Linklaters

January 2014

Technology Media and Telecommunications.

EU - Coordinated enforcement action over Google's 'new' privacy policy

Google issued its new privacy policy in March 2012 to simplify and consolidate its numerous existing policies. However, it provoked a fierce reaction from European privacy regulators, not least because the policy allows greater sharing of user data across Google's different services. After a prolonged investigation, six regulators have taken coordinated enforcement action against Google. We provide an overview of that action and consider the wider privacy implications.

The 'new' privacy policy

Since its incorporation in 1998, Google has grown significantly, developing or acquiring numerous services along the way, including Google Maps, Gmail and YouTube. It has been particularly successful in Europe where its market share in web search is well above 90%. Its services have tended to have their own privacy policies, however, leading to 60+ privacy policies at one point.

Google therefore set out to simplify and consolidate these policies, whilst at the same time allowing information about users who have signed into Google services to be shared and providing a "simpler, more intuitive Google experience". Recognising this would be a significant change affecting a large number of people, Google added a prominent notice on many of its web pages about this change.

The new policy runs to nearly 2,300 words and sets out in broad terms what information Google collects, how it is used and what choices users have about the use of that information. Whilst it is clearly intended to be as user-friendly as possible and is written in (relatively) plain English, it has been subjected to a range of criticisms.

Regulators investigate

The new policy provoked a swift response from regulators. Prior to the change taking place, the Article 29 Working Party (a representative body of European data protection regulators) appointed the French data protection authority (the "**CNIL**") to lead an investigation into these changes.

Contents

EU - Coordinated enforcement over Google's 'new' privacy policy 1

EU – Proposals for Europe-wide protection of trade secrets 7

Belgium – Court uses criminal powers to take The Pirate Bay offline 14

Belgium - The Privacy Commission stretches its muscles! 16

France – New "Patriot Act" imposes surveillance obligations 18

China – New privacy rules for the telecoms sector 20

China – Shanghai Free Trade Zone opens to telecoms investment 23

South Africa - New comprehensive data privacy law passed 25

UK - Court of Appeal considers software copyright 28

UK - Social media and the law: A company handbook 32

The CNIL issued Google with a detailed list of questions and asked that the changes to the privacy policy be suspended until that investigation was complete. Google refused, arguing that it had made strenuous efforts to discuss the policy well in advance of its launch and to suspend it now was unfair. Google's new privacy policy went live as scheduled at the start of March 2012.

Findings and recommendations

The CNIL completed its investigation in October 2012 and issued its findings and recommendations. In broad terms, it identified three categories of individuals who use Google's services:

> *authenticated users* – these are users who have created an account with Google in order to receive services such as Gmail or Google Apps. Google is likely to obtain more information about those users but equally has greater opportunity to notify and obtain their consent to that use;

> *non-authenticated users* – these are users who use Google services, such as Search or Maps, without a Google account; and

> *passive users* – these are users who do not directly use Google's services but whose personal data is captured by Google from third-party websites, for example because of third-party cookies placed on their computer by Google's DoubleClick or Analytics businesses.

The investigation found a number of breaches of European data protection laws. In summary:

> *lack of information* – the new privacy policy did not provide enough information about what personal information was being collected and how it was being used. For example, the policy specified a number of vague purposes such as "*improving user's experience*". Nor was it clear how it used "the innocuous content of search queries" differently from more intrusive types of data such as credit card details or data on telephone communications; no distinctions were drawn. Finally, some types of data (the +1 button for example) weren't explained at all. Essentially, Google got the balance between simplifying the policy and providing comprehensive information to users wrong.

> *improper combination of data across services* – Google could not justify its processing of personal data. The CNIL focused on the combination of data about users from different services. This did not satisfy a statutory processing condition. In particular: (i) the privacy policy is too vague to form the basis of a specific and informed consent from users; (ii) in the majority of cases the processing was not necessary for a contract with the individual; and (iii) the extensive nature of the data collected by Google meant it cannot rely on the legitimate interests test (see art. 7(a), (b) and (f) respectively). The investigation also considered a number of other processing activities carried out by Google under the new privacy policy. The CNIL decided

that some were justified (such as security and academic research) but others were not as they required unambiguous consent (such as personalisation, product development, advertising and analytics);

> *use of cookies without consent* – Google's use of DoubleClick and Analytics cookies was in breach of art. 5(3) of the ePrivacy Directive as it failed to obtain informed consent to their use. This is a particular issue for passive users; and

> *retention period* – despite "numerous and detailed" questions, Google failed to clearly explain how long it retained copies of users' information.

The CNIL report made a range of recommendations to address these issues. For example, Google should improve the information its provides to users through the use of three tiered layered privacy notices (as recommended by the Berlin Group of data protection authorities over nine years ago), product-specific privacy notices and "interactive presentations". Google should also take a number of steps to legitimise its processing, including limiting the circumstances in which data is combined, simplifying opt-out mechanisms and making it easier for authenticated users to use Google's services on a non-authenticated basis.

The CNIL suggested greater protection for passive users and recommended Google take greater steps to inform them of any processing and limit the information collected about them.

National enforcement action

Google was asked to implement these recommendations by February 2013 but failed to do so. As a result, the CNIL established a working group of national data protection authorities to take coordinated enforcement action. In April 2013, it was announced that enforcement action would be taken by the French, German, Italian, Dutch, Spanish and United Kingdom data protection authorities. A brief overview of this enforcement action is set out below.

France – The CNIL fined Google €150,000 on 3 January 2014. This is the highest fine available. The fine was largely based on the breaches found by the CNIL in its earlier investigation in October 2012. The CNIL also ordered Google to publish an announcement about this sanction on its French website www.google.fr for 48 hours, indicating that Google was fined €150,000 for breach of data privacy rules and providing a link to the CNIL decision. Google has filed an appeal before the highest administrative Court (*Conseil d'Etat*). Should this appeal be rejected, Google will have to amend its privacy policy and practices or face further fines (which will double to €300,000 as it will be a repeat offence) and an injunction to prevent further processing.

Germany – In July 2013 the Hamburg DPA initiated administrative proceedings against Google Inc. challenging Google's privacy policies. Google was asked to present its case by mid-August 2013. Recently, the Hamburg DPA proclaimed that the information Google provided is currently

under examination in order to decide whether further steps against Google will be initiated.

Italy – The Italian data protection authority (*Garante per la protezione dei dati personali*) issued a press release on 20 June 2013 indicating it was seeking further information from Google about the processing of data of Italian users, particularly its use of privacy notices, the manner in which user consent is obtained, the storage of data and their combined use among different products and services. In a separate interview the Chairman of the Garante suggested that it wanted a response by 30 June 2013 and should Google fail to respond, the Garante "*will open a procedure that may lead to a sanction in the range of millions of Euro. Money is not a problem for Google, in fact the real sanction would be the loss of trust by consumers. Injuring privacy rights means limiting freedom for all*".

