Linklaters

December 2014

Technology Media and Telecommunication.

EU – Have privacy regulators given the "right to be forgotten" global reach?

European privacy regulators have issued a formal opinion on the "right to be forgotten". It sets out criteria to determine when search results should be delisted. Regulators have indicated search engines should provide "effective" delisting of search results on all their domains, including .com, potentially giving this right global effect. They have also criticised the practice of notifying website operators when search results linking to their sites are delisted. These recommendations are not surprising but it remains to be seen how they will be implemented in practice.

Background

The "right to be forgotten" arises out of the European Court of Justice's decision in *Google Spain v AEPD* (C-131/12). The Court decided that Google was a data controller and so obliged to comply with European data protection laws. Other search engines with establishments in the EU, such as Bing and Yahoo!, should follow equally the principles of the decision.

These laws give individuals the right to ask affected search engines to supress any result returned on a search against their name. This right is not limited to old, irrelevant or excessive data and applies even if the underlying information is publicly available on the underlying website. Moreover, the search engine must comply with that request unless there is a public interest in continuing to make that information available.

This right is skewed heavily in favour of the individual because of the "jigsaw" effect. Even if the search result is of limited relevance in isolation, the combination of this information can create a structured and detailed profile of that individual.

The Article 29 Working Party

The decision seems to have been popular as shown by Google having received 178,119 requests for the removal of 625,116 URLs. So far the company has removed more than 250,000 links[1].

[1] Figures as at 1 December 2014 from https://www.google.com/transparencyreport/removals/europeprivacy/

Contents

The Article 29 Working Party, the representative body of European data protection regulators, has therefore prepared an opinion on the judgment[2]. The opinion should help to clarify how this new right operates in practice and ensure some degree of conformity in its application across the EU.

The opinion is "soft law", so is not binding on regulators or the courts. However, it is likely to have some persuasive effect and hard law effects. More importantly, it is a statement of intent by the regulators and so foreshadows their likely enforcement of the judgment in practice.

Global reach?

One of the more difficult questions raised by the judgment is its geographic reach. Google has taken a hard stance on this issue, supressing search results on European domains only (such as www.google.co.uk, www.google.fr) whilst leaving the results on other domains unaffected (such as www.google.com).

On the face of it, this reflects an understandable objection to the judgment having extra-territorial effect. For example, it could prevent US citizens accessing information in the US, a restriction that would be incompatible with US First Amendment rights.

However, only suppressing results on European domains undermines the effect of the judgment. It is trivially easy for European users to search on a .com site and so bypass any suppressions, and some do it as a matter of course. For example, Google has recently admitted that www.google.com is widely used by individuals in the United Kingdom, see *Hegglin v Google Inc.* [2014] EWHC 3793.

In light of this, the Article 29 Working Party has called on affected search engines to ensure delisting is "effective" on all domains and "cannot easily be circumvented". What this means in practice is not clear. At one extreme it might require the suppression of search results on all domains regardless of where the searcher is based. There is precedent for such an approach, such as the Canadian court's order that Google remove links to material infringing intellectual property rights[3], and the French court's order that links to a defamatory article are removed from Google's entire global network.

This would be a very aggressive application of the judgment. The regulators may feel this is justified on the basis they will apply a *de facto* limit on this right so it only applies to individuals with close links to the EU (see below). Alternatively, they may have chosen the word "effective" to open the way for targeted suppression based on geo-location information about the person making the request. Geo-location blocking is certainly possible and Google has recently admitted that they can block search requests on this basis by reference to IP addresses (see *Hegglin* above).

---

[2] *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* (WP 225).

[3] *Equustek Solutions Inc. v Jack*, 2014 BCSC 1063.

Obviously users may try to circumvent location-based filtering in order to get full search results, e.g. by making searches using a US-based proxy engine. However, at the very least this will make it more difficult for users to obtain supressed search results and the "hassle" factor has been sufficient for the English courts to impose filtering obligations in the past[4].

Highlighting delisted results to websites

Google currently informs website hosts if search results for webpages on those sites are delisted. This practice has, in some cases, attracted significant further attention to the underlying webpage, for example by creating further extensive press coverage[5]. In addition, there are a number of websites that track suppression requests.

Whilst there is a public interesting in understanding how the "right to be forgotten" is working in practice, the fact that the search result has been removed indicates the balance of interest favours its suppression. It is difficult to see how rebroadcasting its contents is justified.

In any event, the Article 29 Working Party is quite clear that these notices will, in many cases, relate to an identifiable individual[6] and so involve the further processing of personal data. Moreover there is no legal ground to justify the processing, and so the routine notification of delisting results to websites should stop. Search engines may, however, contact the website where it needs further information to assess borderline requests to supress a search result.

Equally, search engines should only add a notice to search result pages indicating that search results may have been supressed, if that notice is generic and does not inform the user whether a request for result suppression has actually been made.

Criteria for delisting

The opinion sets out 13 criteria that can be used by data protection when there is a complaint that a search engine has not supressed a search result. The criteria are set out in the table below.

