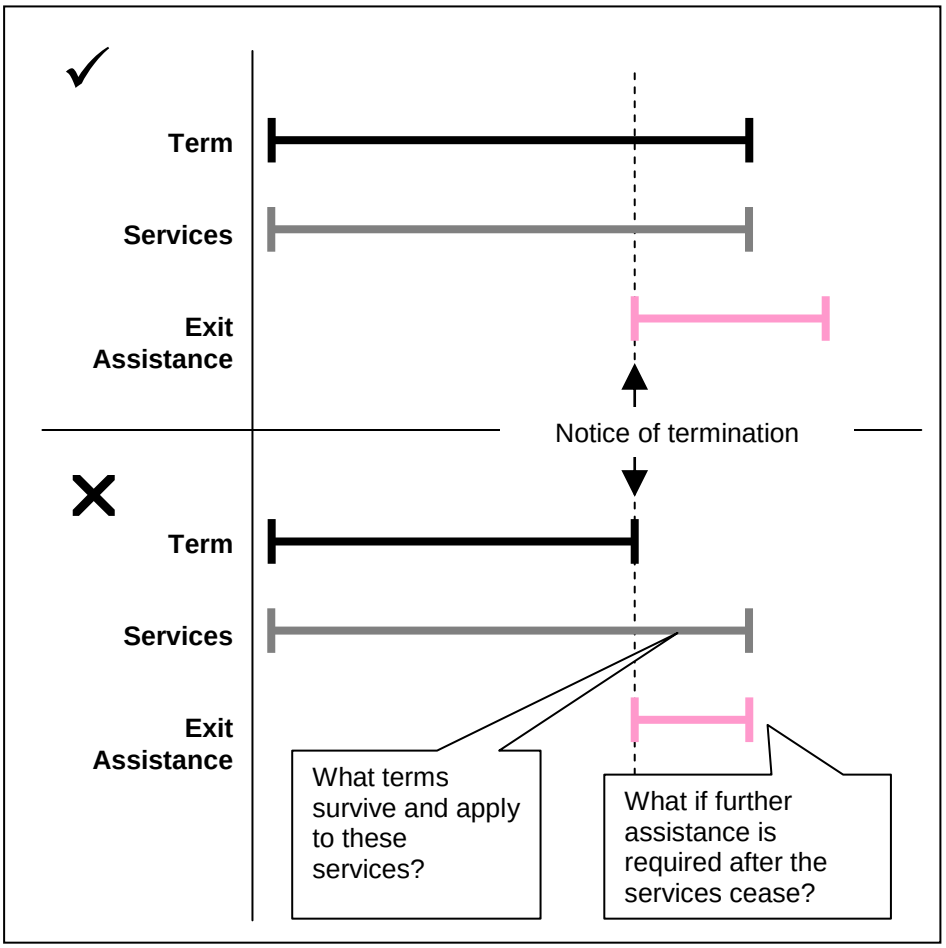
However, there was no prohibition on solicitation of clients during the Wind Down Period! Interactive argued that a commercial construction should be taken of the phrase "*during the agreement*" such that it extended to also include the Wind Down Period. This would reflect Interactive's expectation that it would retain complete ownership over any customer under a white-label arrangement. However, Tomlinson LJ concluded that "*language is used consistently within the four corners of an agreement*" and there was a window of opportunity during the Wind Down Period in which City Index was permitted to directly solicit clients to remain with it. A detailed and semantic

analysis of words might have to yield to business commonsense in some cases but not this one[3].

Drafting tips

The outcome in *Interactive v City Index* demonstrates the pitfalls of not adequately specifying what terms should apply during an exit period and, in the case of an exit period continuing after the term of the agreement, which terms should survive termination.

The best solution is normally to ensure that the provision of any business-as-usual services (as opposed to exit assistance services) does not extend beyond the termination of an agreement (see Diagram). It may be stating the obvious, but if the term and exit assistance period are not properly defined and the drafting does not clearly express whether or not the exit period is or is not part of the term of the agreement, the result can quite materially alter the "four corners of an agreement". In *Interactive v City Index* this meant that under a white-label agreement the provider was given access rights to clients which ordinarily would not be intended for such arrangements.



[3] *The Antaios Compania Neviera SA v Salen Rederierna AB* [1985] 1 AC

Similarly, it is important to consider exit assistance obligations. From a business continuity perspective, it is prudent for these duties to commence on the date that a termination notice is issued and to expire some time after the cessation of the services (see Diagram).

By Melissa Fai, Linklaters LLP, London

An extended version of this article will appear in the October/November edition of Computers & Law (see www.scl.org).

Author: Peter Church

Contacts

For further information please contact:

For further information please contact:

Tanguy Van Overstraeten
Partner

(+32) 2501 9405

tvanover@linklaters.com

Peter Church
Managing PSL

(+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