Netherlands – In November 2013, the Dutch data protection authority (*College bescherming persoonsgegevens*) issued detailed findings following its investigation into Google's new privacy policy. Those findings are broadly similar to those in the CNIL's earlier investigation in October 2012. The chairman of the Dutch data protection authority, Jacob Kohnstamm, stated that "*Google spins an invisible web of our personal data, without our consent. And that is forbidden by law*" and has invited Google to attend a hearing, after which it may take formal enforcement action such as an injunction to prevent further processing subject to periodical fines for failure to comply. The Dutch data protection authority can only impose relatively small fines itself. Criminal enforcement could lead to fines of up to €78,000, and even six months' imprisonment, but is unlikely in this case.

Spain – The Spanish Data Protection Authority (*Agencia Española de Protección de Datos*) has taken the strongest action. In December 2013, the AEPD found that Google does not give users enough information about what data they collect and for what purposes it uses them, that Google combines those data gathered through various services, keeps them for an indefinite time and makes it difficult for citizens to exercise their rights. Therefore, the AEPD found that Google has breached three provisions of the Organic Law 15/1999, of 13 December: (i) article 4.5 regarding the period of retention; (ii) article 6.1 regarding the consent of the data subjects (because of the lack of transparency); and (iii) articles 15 and 16 regarding the rights of citizens (for example, to access and rectify their data). The AEPD imposed a fine of €900,000 (€300,000 for each of the three breaches). It also ordered Google to amend its practices to comply with the law without delay.

United Kingdom - In contrast, the Information Commissioner has only taken limited steps to date. It contacted Google in July 2013 raising "*serious questions*" about the compliance of its new Privacy Policy with the Data Protection Act 1998. The main objection was the lack of information provided to users. Google was given until September 2013 to comply or face "*formal enforcement action*". So far no formal action has been taken. As much as anything this may be a result of the limited remedies available to the Information Commissioner.

Issues for privacy policies

The current enforcement action illustrates some of the problems with privacy policies. The data protection authorities want Google to include a lot more detail and for each service to set out exactly what personal data is collected, how it is used and to whom it is disclosed. In contrast, Google would clearly prefer to provide a simplified privacy policy that only describes at a high level how it uses personal data. This would allow it to innovate and amend its services without necessarily having to reissue its privacy policy each time.

Google's approach may reflect the hard fact that very few users will bother to read its new 2,300-word policy, let alone the more detailed policy envisaged by regulators. However, there are other ways to get your message across. For example, the CNIL's initial investigation in October 2012 made a number of recommendations such as the use of layered privacy notices, in-product privacy reminders and interactive presentations.

The privacy policies ought to also lead on to meaningful choices for users. However, Google's opt-out mechanism was found to be "too complex and ineffective". The CNIL's report suggests that a mobile authenticated Google+ user who does not want personalised ads would have to perform six different opt-outs. Moreover, the operation of some of the opt-out mechanisms is not clear in that they do not prevent the collection of data, but only the display of personalised content.

Jurisdiction questions remain open

The enforcement action is also predicated on the relevant national regulators having jurisdiction over Google. This issue is complicated by the fact that Google's search engine is operated solely by Google Inc., which is based in California. Local jurisdiction would therefore only arise if Google Inc. is established in that jurisdiction by way of a local subsidiary or because Google Inc. is using equipment, i.e. cookies, on users' equipment (see art. 4(1)(a) and (c)).

Establishing jurisdiction through either route is far from certain. Both Google and the national regulators must be eagerly awaiting the CJEU's decision on this issue in *Google v AEPD* (C-131/12). This is perhaps a good example of the justification for an extra-territoriality provision in the proposed General Data Protection Regulation.

Effectiveness of enforcement action

While this enforcement action is notable because of the close co-ordination of data protection authorities in a number of Member States, there is a question about how effective it will be in practice. So far Google has been fined a total of €1,050,000. In purely financial terms, this is around 0.003% of Google's turnover and was described as "pocket money" by Viviane Reding, the European Justice Commissioner. Ms Reding has instead called for fines of up to 2% of annual worldwide turnover in the General Data Protection Regulation (and the Parliament has gone further and called for fines of up to 5% of turnover).

Equally, it is not clear that the national regulators' actions are winning the war of hearts and minds. The single thing most likely to force Google to make significant and sustained changes to its privacy practices would be a migration of its customers to more privacy-friendly alternatives, such as the privacy-friendly search engine ixquick. However, despite fairly vigorous ad campaigns warning of the impact these changes could have on user's privacy (such as the "Every data point" campaign run by Microsoft) Google has held on to market shares in web search well above 90% in most European countries for several years now and there is little to suggest the latest action by regulators will reduce its dominance in the near future.

An extended version of this article appeared in the January 2014 edition of World Data Protection Report. See http://www.bna.com/world-data-protection-p6718/ for further details.

By Richard Cumbley (London), Daniel Pauly (Frankfurt), Paul Kreijger (Amsterdam), Alexandre Entraygues (Paris), Beatriz Pavon (Madrid) and Federica Barbero (Milan)

EU – Proposals for Europe-wide protection of trade secrets

At the end of 2013, the European Commission proposed a new Directive to harmonise the protection of trade secrets. The Directive contains a number of familiar concepts and broadly follows the provisions in the TRIPS Agreement relating to the protection of undisclosed information. We consider why these changes are being proposed and the implications for the IT sector.

Why is reform needed?

Almost all businesses rely on trade secrets, as much they rely on other forms of intellectual property. Trade secrets can be particularly important to small and medium-sized enterprises which lack the specialist resources to obtain and manage registered intellectual property rights. The protection of those trade secrets is also an important part of the European Commission's 2020 strategy to promote research and development investment and make Europe a more rewarding place for innovation.

However, the Commission considers that investment, particularly cross-border investment, is held back by the current diversity and fragmentation in the protection of trade secrets across Europe. Some Member States have specific legislation whereas others rely on general unfair competition or tort law. Some provide very limited protection, such as Malta which primarily relies on contract law. A summary of the position in some key European jurisdictions is set out below.

How will the proposed regime operate?

The proposals broadly follow the provisions in Article 39 of the TRIPS Agreement. The Directive will protect against the unlawful acquisition, use or disclosure of trade secrets, being information that:

> is secret, in that it is not generally known among or readily accessible to relevant persons in the field;

> has commercial value because it is secret; and

> has been subject to reasonable steps to keep it secret.

The acquisition of a trade secret will be unlawful in a range of circumstances including where it is the result of breach of a confidentiality agreement or other practice "*contrary to honest commercial practices*". Equally, the Directive sets out a number of situations in which acquisition will be lawful. Some of these are relatively familiar, such as independent discovery or reverse engineering. However, the Directive also expressly allows acquisition of trade secrets in conformity with "*honest commercial practices*" or, more unusually, as a result of workers' rights to information and consultation.