The criteria are interesting in a number of respects. There is an argument that they start at the wrong point. The Court of Justice's judgment makes it quite clear that, as a "general rule", the rights of individuals to supress search results prevail over other interests and only in specific cases will the wider interests of the public in accessing that information justify the retention of the search result.

---

[4] For example, see *Richemont & Oths v British Sky Broadcasting & Oths* [2014] EWHC 3354 in which the English courts imposed a filtering obligation on ISPs to prevent access to websites selling fake goods. The court considered the effect of the order and stated: "*No doubt it is the casual, inexperienced or lazy users who stop visiting those websites, whereas the experienced and determined users circumvent the blocking measures; but that does not mean that it is not a worthwhile outcome*."

[5] See for example Robert Peston's article *Why has Google cast me into oblivion?* BBC News, 2 July 2014.

[6] While the removal notices do not identify the individual making the request, it is normally easy to work out their identify from the context and/or by making further searches against all named individuals on the webpage.

The criteria might better reflect this position by first considering what "specific cases" might justify retention of the search result, such as where the individual is a public figure or there is other public interest in retaining the search result. Only if there is such an interest is it then necessary to consider some of the more specific balancing criteria below. The criteria could also do more to address the "jigsaw" issue – i.e. the fact that the individual search result may have little impact in isolation, but might have a much greater impact when combined with other search results.

Equally, the criteria suggest that delisting is more likely where the information constitutes sensitive personal data. If you follow the Court of Justice's decision to its logical conclusion, this information should almost always be delisted as the search engine will not generally be able to satisfy a sensitive personal data processing (Article 8 of the Directive). Perhaps alive to the fact that such an approach would allow public figures to supress all sorts of information about their criminal behaviour and sexual proclivities, the Article 29 Working Party has chosen to gloss over this complication.

Finally, the criteria confirm that individuals can ask for search results to be supressed based on the individual's pseudonyms and nicknames.

Forum shopping

European data protection legislation applies to entities based on their location, not the location of the underlying individual. This means the right to be forgotten should apply to everyone, regardless of whether or not they are EU citizens or have a connection with the EU. The opinion suggests a significant weakening of this principle. It states that regulators will focus on claims where the individual has a "clear link" to the EU.

The reason for this restriction is not clear. It may be a question of resources and an attempt to limit the volume of complaints the regulators have to handle. Alternatively, it might be the *quid pro quo* for the extra-territorial application of the "right to be forgotten" (see above), in that while the regulators expect worldwide suppression of search results, that suppression right will only benefit EU citizens.

Forum shopping is also a potential issue within the EU. The regulators must hope the "common criteria" will help to harmonise their approach to this issue. However, it is not clear if this will happen in practice given the different cultural expectations in different Member States. For example, prior to the decision in *Google Spain*, two individuals in Germany successfully suppressed details of their conviction for murder in 1993. It's difficult to see an English court or regulator coming to a similar conclusion.

This may well be why the criteria are described as a "flexible working tool" to be "applied in accordance with the relevant national legislation" and the UK Information Commissioner will issue his own guidance on his application of the opinion. Whether national regulators allow forum shopping within the EU to exploit these divergences remains to be seen.

Finally, the opinion makes it clear the decision does not affect internal search engines – i.e. those that only search within a single website, as that will not create a complete "profile" of an individual in the same way as an external search engine.

By Tanguy Van Overstraeten, Brussels, and Richard Cumbley, London

This article first appeared in the December 2014 edition of World Data Protection Report. For further details, please see http://www.bna.com/world-data-protection-p6718/

	Criteria for assessing requests to supress search results
1	Does the search result relate to a natural person – i.e. an individual? And does the search result come up against a search on the data subject's name?
2	Does the data subject play a role in public life? Is the data subject a public figure?
3	Is the data subject a minor?
4	Is the data accurate?
5	Is the data relevant and not excessive? (a) Does the data relate to the working life of the data subject? (b) Does the search result link to information which allegedly constitutes hate speech/slander/libel or similar offences in the area of expression against the complainant? (c) Is it clear that the data reflect an individual's personal opinion or does it appear to be verified fact?
6	Is the information sensitive within the meaning of Article 8 of Directive 95/46/EC?
7	Is the data up to date? Is the data being made available for longer than is necessary for the purpose of the processing?
8	Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?
9	Does the search result link to information that puts the data subject at risk?
10	In what context was the information published? (a) Was the content voluntarily made public by the data subject? (b) Was the content intended to be made public? Could the data subject have reasonably known that the content would be made public?
11	Was the original content published in the context of journalistic purposes?
12	Does the publisher of the data have a legal power – or a legal obligation – to make the personal data publicly available?
13	Does the data relate to a criminal offence?

EU - The evolving relationship between data protection and consumer protection laws

The interaction between consumer protection, competition and data protection laws is getting increased attention from regulators and policy makers. This article considers the important role that consumer protection plays as a means to regulate privacy in the US and the reasons why European regulators are also turning to consumer protection laws. It also has an in-depth review of the data protection aspects of consumer protection laws in the UK.