The Directive also contains a number of general exemptions and permits the acquisition, use or disclosure of a trade secret:

> for making legitimate use of the right to freedom of expression and information;

> where necessary to reveal misconduct, wrongdoing or illegal activity;

> to fulfil a non-contractual obligation; or

> for the "*purpose of protecting a legitimate interest*".

Finally, the Directive includes a minimum set of measures and remedies for trade secret owners. This includes the availability of interim measures, preservation of confidentiality during legal proceedings, injunctions and damages. However, a limitation period will apply and all claims must be brought within 12-24 months (depending on the national implementation of the Directive).

How will these rights interact with confidentiality agreements?

It appears that the new rights under the Directive are intended to co-exist with contractual confidentiality provisions. For example, the recitals expressly state the Directive will not affect the laws of contract.

Confidentiality agreements are likely to continue to be important because they can be used to impose more tightly-defined obligations (for example, avoiding difficult questions about what is an "*honest commercial practice*") and provide a parallel action for breach of contract. This could offer a longer limitation period for bringing claims than the 12-24 month period under the Directive.

Moreover, while a confidentiality agreement will not provide a direct contractual right against a third party who subsequently obtains the information, it may well assist with the enforcement of the trade secret owner's rights against that third party. For example, Directive expressly states that acquisition or use of a trade secret is automatically unlawful if it results from the breach of a confidentiality agreement or similar duty. In other words, the confidentiality agreement may well help define the statutory protection for the relevant trade secret.

What is an "honest commercial practice"?

The acquisition of a trade secret will be lawful if it is in accordance with "*honest commercial practice*". This concept originates from the TRIPS Agreement and, while the answer may be self-evident in many cases, it is easy to envisage more borderline situations.

The courts will have limited guidance in interpreting this term. While it is defined in a footnote in the TRIPS Agreement, the footnote does little to actually clarify its meaning[1]. Moreover, it will be some time before any cases on its meaning come before the CJEU and, even if they do, it may be difficult for the CJEU to make a definitive ruling on what is a very much a question of fact. Finally, the concept of an "*honest commercial practice*" will be new to a number of Member States, so their courts will not be able to rely historic practice.

[1] The footnote states: "For the purpose of this provision, 'a manner contrary to honest commercial practices' shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition".

What steps should you take to protect confidential information?

The Directive only protects a trade secret if it is subject to reasonable steps to keep it secret by the person lawfully in control of the information. This concept also originates from the TRIPS Agreement, but will be new in some Member States.

Businesses that rely on trade secrets may want to review the measures they use to protect that information - for example confidentiality agreements with employees and counterparts, protective markings and information security measures. They may also want to document these measures should they be challenged on this point.

What about other confidential information?

The Directive only applies to limited class of confidential information, i.e. information that has "commercial value". Confidentiality laws are drawn more widely in some Member States to protect not only commercial information but also other types of confidential information, including personal information.

Accordingly, the implementation of the law will raise difficult questions in some cases. Should it just cover trade secrets, thus creating a two-tier regime for confidential information? Or is this an opportunity to also "sweep up" other types of confidential information and protect them under a single statutory framework?

Implications for the IT sector and next steps

The proposed Directive does not radically change the protection of trade secrets across the European Union but should help to harmonise their protection, which may well help to foster cross-border investment and innovation. Unfortunately, these changes will not remove the need for confidentiality agreements and it is likely those in the information technology sector will continue to have the joy of negotiating these arrangements as a pre-requisite to the exchange of valuable confidential information.

The Commission's proposals will now be forwarded on to the Council and Parliament for consideration. If the proposals are adopted, Member States will have two years to implement the Directive into national law.

The Commission's proposals are available here.

This article has also been published in Computers & Law. For more details see www.scl.org

By Daniel Pauly (Frankfurt), Pieter Van Den Broecke and Tom de Coster (Brussels), Ewa Kurowska-Tober (Warsaw), Pauline Debré (Paris) and Peter Church (London)

Overview of the current protection of trade secrets in Europe	
Belgium	The proposed Directive would make minor changes in Belgium. There is no single Act for the protection of trade secrets. Trade secret owners can instead rely on general tort and unfair competition law as well as specific provisions in employment and criminal law. The misappropriation, use and disclosure of trade secrets can lead to civil liability under Belgian tort law (Article 1382 of the Belgian Civil Code). It can also be a breach of unfair competition law (Article 95 of the Act of 6 April 2010 on Market Practices and Consumer Protection). Employees and former employees may not disclose any trade secrets belonging to their (former) employer and more generally any secret in respect of a personal or confidential matter of which the employee became aware in the framework of his professional activity (Article 17,3° of the Act of 3 July 1978 on employment agreements). It is possible to file a complaint for disclosure in bad faith of specific technical know-how (so-called "manufacturing secrets") by employees or former employees of a manufacturer (Article 309 of the Belgian Criminal Code). Trade secret violations can lead to civil and criminal remedies including interim measures, compensatory damages, criminal fines and prison sentences. Although the court can take into account any profits made by the infringing party, there exists no separate measure of recovery of profits. Permanent injunctions to prevent further misuse are not easily granted, as most of the courts are reluctant to grant the holder of a trade secret a broader protection (unlimited in time) than most IP right holders (limited in time). In addition, it is not possible to launch a cease-and-desist procedure for breach of contract only. An *ex parte* search and seizure procedure is not available for holders of a trade secret either. Finally, the preservation of trade secrets during court procedures is not certain.
England	The proposed Directive would make a significant change in England in form and, to a lesser extent, substance. There is currently no statutory protection of trade secrets. Trade secrets are instead protected by contract and the laws of equity. Protection under the laws of equity applies to confidential information generally, rather than being limited to trade secrets. It protects information where: (i) it has the necessary quality of confidence; (ii) it was imparted in circumstances importing an obligation of confidence; and (iii) there is unauthorised use of the information to the detriment of the confider.

	Employees are obliged to keep confidential information secret during their employment as a part of their general duty of good faith to their employer. After employment, the employee is only generally prevented from using high-grade confidential information unless further restrictions have been imposed by contract. Breach of confidence gives rise to a range of civil remedies including injunctions to prevent further misuse, compensatory damages and an account of profits. There are no criminal sanctions.
France	The proposed Directive will introduce some minor changes in France and create a single set of rules that will help unify the current legislations on trade secrets. One major change is the limitation period of two years, which is shorter than the current limit of five years. Currently, trade secrets are subject to a patchwork of legislation with the main provisions being found in the Civil code and the Labour code, as well as in the Intellectual Property code. There is no single definition of trade secrets under French law, as various terms coexist such as "*know how*" and "*manufacturing trade secret*". Case law has defined the concept of know-how to be similar to the definition in the proposed Directive. In practice, trade secrets are mainly protected by tort and contract law. The general provisions of the Civil code provide a remedy in tort for a range of abuses including poaching, company disruption and abuse of pre-contractual discussions. Contract law is also widely relied upon and organisations will normally include confidentiality clauses in their employment contracts and sign confidentiality agreements with counterparties. A wide range of remedies are available under French law in case of trade secret violation, including injunctions, return and destruction or seizure of infringing goods, as well as damages. Criminal sanctions may also be imposed, including under French labour law. Finally, a trade secrets bill was proposed in early 2012. This bill contains similar provisions to the TRIPS Agreement and introduces a new offence of violation of "economic information" punishable by up to three years' imprisonment and a maximum fine of EUR 375,000. This bill was approved by the Assemblée Nationale but is currently stuck in the Senate.

Germany	The proposed Directive would lead to some helpful clarifications in German law, but will not make major changes. In particular, the law would need to more clearly define: (i) when trade secrets can be used; and (ii) how trade secrets are to be treated in legal proceedings. The protection of trade secrets is addressed in various areas of German law. The most important statutory provisions are included in the German Act against Unfair Competition and require employees and third parties to treat trade secrets confidentially. In addition, the protection of trade secrets is often covered in contracts, including employment contracts. Pursuant to German case law, a trade secret is any information: (i) in connection with the company; (ii) which is not public and known only to a limited number of persons; (iii) in relation to which the owner of the company has an economic interest to keep such information a secret; and (iv) which is kept a secret by the company owner. According to the German Unfair Competition Law, employees are prohibited from disclosing trade or business secrets learned during the term of the employment to any third party: (i) to compete with the company; (ii) to promote their own interests; (iii) to promote the interest of a third party; or (iv) with the intention of harming the company. After termination of the employment relationship, employees may use any (non-deliberately) memorised information if their personal interest in using such information outweighs the interest of the company in keeping such information a secret. The unauthorised disclosure of trade secrets may trigger civil law liability, including the obligation to compensate for damages, as well as criminal liability.
Poland	The proposed Directive would not make any major changes in Poland, as it is similar to the current protection for trade secrets provided under article 11 of the Act on Counteracting Unfair Competition of 16 April 1993. Under the Act, a trade secret includes technical, technological, commercial or organisational information having a commercial value, not revealed to the public, in relation to which the business entity took necessary steps to maintain its confidentiality. Employees are obliged to take care of their respective place of work, including protecting and maintaining the confidentiality of any information significant to the employer (art. 100 para 2 of the Labour Code). Moreover, arts. 101 and 102 of the Labour Code include non-competition provisions which *inter alia* impose non-compete provisions post-termination for employees

	who have access to particularly important information. Remedies available against trade secret violations have both civil and punitive character, including injunctions to prevent further misuse, compensatory damages and an account of profits. Criminal remedies are also available in certain cases.

Belgium – Court of Cassation approves use of criminal powers to take The Pirate Bay offline

In April 2012, the competent investigative magistrate ordered all Belgian internet service providers to block access to the notorious file sharing website, The Pirate Bay. He also ordered the Belgian cyber-crime unit to monitor the IP addresses used by The Pirate Bay and inform the internet service providers of any changes to those addresses so access can be blocked on an ongoing basis. This order is controversial as it is based on criminal powers of seizure. However, it has now been upheld by the Belgian Court of Cassation.

Blocking access to The Pirate Bay

A Belgian investigating magistrate issued the order using his power to seize data in the context of a criminal investigation. In this particular case, an investigation into the infringement of intellectual property rights.

While websites, such as illegal gambling websites, have been subject to blocking orders in the past, the current order is new and much more extensive in that it:

> applies to all Belgian internet service providers; and

> requires the blocking by all possible technical means of access to The Pirate Bay. This includes any IP address used by the site and any domain name used by the site, i.e. not just the main domain www.thepiratebay.org.

Use of criminal powers of seizure

The order was made under the Belgian Criminal Procedure Code. Article 35 gives judicial authorities the power to seize materials related to a criminal offence. Such a measure is temporary and subject to confirmation during the criminal trial. The purpose of these measures is in principle either to take away the object/produce of a crime or to preserve evidence thereof.

Articles 39*bis* and 89 of Criminal Procedure Code allow the authorities to make seizures of electronic data on IT systems by ordering appropriate technical measures to copy, block access to or delete such data. The order against The Pirate Bay used the latter two articles to block access to the website.

Appeal by the internet service providers

Unsurprisingly, three internet service providers appealed against the decision. However, on 22 October 2013, the Belgian Court of Cassation dismissed the final appeal, thereby confirming the legality of the order.

The internet service providers first argued the blocking measure is clearly imposed as a measure to prevent further intellectual property infringements and avoid damages incurred by the victims, i.e. the relevant rights holders. This exceeds the purposes for ordering such measures as they do not explicitly allow seizures to preserve the interest of the victim (although this

can be a reason to refuse the lifting of such measures). However, the Court of Cassation rejected this argument.

Secondly, the internet service providers argued they had immunity under the e-Commerce Directive (2000/31/EC) and could not be obliged to actively search for illegal activity or monitor the information they transmit and store. However, the Court of Cassation dismissed the argument. The order was validly issued under the Criminal Procedure Code and did not constitute a prohibited general monitoring obligation under the e-Commerce Directive.

Finally, the internet service providers argued that the measure was not being used to secure the integrity of the evidence, as the owners and users of The Pirate Bay are located outside of Belgium and can still access the website and its content. The Court of Cassation nevertheless considered it is not a requirement of Article 39*bis* par. 4 of the Criminal Procedure Code that the infringing party can no longer consult, modify or delete the affected data.

Conclusion

Rights holders will welcome the investigative magistrate using these powers to protect their rights, particularly because it will apply on an ongoing basis and The Pirate Bay cannot avoid its effect simply by changing their IP address.

However, it appears somewhat questionable that the Court of Cassation has allowed such measures to be ordered in the context of a criminal investigation. If the case does not go to trial, the measures should cease, and if it does go to trial, it is unclear what legal basis could be used to continue those measures. All the more striking is that it is unlikely this order would have been made in the framework of civil procedures for infringement of intellectual property rights.

There is also little consideration of the potential drawbacks and limitations of such an order. For example, IP address blocking can result in "over-blocking" of other sites sharing the same IP address and is easily circumvented through the use of a proxy server (see *Website blocking: Do easy cases make bad law?*).

Finally, these measures are also not necessarily limited to intellectual property cases. It will be interesting to see how it is used in the future and we could see an increase in criminal cases being brought to obtain such measures in other circumstances, for example in defamation cases.

By Guillaume Couneson and Tom De Coster, Brussels

Belgium - The Privacy Commission stretches its muscles!

In late October 2013, the President of the Privacy Commission announced his plan to create a special team to actively investigate privacy and data protection offences in Belgium. In the longer term, the Commission wants this team to be given the power to take enforcement action themselves rather than rely on the Public Prosecutor.

Data protection enforcement

Currently, the Public Prosecutor is in charge of enforcing individuals' privacy and data protection breaches while the Privacy Commission's role is to monitor overall compliance with these rules.