The US approach

In the absence of comprehensive federal data protection laws, consumer protection has formed a key component of data protection enforcement in the US for many years. This can be seen in the Federal Trade Commission's high profile actions against household names such as Google, Facebook and MySpace for deceptive trade practices in relation to their privacy promises. Furthermore, the availability of class actions for aggrieved consumers has seen multi-million dollar claims made against the likes of Target, Yahoo and LinkedIn in respect of alleged data security breaches and the use and disclosure of customer data in contravention of stated privacy commitments.

The stringency of the orders imposed by the Federal Trade Commission (e.g. mandatory 20 year audit commitments and publication of details of breaches), and the level of fines levied for the breach of those orders (such as the record $22.5m imposed on Google for tracking Safari users) have helped to establish data privacy as an important compliance obligation in the US.

Evolving thinking in the EU

In contrast to the US, because the EU has specific, omnibus data protection laws with national data protection regulators to enforce them, there would seem to be little or no need to fall back on consumer protection law as a means to enforce privacy compliance.

However, with personal data increasingly perceived as an important currency in modern commerce, EU regulators and policymakers are considering whether the commercial exploitation of personal data is being adequately policed using existing legal and regulatory measures.

In March, the European Data Protection Supervisor lent its weight to the issue by publishing a preliminary opinion on "*The Interplay between data protection, competition law and consumer protection in the Digital Economy*". The opinion highlighted the focus of EU consumer policy on common standards, choice and fairness, including:

> the need for accurate information and market transparency;

> the promotion of consumers' welfare in relation to price, choice, quality, diversity, affordability; and

> safety and the protection of consumers from potential risks.

These principles are closely aligned to some of the key tenets of European data protection law, such as: the requirement for fair and lawful processing (including the provision of fair processing information); freedom of choice for data subjects; and the need for products and services to be designed to minimise data protection risks for affected individuals.

Jurisdiction and other issues

There are also a number of more prosaic reasons why some EU Member States might want to rely on consumer protection legislation rather than data protection law. For example, there might be more effective remedies under consumer protection legislation (such as the criminal penalties available under English law, as discussed below) and the law is likely to be enforced by a different regulator who may have greater resources and powers to bring offenders to book.

Another reason to invoke consumer protection law is to evade the "country of origin" principles mandated by the Data Protection Directive. Under these principles a data controller established in an EU Member State is subject to the regulation of that State alone (assuming there are no other relevant establishments). This has been a source of frustration for some regulators, particularly because a number of the large American tech companies have chosen to establish themselves in the Republic of Ireland which is seen by some as having a more lenient data protection regime.

However, consumer protection laws may provide a means to help overcome this jurisdictional hurdle. For example, is has been used recently in the German courts to help argue that certain retail terms and conditions (including data protection provisions) of major technology companies were invalid. Similarly, the consumer protection authorities in Sweden and Norway have specifically addressed issues such as the specificity of company privacy policies and the scope and effectiveness of consumer privacy consents for a number of years, often using laws designed to regulate marketing and unfair contract terms as a basis for their enforcement activity.

Further developments are expected in Germany, as the coalition agreement of the new German Government states that a new act will be implemented, extending consumer protection bodies' rights to issue cease and desist letters and to start legal proceedings so that they now apply to data protection breaches generally, and not just where such breaches relate to promises enshrined in customer terms and conditions.

The position in the UK

Until recently, the ability of individuals to use English consumer protection law to seek direct redress for alleged privacy breaches has been limited. These laws tended to focus on the product itself. Claims about the wider conduct of a merchant would have to be made via a variety of fairly tangential doctrines such as duress, undue influence, harassment and/or misrepresentation.

Equally, there have been a number of hurdles for those wishing to exercise direct rights of enforcement under the Data Protection Act 1998 (the "**DPA**").

For example, compensation for distress is only available where individuals can demonstrate that damage has been caused to them as a result of a breach of the requirements of the DPA. This has traditionally been seen as a high hurdle requiring pecuniary damage to be proved (see *Johnson v Medical Defence Union* [2007] EWCA Civ 262), which may not always arise. The position of the courts appears to have shifted on this issue, such as the suggestion that the courts should award nominal damages for a breach thus opening the way for a claim in distress, see *Halliday v Creation Consumer Finance* [2013] EWCA Civ 333. However, there have, to date, been few claims and the level of damages recovered has historically been low.

However, there are some areas in which consumer protection has started to make in-roads into areas traditionally covered by data protection laws. For example, The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing contains rules on database practice that closely mirror those under the Privacy and Electronic Communications Regulations 2003. Furthermore, the CAP Code obligations go slightly further than the Regulations by also controlling the sending of direct marketing for personal items to corporate email addresses. The CAP Code is enforced by the Advertising Standards Authority, whose more lightweight enforcement powers have sometimes provided a quicker and more effective remedy than the powers of the Information Commissioner.

New consumer protection legislation in the UK

More substantial crossover comes from the introduction of the Consumer Protection from Unfair Trading Regulations ("**CPUT**"), which implements the Unfair Commercial Practices Directive. CPUT prohibits misleading actions or omissions and aggressive commercial practices. These include:

> providing false product information or deceptive presentation;

> failure to abide by commitments under a code of conduct; or

> providing material information in a way that is unclear, unintelligible, ambiguous or untimely.