To that end, the Privacy Commission has a general power of investigation. It may file a complaint with the Public Prosecutor and institute a civil action before the President of the Court of First Instance. However, it may not impose fines or decide on any other enforcement action against infringers.

New special investigation team

The Commission considers that its current means and powers are not sufficient and that there is a strong need for it to proactively investigate breaches and increase its enforcement powers.

The Commission intends to set up a special investigation team in the coming months. Its initial focus is due to be data rich organisations, especially those massively processing sensitive data such as insurance companies and hospitals. Every year, a specific sector could become subject to an in-depth investigation.

Poor compliance calls for greater enforcement

This initiative has been triggered by recent data protection issues that occurred in Belgium, including a leak that affected data of thousands of railway travellers and a hacking incident that occurred in the telecommunication sector.

The Privacy Commission intends to actively seek out organisations that process personal data in a non-compliant manner, e.g. unlawfully selling information for marketing purposes or illegally transferring data beyond EU borders. Currently, the Commission considers control over these activities is almost non-existent or insufficient in practice.

The main source of information available to the Commission about data processing activities is the notification that data controllers are supposed to file with the Privacy Commission but there are still a lot of organisations that do not file such notification and so escape the Commission's scrutiny.

Wider European enforcement agenda

These changes mirror those in other parts of the European Union where an increasing number of regulators have been granted enforcement power, including the right to order the payment of administrative fines. This is the

case for example in France or in the UK, where fines can reach hundreds of thousands of euros.

The draft General Data Protection Regulation also provides greater enforcement powers for regulators with fines that can go as much as EUR 100 Million or 5% of the global annual turnover according to the most recent amendments of the draft voted by the European Parliament's LIBE Committee.

The initiatives in Belgium follow this trend and should lead to a stronger deterrent effect on potential infringers as the Privacy Commission should be in a position to act faster and more effectively in case of non-compliance than the Public Prosecutor. For example, the Commission is also seeking specific sanctioning powers such as the denial of access to a specific database, which may be more effective in practice than monetary sanctions.

However, new enforcement powers would require a change to Belgian data protection legislation which seems unlikely in the middle of the adoption process of the draft General Data Protection Regulation.

By Tanguy Van Overstraeten and Alana Van Caenegem, Brussels

France – New "Patriot Act" imposes surveillance obligations

Article 20 of the new *Loi de Programmation Militaire* has been described as the "French Patriot Act". It gives the French administration new surveillance powers, allowing it to request both content, data and metadata, including geo-location data. We provide an overview of the key provisions of this new law.

The *Loi de Programmation Militaire*

The French Parliament voted for the *Loi de Programmation Militaire* ("**LPM**") on 10 December 2013. It sets out various defence-related provisions for the period 2014-2019 but also includes new surveillance powers for the administration.

The changes are intended to consolidate existing surveillance powers regarding the content of correspondence (Article L.241-1 of the *Code de la sécurité intérieure*) and connection data and metadata (Article L.34-1-1 of the *Code des postes et des communications électroniques*) into a single new corpus (Articles 246-1 to 246-5 of the *Code de la sécurité intérieure*).

The changes also clarify these powers and extend their scope. For example, allowing geo-location data to be used for purposes other than fighting terrorism. The LPM also continues some surveillance provisions which were originally introduced on a temporary basis.

Main features

Article 20 of the LPM enables public authorities to require all "*information and documents*" from internet services providers, hosting services providers and telecoms companies. This includes:

> technical data concerning subscriptions or connection numbers to electronic communications services;

> data relating to all the subscription or connection numbers attached to a designated person;

> data enabling the geo-location of devices;

> data concerning the incoming and out-going calls of a subscriber; and

> the duration and date of the communications.

These rights have been provided to the Internal Affairs Department (*Ministère de l'Intérieur*), the Defence Department (*Ministère de la Défense*) and the Economy and Finance Department (*Ministère de l'Economie et du Budget*) who can access the information "in real time", by "solicitation of the network" or by direct requests to the relevant operators. There are little controls over the subsequent use of this information by public authorities.

However, the rights can only be exercised for the purpose of safeguarding national security, preventing terrorism, safeguarding essential French scientific and economic interests, prevention of cross-border and organised criminality and responding to hate groups.

There are only limited safeguards over these rights. Prior approval from a judge is not required. Instead, the Prime Minister office authorises surveillance. The National Commission for Security Interception must be informed of any authorisation granted within 48 hours and can investigate.

Constitutional challenge

Article 20 could still be subject to challenge on the basis it is not compatible with the French Constitution or with international Conventions.

Such a challenge could be based on the need for geo-location requests to be approved by a judge in advance in order to respect privacy rights. The French Supreme Court (*Cour de Cassation*) issued two judgments in October 2013 stating that geo-location requests from the police should be subject to prior approval by a judge in order to comply with Article 8 of the European Convention on Human Rights. A new bill regarding geo-location and real-time location has been submitted by the Government on 23 December 2013 to resolve this issue, although it does not cover all of the geo-location measures under the LPM.

Alternatively, the Constitution requires statutes to be sufficiently precise in their operation. Article 20 could arguably be challenged as it allows public authorities to ask for all "information or documents", without any details about the meaning of these terms.

Facing the Internet and privacy communities

The Internet and privacy communities consider that these sorts of surveillance powers damage customers' trust in cloud services and a number of major US Internet firms are publicly pushing for a reform of surveillance laws based on five cornerstone principles: limiting governments' authority to collect users' information; oversight and accountability; transparency about requests; respecting free flows information; and avoiding conflicting government demands.

Surveillance is, of course, a controversial topic given the recent PRISM revelations and the Advocate General's recent opinion that the Data Retention Directive breaches fundamental rights (Cases C-293/12 and C-594/12). In France, Isabelle Falque-Pierrotin, head of the CNIL, has objected to the fact she was not consulted about Article 20 and has called for a national debate on the surveillance society.

In the meantime, these rules will impose an additional burden for the telecoms sector. In theory, operators should be reimbursed for their costs in complying with these new requirements, but as for the HADOPI Act, no detail has been given about how this will work in practice.

The LPM should enter into force in February 2014. It is available here (French only).

By Alexandre Entraygues, Paris

China – New privacy rules for the telecoms sector

Chinese authorities took a number of important steps towards the implementation of national data protection regulation through the course of 2013. We consider the latest developments in the telecoms sector.

Privacy laws in China

As we reported in May 2013, the Standing Committee of the National People's Congress published a set of binding national rules in December 2012 relating to personal information collected electronically (e.g. over the Internet). These rules were the first of their kind to be issued by the Standing Committee, one of the highest legislative bodies in China.

In July 2013, following a public consultation period, the Chinese telecoms regulator (the Ministry of Industry and Information Technology) issued two further sets of binding rules relating to personal information. Both sets of rules, which implement the Standing Committee's December 2012 rules, became effective on 1 September 2013.

Privacy rules for the telecoms sector

The first set of rules relates to the handling of personal information by telecommunications and Internet companies. The rules apply to telecommunications business operators and Internet information service providers, including ISPs and any entity which provides goods or services over the Internet under an Internet Content Provider, or ICP, licence. The key provisions of these rules are set out below.

Definition of personal information - The rules define personal information (or "personal user data") as user names, dates of birth, identity card numbers, addresses, telephone numbers, account numbers, passwords and any other information from which the identity of a user may be ascertained by itself or in combination with other information. The definition extends to the time at which, and the location from which, a user uses a service and any other information collected by the service provider in providing the service.

Substantive obligations - The rules impose the following obligations on telecommunications and Internet businesses:

> When collecting and using personal data, businesses must notify users of the objective, method and scope of that collection and use.

> Businesses must obtain the consent of an individual prior to collecting or using their personal data. The rules do not specify if deemed consent is sufficient, or if express consent is required.

> Businesses must have policies related to personal data and make them publicly available.

> Businesses may not collect personal data in excess of what is necessary to provide the service for which the data is collected, and may not use that data for other purposes.

> After a customer has terminated their use of the relevant telecommunications or Internet service, businesses must cease collection and use of that customer's personal data. The rules do not go as far as to require organisations to delete personal data already collected, but simply to cease using that data.

> Businesses must establish complaint handling mechanisms and publish contact details for individuals to make complaints.

> Businesses must take certain prescribed action to protect the security of personal data held by them, including establishing security management systems, allocating internal responsibilities for protecting data and training personnel in data protection issues.

> In the event of a data security breach, businesses must take immediate action to rectify the breach and, if the consequences of the breach are serious, notify their supervising authority of the breach.

> Businesses must review their data protection practices each year and take action to rectify any issues identified in such review.

Sanctions - Businesses in breach of these rules may face penalties of up to RMB 30,000 (about USD 5,000). Criminal liability may be imposed for serious breaches.

Additional rules for fixed and mobile operators

The second set of rules applies to operators and users of fixed and mobile telecommunications services only. It requires:

> Operators to obtain documents (such as copies of passports or ID cards) to evidence the real identity of users of their services.

> Users to provide such information to operators.

Operators must not provide services to users that do not provide documents to prove their real identity or provide counterfeit documents. Operators must protect the confidentiality of the identity documents provided by a user and retain these documents for two years after the termination of the service provided to that user. Penalties of up to RMB 30,000 (about USD 5,000) apply to breach of these rules, and criminal liability may be imposed for serious breaches.

Other developments

There have been other data protection developments in China in 2013. Significant amendments to the Consumer Protection Law were passed in October 2013 to take effect from March 2014. These amendments include provisions requiring retailers (including online retailers) to obtain informed consent before collecting consumer personal data, to adopt measures to ensure confidentiality and security of that data, and to refrain from sending commercial information to consumers without prior consent. For more information on the amendments generally, refer to our October 2013 client alert available here.

In November 2013, a draft set of rules relating to the collection and use of personal information (including sensitive health information) by medical institutions was released for public consultation. These draft rules propose similar obligations as found in the telecoms and Internet rules described above, along with a prohibition on storing sensitive health information on servers outside of China.

Greater enforcement

These developments illustrate that the Chinese authorities have increased their focus on regulating personal information over the last 12 to 18 months, albeit on a sector-by-sector basis.

There have also been recent press reports of criminal action being taken in Shanghai and elsewhere for allegedly fraudulent collection and sale of personal data, indicating some willingness on the part of the authorities to enforce this growing privacy framework. We expect that further rules on personal data will come into effect during the course of 2014.

By Adrian Fisher, Shanghai

China – Shanghai Free Trade Zone opens to foreign investment in telecoms services

In September 2013, the Chinese authorities established the Shanghai Free Trade Zone (the "**FTZ**") which comprises four different areas, including the main FTZ area in the Waigaoqiao area of Shanghai. We provide an overview of recent changes to liberalise foreign investment restrictions for value added telecoms services in the FTZ.

Relaxation of foreign ownership

The original implementing rules for the FTZ were scant on detail, but indicated that foreign investment restrictions would be loosened within the FTZ in a number of different industries, including for value added telecoms services.

On 6 January 2014, the Shanghai government and the Chinese telecoms regulator (the Ministry of Industry and Information Technology) issued rules containing further detail of the liberalisation of foreign investment rules for the telecoms industry in the FTZ. These rules (which are still relatively high level) apply to the following services:

> *Ecommerce*: Foreign investors may hold up to 55% of the equity of an ecommerce business established within the FTZ. The national rules restrict foreign investors to a 50% equity interest in such businesses. This is most relevant for ecommerce platforms which sell third party products as an ecommerce platform that only sells the operator's own products is not generally subject to limits on foreign ownership.

> *Call centres, domestic multi-party communications services, Internet access services, mobile app stores and 'store and forward' services*: Within the FTZ, foreign investors can hold more than 50% of the equity of businesses that provide these types of services. Outside the FTZ, foreign investment is limited to 50% although in practice few licences have in fact been granted. The rules do not identify any cap on foreign investment within the FTZ, referring just to "more than 50%". An official interpretation of these relaxations posted on the government website confirms that foreign investors are able to operate these businesses within the FTZ through wholly owned subsidiaries (i.e. a WFOE).

> *Domestic Internet virtual private network (VPN) services*: The rules confirm that foreign investors will be able to hold up to 50% of the equity of businesses established within the FTZ that provide VPN services. This is the same as the cap under the existing telecoms rules.

While limited foreign investment in these services is already allowed to a limited extent, only a small number of foreign invested enterprises have been approved in practice. The fact that value added telecoms services are expressly referenced in the new rules may indicate the authorities are now more willing to actually grant foreign invested entities licences to provide these services.

National service provision

Significantly, all of the above types of value added services may be provided nationally, provided that all infrastructure/servers relating to the services are housed within the FTZ. The only exception is Internet access services which may only be provided within the FTZ.

So, for example, a foreign company could establish in the FTZ a joint venture with a local partner, held 55% by the foreign company and 45% by the local partner, to run an ecommerce platform. Provided the platform's infrastructure was located within the FTZ, the platform could sell products to consumers anywhere in China.

Similarly, a foreign company could establish a call centre through a wholly owned entity or in joint venture with a local partner, with the call centre housed within the FTZ but servicing clients throughout China.

Implications for telecoms policy

Telecoms services are currently, and will continue to be, highly regulated. These new rules appear to signal a certain degree of liberalisation in the ecommerce and value-added telecoms sectors and they represent an important development in Chinese telecoms policy. However, regulatory approval will still be required on a case-by-case basis and will not be automatic. It remains to be seen how the rules will be implemented in practice and it is likely further more detailed guidelines will be issued in the coming months.

By Adrian Fisher, Shanghai

South Africa - New comprehensive data privacy law passed

The Protection of Personal Information Act ("**POPIA**") was finally passed in November 2013. It has been a work-in-progress since it was earmarked for implementation by the South African Law Reform Commission in 2005. The delay in its enactment can be attributed in part to the publication of the draft EU General Data Protection Regulation as the POPIA drafting Committee paused to consider some of the proposed innovations in that Regulation. Indeed, it has adopted some of the more radical suggestions, such as mandatory breach notification and the so-called "right to be forgotten".