Based on this definition, you could imagine claims being made in respect of issues such as inaccurate fair processing information, or failure to adhere to published privacy policies or binding corporate rules.

The CPUT also prohibits traders from imposing onerous or disproportionate barriers to a consumer wishing to switch to another supplier. This might capture constraints imposed on consumers seeking to extract their data from a supplier in order to establish a relationship with a replacement provider.

In addition, the CPUT prohibits aggressive commercial practices, including making persistent and unwanted solicitations by telephone, fax or email, which could well capture some unsolicited direct marketing.

Finally, a number of consumer protection laws require disclosure of information, such as the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 and the Electronic Commerce (EU

Directive) Regulations 2002. From a data protection perspective, these disclosure obligations are closely aligned with some of the requirements to provide fair processing information under the DPA. They include requirements to identify the name and contact details of the provider of the goods or services, details of any third parties on whose behalf they are provided, as well as the salient characteristics of the goods or services.

Enforceable rights for consumers

Breach of the restrictions on misleading actions or omissions and aggressive commercial practices is an offence under CPUT, punishable by up to two years' imprisonment. As a result of the Consumer Protection (Amendment) Regulations 2014, there are also significant remedies offered to consumers.

These remedies are triggered by misleading or aggressive practices which are a significant factor in the consumer's decision to enter into the contract. On first glance, it appears this might not be that relevant to data protection breaches. However, many traders are now seeking to differentiate their products on the basis of their level of data protection compliance, and so such claims may become more feasible. Furthermore, once the components of a CPUT claim had been made out by the consumer, the burden of proof is on the trader to demonstrate that a breach of CPUT had not occurred.

If a breach of CPUT is proved, then the potential remedies for the consumer include a right to unwind, a right to a discount of between 25-100% of the price (for transactions under £5,000), or an entitlement to seek damages for consequential financial loss and alarm, distress or physical inconvenience or discomfort.

Use of these rights in practice

To date, consumers have faced considerable difficulties obtaining meaningful levels of individual redress for breaches of English data protection law. This is particularly apparent when compared with the volume and value of claims by individuals for privacy breaches in the US. The disparity with the rights enjoyed by US consumers derives from various factors, including US citizens' awareness of their rights, and the availability of class action suits and punitive damages in the US legal system.

While the recent changes to consumer protection law in the UK will not reduce these fundamental differences between the two legal regimes, they have established a number of new sources of individual redress for consumers. These new sources of redress are fairly broadly drafted and far less complicated to enforce than under the previous regimes. Therefore it is possible that resourceful consumers may find ways to exercise these new rights to address deficiencies in the data protection practices of UK traders. Whether this will deliver a meaningful improvement to the level of data protection compliance by traders in the UK remains to be seen.

By Julian Cunningham-Day, London

An extended version of this article first appeared in the November 2014 edition of Privacy Laws & Business, see http://www.privacylaws.com/.

EU - What is personal data? Just the facts…

The European Court of Justice has issued a significant decision on the meaning of personal data, *YS v Minister voor Immigratie* (Joined Cases C-141/12 & C-372/12). It suggests personal data should be limited to the facts and/or information necessary for the data subject to exercise their rights. This is a narrower definition than previously advocated by some regulators, including the Article 29 Working Party. The decision's most immediate impact is to limit the information that must be provided in response to a subject access request, though it will have wider ramifications as well.

Access to immigration files

The applicants made subject access requests to the Dutch immigration office for details of their immigration applications. The immigration office held a draft decision (a "minute") for each applicant. The minute contains:

> factual information about the application, being: "name, telephone and office number of the case officer responsible for preparing the decision; boxes for the initials and names of revisers; data relating to the applicant, such as name, date of birth, nationality, gender, ethnicity, religion and language; details of the procedural history; details of the statements made by the applicant and the documents submitted; the legal provisions which are applicable"; and

> the legal analysis of the applicant's case.

The immigration office used to provide applicants with a copy of the minute, but found this created a significant additional workload as applicants challenged its contents. It therefore adopted a policy of refusing to provide a copy of the minute, including in response to subject access requests. The applicants challenged this refusal and the matter eventually came before the Court of Justice.

What is personal data?

The key issue for the Court was whether the minute contained personal data. Unsurprisingly, it found that factual data about the applicants, i.e. "name, date of birth, nationality, gender, ethnicity, religion and language", was their personal data.

In contrast, the legal analysis, whilst it may contain personal data, was not itself personal data. In particular:

> the legal analysis "is not information relating to the applicant for a residence permit, but at most, in so far as it is not limited to a purely abstract interpretation of the law, is information about the assessment and application by the competent authority of that law to the applicant's situation"; and

> providing access to the legal analysis would not assist the applicants to guarantee the protection of their personal data – i.e. to confirm their personal data is accurate or processed in a lawful manner or to exercise their rights to rectification, erasure or blocking. Instead, it

would, in effect, provide a right to access to administrative documents which is not guaranteed by the Data Protection Directive.