The POPIA is expected to come into force in the first quarter of 2014. "Responsible parties" - akin to data controllers - will then have one year within which to comply with the POPIA's conditions for lawful processing of personal information.

Application and jurisdiction

The POPIA provides for a general information protection mechanism applicable to organisations in both the public and private sectors. It will be supplemented by industry-specific and regulator-approved codes of conduct. The eight conditions for lawful processing in the POPIA are largely based on the principles in the 1995 EU Data Protection Directive.

An open-ended definition of "personal information" is contained in the POPIA. The definition goes further than its counterpart in the Directive in that it includes information relating to partnerships and companies, and provides a significantly detailed list of examples of personal information. These examples range from private correspondence and information about age, gender and sex through to assignments such as identity numbers, telephone numbers, location information and online identifiers.

The POPIA also defines "special personal information", such as information about criminal behaviour and biometric information, which is subject to more stringent conditions for processing. However, there are a number of exceptions such as the processing of information concerning a data subject's race, so that South African laws which are designed to redress historical racial discrimination are not compromised.

The POPIA does not apply to the processing of personal information in the course of a purely personal or household activity and includes a journalistic exemption where the responsible party is subject to "a code of ethics that provides for adequate safeguards for the protection of personal information".

Requirements for processing

Eight data protection conditions, based upon those contained in the Directive, inform the "conditions for the processing of personal information" in the POPIA:

1. Accountability
2. Purpose specification
3. Processing limitation
4. Further processing limitation
5. Information quality
6. Openness
7. Security safeguards
8. Data subject participation

Personal data should only be obtained from third parties (rather than the data subject) in limited circumstances such as: consent; where the information is contained in a public record; and where the collection of the information from another source would not prejudice a legitimate interest of the data subject.

Regulation, compliance and enforcement

The POPIA establishes an independent supervisory authority, the Information Regulator, with significant powers. These include the power to: authorise a specific breach of the processing of personal information; issue codes of conduct on its own initiative; and issue enforcement notices which, in the case of non-compliance, carry the penalty of a criminal offence. The Information Regulator also has substantial powers to conduct search and seizure operations.

The Information Regulator is tasked with the responsibility of regulating and overseeing compliance, receiving and processing data controller notifications, investigating non-compliance, facilitating mediation and conciliation of disputes, and referring non-compliance for prosecution.

A responsible party must take reasonably practicable steps to notify a data subject when collecting personal information, including the purpose of the collection, whether or not the supply of information is voluntary or mandatory, and whether the responsible party intends to transfer the information to a third country.

The data subject's rights under the POPIA include the right to request, free of charge, whether or not the responsible party holds personal information about them, as well as a description of the personal information held.

Breach notification and right to be forgotten

Where the responsible party has "reasonable grounds to believe" that data security has been compromised, the responsible party must notify both the Information Regulator and the data subject. Notification must take place "as soon as reasonably possible", but more exact time periods may be delineated in further regulations.

In what may be construed as a "right to be forgotten", a data subject may request the deletion of personal information that is "inaccurate, irrelevant,

excessive, out of data, incomplete, misleading or obtained unlawfully". These grounds for deletion are independent of the conditions for lawful processing.

Transborder flow of information

The POPIA prohibits transfers of personal information outside of South Africa subject to exceptions such as consent or where the recipient is subject to a law, binding corporate rules, or another binding agreement which effectively upholds data processing principles similar to the conditions for processing of personal information under the POPIA. It is at this stage unclear whether the Information Regulator will require prior approval of data transfer agreements, but from the wording of the POPIA it is doubtful that it will have the statutory power to insist upon such a process.

In some instances, a responsible party must obtain prior authorisation from the Information Regulator. For example, permission must be sought for planned transborder flows of special personal information or personal information of children to a foreign country not deemed "adequate". It is unclear how "adequacy" will be determined and indeed whether it may be assessed independently of the Information Regulator. This may be dealt with in further guidance or regulations.

Penalties

The POPIA imposes criminal penalties for offences that include the unlawful obstruction, interference or influence of the Information Regulator, the failure to assist without reasonable excuse a person executing a warrant in accordance with a search and seizure operation, and the failure to comply with an enforcement notice. In general, a person convicted of an offence in would be liable to imprisonment for a period not exceeding 10 years.

At the election of the offender, an administrative penalty in an amount not exceeding Rand 10 million (approximately Euro 650,000) may be imposed as an alternative to a criminal sanction.

Conclusion

The POPIA is an ambitious data privacy statute that will require careful attention from public and private bodies in South Africa and foreign entities seeking to receive personal information from South Africa. It is likely that some of the more vague requirements of the POPIA, such as time periods for breach notification and the determination of "adequacy" for the purposes of data transfers, will be articulated in greater detail by the Information Regulator once it is established.

Privacy professionals in South Africa will be following the developments of the EU Regulation closely in the hope it matches up to the provisions of the POPIA and that South Africa will in turn be found adequate for the purpose of European data protection laws.

By Dario Milo and Greg Palmer, Webber Wentzel, South Africa

UK - Court of Appeal considers software copyright

On 21 November 2013 the Court of Appeal gave its decision in the leading software copyright case *SAS Institute Inc v World Programming Limited* [2013] EWCA Civ 1482, confirming that WPL did not infringe SAS' copyright by creating a competing software system, except for minor aspects of WPL's users manuals literally copied from SAS' user manuals. This decision confirms that it will be difficult to establish infringement of copyright in software programs without evidence of copying of the underlying source code.

Background

This case has a long history. SAS developed a software package for data processing and analysis (the "**SAS System**"). WPL developed a competing system (the World Programming System, "**WPS**"), seeking to emulate the functionality of the SAS System. WPL had no access to SAS' source code and instead studied the SAS user manuals and the Learning Edition of the SAS System. SAS claimed that WPL infringed its copyright:

> in the SAS System, indirectly by creating the WPS (the "**Program to Program claim**");

> in the SAS manuals, by creating the WPS (the "**Manual to Program claim**");

> in the SAS manuals, by creating the WPS manuals (the "**Manual to Manual claim**"); and

> in the SAS Learning Edition, by using it to create the WPS, which was beyond what the licence permitted (and is thus also a breach of contract) (the "**Learning Edition claim**").

In 2010, Arnold J gave his first judgment in this case. He referred a number of questions to the CJEU on the interpretation of the Software Directive (2009/24/EC) and the Information Society Directive (2001/29/EC). In May 2012, the CJEU (Case C-406/10) held that functionality of software is not protected by copyright (see our newsletter *here*). In January 2013, Arnold J applied the CJEU's guidance and dismissed all of SAS's claims, save that the WPS user manuals infringed the SAS manuals as there had been a limited amount of literal copying. SAS appealed on all claims except the Program to Program claim.