However, this position is not absolute and there may still be elements of personal data contained in the legal analysis, albeit the legal analysis as a whole is not personal data.

How does this change things?

The definition of personal data is a core part of European data protection law. It determines the ambit of that law and the activities that fall inside or outside its scope. Accordingly, it has been considered on a number of occasions by both the courts and regulators.

One of the more significant developments is the Article 29 Working Party's Opinion 4/2007 on the concept of personal data (WP 136). This advocated a four stage test to determine what constitutes personal data, namely: (i) Is it information? (ii) Does it relate to a person? (iii) Is that person identified or identifiable? (iv) Is that person a living individual?

The second question, whether the information relates to an individual, has been a controversial issue. The Article 29 Working Party's opinion advocates a broad approach by reference to its:

> *content* – Is the information actually about an individual?

> *purpose* – Is the information collected with the intention of evaluating, affecting or influencing a particular individual?

> *result* – Is the use of that information likely to have an impact on that particular individual?

The Court of Justice's decision casts significant doubt on the Article 29 Working Party's analysis. For example, the legal analysis would clearly "result" in a significant impact on the individuals making the subject access request as it could determine if their immigration status. Equally, the "purpose" of the legal analysis is to affect or influence those individuals.

UK gold plating

The decision also has implications for the interpretation of the term personal data in the UK. The leading case is *Durant v Financial Services Authority* [2003] EWCA Civ 1746 which suggested that for information to be personal data, it must affect the individual's privacy, whether personally or professionally and that the subject access rights should not be used a proxy for litigation disclosure. A further gloss to this definition was added by *Edem v Information Commissioner* [2014] EWCA Civ 92 which suggested that the concepts in *Durant* were only relevant to borderline situations and did not apply where information is "obviously" personal data.

Durant has been extremely controversial and was one of the reasons for the European Commission's infringement proceedings against the UK for failing to properly implement the Data Protection Directive. It is therefore somewhat ironic to see the Court of Justice now issuing a decision that mirrors some

aspects of *Durant*, such as the fact that subject access requests should not be used as a means to obtain access to administrative documents[7] and that the definition of personal data should be shaped by the context in which it is used – i.e. access should be limited to information needed to assist the individuals to ensure the protection of their personal data under the Data Protection Directive.

However, perhaps more ironic is the fact that UK data controllers may obtain limited benefit from this decision. In particular, the definition of personal data in the UK expressly includes "any expression of opinion about the data subject" which is arguably wider than the equivalent definition in the Data Protection Directive. This could mean the legal analysis is potentially personal data in the UK albeit likely to be exempt from disclosure in response to a subject access request because it is legally privileged[8].

Further limits on subject access rights

The Court also confirmed that it is not necessary to provide documents to those making subject access requests. Instead, it is permissible to provide a "full summary" of personal data that allows the individual to check it is accurate, processed in accordance with the Data Protection Directive and to exercise their rights.

The decision may have other implications for subject access requests and provide further grounds to push back against onerous or unreasonable search requests. For example, it is not uncommon for subject access requests to ask for very broad searches of emails. The decision provides some grounds to push back on these requests on the basis that:

> the emails are unlikely to contain many additional "facts" about the data subject. The other information in the email is likely to be "assessment" or "application" of those facts to the data subject and therefore not personal data; and

> any information uncovered is unlikely to help the data subject identify inaccurate information, to determine if his personal data is processed fairly or to exercise his rights (though this will depend on the facts).

The decision may also provide grounds to resist subject access requests made in the context of litigation. The Court expressly stated that the subject access right is not intended to allow access to administrative files which, by analogy, would also suggest that the subject access right is not intended to be a proxy for disclosure.

[7] Or in *Durant* terms be a proxy for litigation disclosure.
[8] Schedule 7, para 10 of the Data Protection Act 1998.

Wider implications

The wider implications of this decision remain to be seen but the narrow approach to personal data taken by the Court of Justice is likely[9] to be applicable in other circumstances as well.

It is also interesting to note that the Court of Justice has not adopted a broad definition of personal data, suggesting that the earlier cases of *Digital Rights Ireland* (Joined Cases C-293/12 and C-594/12) and *Google Spain* (C-131/12) do not indicate a one way flow towards broader and stronger privacy rights.

By Peter Church, London

[9] For example, it could be argued that the decision should be limited to determining what is personal data in the context of a subject access request. However, there is nothing in the judgment to support such a narrow approach to its application.

Australia – Law Commission Report: "Serious Invasions of Privacy in the Digital Era"

The Australian Law Reform Commission has released its long-anticipated final report on serious invasions of privacy. The report proposes that a new statutory cause of action be implemented in a new stand-alone Commonwealth Act. If adopted, the proposal would have far reaching ramifications for investigative journalism in Australia and could also raise the spectre of class actions being brought against companies that have deliberately or recklessly mishandled their customers' personal information.

Background

On 3 September 2014, the Australian Law Reform Commission ("**ALRC**") released its final report on Serious Invasions of Privacy in the Digital Era (the "**Report**"). The Report follows on from the Terms of Reference (released on 12 June 2013) and the Discussion Paper (released on 31 March 2014).

The proposed cause of action has been designed to complement the existing privacy legal framework, including the Privacy Act 1988 (Cth), civil and criminal laws relating to harassment, unlawful surveillance and common law duties of confidence.

Elements of the cause of action

The proposed statutory action for serious invasion of privacy is conceived as an action in tort. This provides certainty with respect to a number of ancillary matters, such as vicarious liability, and a level of consistency that allows the action to operate in concert with existing tort law. The proposed cause of action also aligns Australia with a number of other jurisdictions (notably New Zealand and a number of Canadian provinces), allowing courts to draw on analogous case law.

The Report sets out five primary elements of the proposed tort:

> The invasion of privacy must occur by intrusion into the plaintiff's seclusion or private affairs (including by unlawful surveillance) or by misuse or disclosure of private information about the plaintiff.

> The invasion of privacy must be either intentional or reckless. In relation to what should constitute reckless, the ALRC recommended that a statutory definition be included in the Act, which could be based on the current definition in the Commonwealth Criminal Code.

> A person in the position of the plaintiff would have had a reasonable expectation of privacy in all of the circumstances. In determining this, the court may take into consideration: •the nature of the private information: the means used to obtain the information, the purpose of the misuse, disclosure or intrusion, how the private information was held/communicated, the relevant attributes of the plaintiff (eg age, occupation), and whether they displayed a desire to have their privacy invaded.

> The court must consider the invasion of privacy to be 'serious', having regard to, amongst other things, whether the invasion was likely to be highly offensive, distressing or harmful to a person of ordinary sensibilities in the position of the plaintiff.

> The court must be satisfied that the public interest in privacy outweighs any countervailing public interest. Public interest matters which a court may consider include: •freedom of expression and political communication: freedom of the media to investigate, the proper administration of government, public health and safety, and national and domestic security.

Remedies

The Report outlines a number of remedies which should be available to plaintiffs where a serious breach of privacy has been proven. These include, where appropriate:

> compensatory damages, including damages for the plaintiff's emotional distress;

> exemplary damages where exceptional circumstances have been proven;

> account of profits;

> injunction; and

> an enforceable undertaking (including a public apology).

A critical element of the Report's proposal is the recommendation that the tort be actionable per se, that is, a plaintiff should not have to prove that they suffered actual damage in order to bring an action. The Report also recommends that any damages awarded for a serious breach of privacy (other than those for economic loss) should be capped at the same amount for damages for non-economic loss in defamation.

Broad scope

As noted above, for the elements of the proposed tort to be met, an individual or entity will have had to either intentionally, or recklessly, seriously invaded an individual's privacy. The concept of recklessness sets a higher level of proof than the concept of negligence. It would, however, be triggered in circumstances where a person or company was aware of the consequences of their actions or omissions, but failed to act to avert those consequences. The obligations of organisations under the Privacy Act, and the Office of the Australian Information Commissioner's Guide to Information Security, may provide a useful reference guide for companies as to what positive actions would mitigate against any claim of recklessness. However, it is noted that the scope of the proposed legislation is significantly wider than under the Privacy Act, as are the potential consequences for the offending entity.

Primary among these is the right, under the proposed legislation, for an individual to take direct action against the offending entity where there has

been a serious breach of privacy. This contrasts with the rights currently available to individuals which are limited to lodging a complaint with the Office of the Australian Information Commissioner ("**OAIC**"). Additionally, the penalties which would be able to be enforced against defendants under the proposed legislation (as described above) are significantly wider than those currently available under the Privacy Act.

Sword not a shield

Although the proposed tort is designed to shield individuals' 'right' to privacy, there is a significant risk that the tort could be used as a sword by those who wish to conceal information that should legitimately be in the public domain. For example, an individual could seek to use the proposed action to bring an injunction against a media organisation seeking to publish information regarding that person. Any application for a permanent injunction would likely be preceded by an application for an interlocutory injunction to ensure the plaintiff is immediately protected from any imminent disclosure.

The Report acknowledges the difficulty of this issue and states that the public interest will be sufficiently protected because the legislation requires the court to weigh an individual's right to privacy against the public interest (which includes the freedom of the media to investigate matters of public concern). Notwithstanding this, it is conceivable that, in ruling on an interlocutory injunction, a court might err on the side of the plaintiff who stands to lose the most in the event that the application is dismissed. Once an interlocutory injunction is granted, it may then be some time before a full hearing can be completed and the matter ruled on by the court. This could have a chilling effect on legitimate investigative journalism.

Representative proceedings

In providing individuals with a right of direct action against offending entities, the proposed legislation also gives rise to the possibility for class action type claims being brought in situations where there has been a serious breach in relation to a large group of people. Although the Report did not make a specific proposal on this issue, it acknowledged the fact that the proposed legislation would be subject to the current law on representative actions (e.g. Part IVA of the Federal Court Act 1976 (Cth)). The effect of this is that it is likely that entities that intentionally or recklessly breach their privacy obligations could be subject to class actions where the personal information of numerous individuals is disclosed. This would provide further fuel to the burgeoning class action industry in Australia.