Appeal Decision

The Court of Appeal affirmed Arnold J's decision and dismissed SAS' appeal. Lewison LJ gave the leading judgment.

Manual to Program claim - In addressing the Manual to Program claim, Lewison LJ made the following general remarks:

> Copyright does not protect ideas, only the expression of those ideas. The Software Directive says this expressly in relation to computer programs: "*only the expression of a computer program is protected and*

that ideas and principles which underlie any element of a computer program…are not protected by copyright under this Directive" (Recital 11 and Article 1(2)). The functionality of a computer program falls on the ideas side of the idea/expression line and is not protectable.

> A work is protected by copyright only if it is original in the sense that it is the *expression* of its "*author's own intellectual creation*". "Intellectual creation" requires both *room* for the exercise of creative freedom, and the *exercise* of that freedom by making free and creative choices. Where expression is dictated by technical function, there is no intellectual creation at all.

> The Information Society Directive and the Software Directive have the same policy goals, and the CJEU interprets Directives dealing with intellectual property consistently in order to establish a harmonised legal framework for copyright. As such, the CJEU's jurisprudence in respect of the idea/expression distinction and the "*intellectual creation*" test applied to software under the Software Directive applies equally to other copyright works under the Information Society Directive.

> The "*intellectual creation*" test may not be quite the same as the traditional test for originality in English law (which emphasises "labour, skills or effort"). "*If the Information Society Directive has changed the traditional test…it has raised rather than lowered the hurdle to obtaining copyright protection*". This is interesting as many view the "*intellectual creation*" test as broadening, not narrowing, the scope of protectable works.

In applying these principles, Lewison LJ held that what counts as an idea for the purposes of a computer program also counts as an idea for the purposes of a manual. The question for the court is not whether there has been a reproduction of the intellectual creation of the author of the manual, but whether there has been a reproduction of the *expression* of this intellectual creation. In this case, when WPL took elements such as statistical operations or mathematical formulae from the description in the SAS manuals, it did not reproduce the *description* of these operations in the WPS, but simply implemented them. WPL's work (the WPS) did not therefore represent SAS' work (the manuals) in any real sense. As such, there was no infringement.

Whilst Lewison LJ agreed with Arnold J on this point, he disagreed with his reasoning. Arnold J was wrong to concentrate on who did what (e.g. whether statistical methods were created by the authors of the manuals, or first created by the author of the software and then reflected in the manuals) – it would have been preferable simply to say that the copying that SAS alleged was not the copying of the form of expression of an intellectual creation.

Finally, it would be contrary to the policy goals underlying both Directives if SAS could achieve copyright protection for the functionality of its computer program indirectly *via* its manual which simply explains that functionality.

Manual to Manual claim - The same reasoning disposed of the Manual to Manual claim, in so far as it related to the WPS manuals describing the WPS' functionality that was based on the description in the SAS manuals.

Lewison LJ affirmed the reasoning of Pumfrey J in *Navitaire v easyJet* [2004] EWHC 1725 in the example of a chef who invents a new pudding and records the recipe (a literary work). If a competitor chef, "*after much culinary labour*", succeeds in emulating the pudding and records his recipe, the new recipe does not infringe the copyright of the earlier recipe, even though *"the end result, the plot and purpose of both (the pudding) is the same*".

Of course, where there had been textual copying from the SAS manuals (as Arnold J had found in some limited respects) that was a different matter and WPL did not challenge that conclusion.

Learning Edition claim

The Learning Edition claim was based on the provisions of the "click-through" licence terms. SAS claimed that the licence was restricted to use by the individual natural person who clicked on the "Yes" button, as the terms began with "*By clicking on the 'Yes' button, the individual licensing the Software ('Customer') agrees…*". In addition, the licence terms restricted licensed use to "non-production" purposes and prohibited certain other activities.

Arnold J had accepted that "Customer" in the licence terms meant the individual WPL employee. In contrast, Lewison LJ read "Customer" to be WPL because:

> the word "individual" can mean a single legal person including a company;

> the human who clicked the "Yes" button may do so as agent for the company;

> the licence prohibited concurrent use – redundant if the "Customer" must be a human;

> the word "Customer" ordinarily means the person who pays – here WPL had paid; and

> SAS positively averred that the licence agreement subsisted between it and WPL. It was difficult to see how there could be a licence agreement with a contracting party under which the contracting party acquired no licence.

Lewison LJ also looked at words on the packaging, but cautioned against taking an overly wide account of factual background in contractual interpretation, criticising, for example, Arnold J's consideration of material on the SAS website, in the absence of evidence that WPL visited the website: "*Almost anything is available on the internet these days and simply because something is available on the internet does not mean that it is relevant background*".

Ultimately, however, Lewison LJ agreed with Arnold J that the Learning Edition claim failed. Lewison LJ noted that the CJEU had interpreted Article 5(3) of the Software Directive (which provides that a person with the right to use a copy of a program shall be entitled, without further authorisation, to observe, study or test the functioning of the program) to mean that anyone entitled to use a program for any purpose was entitled to use the program for a number of other purposes, including to observe it to determine the underlying ideas and principles. Article 9 of the Directive also invalidates any contractual provision to the contrary. As such, Lewison LJ held (without deciding the point) that, even if WPL's use was a "*non-production use*" the restriction would be invalidated as contrary to Article 5(3).

Comment

Lewison LJ noted that the CJEU's decision "*was, at times, disappointingly compressed, if not obscure*". He also noted that, instead of answering the specific questions referred to it, the CJEU answered "paraphrased" questions, making it difficult to be sure whether the referred questions had all been answered and suggested that the CJEU, "*in the performance of its duty of sincere co-operation*", should answer the questions referred unless there are cogent reasons not to.

Lewison LJ emphasised that copyright protected *expression* of the author's intellectual creation, and elements that are unprotectable "ideas" under the Software Directive are equally unprotectable as part of any other work. Lewison LJ's acceptance in the course of this reasoning that the "*intellectual creation*" test applies to copyright generally is notable in light of recent practice of English courts to apply both the "*intellectual creation*" test and the traditional test. Finally, the interpretation of "individual" should be noted by copyright owners using "shrink wrap" or "click-through" licences.

By Kathy Berry and Tommy Chen, London

UK - Social media and the law: A company handbook

Social media has become an established part of our personal and, increasingly, professional and corporate lives. However, the reach and permanence of social media communications have generated a number of novel legal issues. For example, valuable assets such as contact lists become much harder to protect in a social media world, and conduct that might be low risk off-line may carry material legal risks once put in a social media environment.

Read our handbook for guidance and best practice on:

> the risks and rewards for businesses participating in social media;

> managing employees' use of social media;

> ownership of social media accounts; and

> the privacy and data protection implications of social media.

The handbook is available here.

By Richard Cumbley and Marly Didizian, London

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

A17682731/0.1a/31 Jan 2014