Differences between the Discussion Paper and the Report - Safe harbour

One of the key differences between the Discussion Paper and the Report is in respect of the original proposal to introduce a safe harbour scheme. The scheme, as outlined in the Discussion Paper, would have protected internet intermediaries (eg carriage service providers, search engines and social media platforms) from liability for serious invasions of privacy committed by third-party users of their services.

In rejecting the introduction of a safe harbour scheme in the Report, the ALRC noted that the proposed tort only targets positive conduct and is not aimed at omissions. On the basis that the intermediary would often be unaware that their service had been used to invade an individual's privacy, a failure to act by the intermediary would not constitute an invasion of privacy under the proposed tort as it lacks the requisite intention or recklessness. However, the intermediary may be found to have the requisite fault/recklessness where it can be proven that they had knowledge of the invasion of privacy and were reasonably able to stop it but chose not to.

Differences between the Discussion Paper and the Report - Right to be forgotten

The Discussion Paper had also advocated the introduction of a new Australian Privacy Principle ("**APP**") in the Privacy Act that would require APP entities to provide a simple mechanism for entities to destroy/de-identify personal information on an individual's request. Although the ALRC states in the Report that it is concerned that there is currently no simple mechanism for the destruction/de-identification of information, it has decided not to recommend the introduction of a new APP. The Report cites the submission from the OAIC that the introduction of such an APP would be inconsistent with the Archives Act 1983 (Cth) and therefore would not apply to Commonwealth agencies as the reason for not pursuing this further. Additionally, the OAIC pointed to the current obligations that the APPs impose on entities and that a better approach may be for the OAIC to issue additional guidelines in relation to entities' obligations to destroy or de-identify information.

The position taken by the ALRC in the Report runs counter to the current position in other jurisdictions, most notably Europe, where the recent *Google Spain* decision has reinforced individuals' right to direct entities that hold the individual's personal information to remove or de-identify that information.

Next steps

The Report has been presented to the Commonwealth Attorney-General for his consideration. The Attorney-General has already noted his position that he is not in favour of the introduction of a new cause of action for the serious invasion of privacy (and it should be noted that the Report was commissioned by the previous Labor government). On the basis that the Report does not substantially differ from the position put forward in the Discussion Paper, it is highly unlikely that the current government will implement any of the Report's recommendations. This is the second occasion in six years that the ALRC has made similar recommendations. This latest proposal looks destined for the same fate as the last.

By Gavin Smith, William Coote and Brydon Wang, Allens, Sydney

Belgium – Telenet ordered to open up cable services

On 12 November 2014, the Brussels Court of Appeal gave a long-awaited judgement, upholding the decision by the Belgian telecom and media regulators to order cable providers to give wholesale access to their television and broadband services.

Order for wholesale access

In December 2010, the Belgian telecom and media regulators jointly stated their expectation that cable networks should open up their services to alternative operators. The European Commission welcomed this initiative, whilst expressing some concerns with regard to the specific justifications.

A few months later, on 1 July 2011, the Conference of Regulators of the Electronic Communications Sector ("**CRC**") issued a decision to this effect. The CRC is a conference of all telecom and media regulators in Belgium and consists of the national telecom regulator BIPT and the regional regulators CSA, VRM and Medienrat.

The CRC's decision is intended to improve the Belgian television market in terms of price, quality and offering. More specifically, the current operators of the cable networks (i.e. Telenet, Brutélé, Numéricable, Publifin and AIESH) were obliged to offer:

> wholesale access for analogue television;

> access to their digital television platform; and

> wholesale access for cable broadband.

The wholesale offer must be subject to obligations of non-discrimination, transparency and price control. In other words, the current operators of cable networks must open up their networks for competitors. By removing the high entrance barriers, the CRC wished to create a level playing field and a competitive television landscape.

Appeal to the Brussels Court

The cable operators objected strongly to the CRC's decision, and Telenet appealed the decision before the Brussels Court of Appeal.

Belgacom (currently known under its new name "Proximus") also joined this appeal because the decision did not extend to them. In particular, they could not benefit from the wholesale offer for broadband and access to the digital television platform.

The Brussels Court of Appeal has now issued its opinion upholding the decision of the CRC and therefore rejecting the claims of Telenet. The Court confirms that the CRC was well within its power to impose an *ex ante* regulation. In particular:

> the most important condition is the presence of significant market power (i.e. for Telenet) in a defined relevant market. This was the case; and

> the remedies imposed by the CRC were proportionate, necessary, legitimate and answering to a certain need of the market (e.g. Mobistar's indication to enter the digital television market). Therefore, the Court saw no reason to reject the imposed measures.

In addition, Belgacom's claim was also granted. The Court considers that Belgacom was treated unequally and therefore annulled that part of the CRC decision. In other words, Belgacom gets access to the entire regulated wholesale offer.

Consequences for the (Belgian) television landscape

The consequences of this decision are significant for the Belgian television landscape. It appears to be a victory for Belgacom and Mobistar. Mobistar does not have its own cable network, but will now finally be able to offer digital television and internet services via the cable network of Telenet.

This decision may also have a significant impact as a precedent for the wider European market. Potential operators and regulators may use this decision as means to argue for the opening up of their television market.

By Bastiaan Bruyndonckx and Emma Ottoy, Brussels

Belgium – Launch of Cyber Security Centre

On 14 November 2014, the Belgian Government announced the launch of a Cyber Security Centre in early 2015. A Royal Decree setting up this centre was subsequently published in the *State Gazette* on 21 November 2014. The centre will oversee and co-ordinate the handling of cybersecurity issues in Belgium in response to the ever growing threat of cyber attack.

Multi-stakeholder response

The creation of the Cyber Security Centre ("**CCB**") is part of Belgium's wider cybersecurity strategy. Over the years, Belgium has developed expertise in the field of cybersecurity through public, academic and private bodies.

This includes numerous dedicated authorities, such as the Federal Cyber Emergency Team (CERT) for the central reporting of cyber-emergencies, Federal and Regional Computer Crime Units (FCCU/RCCU) within the police force and the Federal Public Service for Information and Communication Technology (FEDICT).

In addition, several public bodies have regulatory powers in the field of cybersecurity, including the Belgian Institute for Postal Services and Telecommunications (BIPT), the Belgian Data Protection Authority (Privacy Commission) and the National Bank of Belgium (NBB). Lastly, the civil and military intelligence and security bodies in Belgium have cyber defence specialists.

The academic sector is also active through the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) coordinated by the University of Leuven and the Centre de Recherche Informatique et Droit (CRID) of the University of Namur.

Finally, there are a number of industry bodies representing private sector entities with expertise in cybersecurity such as Agoria (the Belgian federation for the technology industry), ISPA (the Belgian association of Internet Service Providers) and sector specific organisations such as the Belgian Telecom User Group (BELTUG) and the Belgian Financial Sector Federation (FEBELFIN). These bodies support their members and inform the public at large regarding the fight against cybercrime.

Role of the CCB

CCB will act as a sort of "Chief Information Security Officer" for Belgium, co-ordinating other stakeholders and providing expertise and political support to develop coherent policies and guidelines. Its formal role will be to:

> oversee the implementation of cybersecurity in Belgium and handle crisis management when incidents arise;

> act as a platform for all stakeholders (public, private and academic) to coordinate their efforts and inform the public;

> represent the position of Belgium in international forums; and

> develop standards, security norms and directives for IT systems.

Resourcing

The CCB is expected to have 10 staff members, which is a relatively small number compared to other countries. By way of comparison, the UK Office of Cyber Security and Information Assurance has a staff of more than 700 persons and the French Agence Nationale de la Sécurité des Systèmes d'Information has about 230 staff members.

However, this relatively small number should be seen in the light of the existing specialist bodies charged with cybersecurity tasks and the primary role of the CCB will be one of coordination. It is also interesting to note that prior to the elections, the former Belgian Prime Minister indicated that a portion of the cybersecurity budget would be made available to hire additional personnel for the various other public authorities involved in this field. Overall, the new CCB is a welcome addition to the country's cybersecurity strategy.

By Guillaume Couneson, Brussels

Belgium – Constitutional Court strikes down privacy exemption for Ministry of Finance

The Belgian Data Protection Act used to contain a broad provision limiting data subjects' rights where personal data was being processed for tax audits and investigations by the Ministry of Finance. This provision was successfully challenged before the Belgian Constitutional Court on the basis that it was too wide, and partially annulled. It has in the meantime been replaced by a new, narrower, provision. This provides a useful example of willingness of the courts to strike down legislation that unduly curtails citizens fundamental rights such as the right to privacy.

Overly broad exemptions

Article 3 of the Belgian Data Protection Act (the "**DPA**") limits data subjects' rights in certain situations, such as where data processing operations are carried out by the police or security services. A seventh paragraph was added by an Act of 3 August 2012, providing an additional exception for certain data processing operations by the Ministry of Finance.

It stated that the right of information, access and correction of data subjects does not apply in the period during which an individual is the subject of a tax audit or investigation by the Ministry of Finance, as well as during the preparation of such an investigation.

The Court however considered that this new paragraph limits a data subject's rights beyond what is strictly necessary, as:

> it applies to *all data* processed by the Ministry of Finance about the data subject, even if part of the data is not relevant to the audit or investigation; and

> the new paragraph defines a beginning and an end point for this limitation, but does not provide for a maximum period of time in between.

The Court therefore ruled this paragraph violates the Constitution, as it is incompatible with the principles of equality and non-discrimination laid down in Articles 10, 11 and 172 of the Constitution. As a consequence, the Court partially annulled the provision.

New provision

The partially annulled provision was replaced by the legislator in the course of the proceedings, before the Court issued its decision.

The replacement text in Article 3 paragraph 7 of the DPA is more moderate. The exemption only applies to data subjects' right of access (Article 10, DPA) and only suspends this right where its exercise would jeopardise the (preparatory activities of) an inspection or investigation by the Ministry of Finance. The application of this exception is also limited to a maximum period of one year.

The constitutional right to privacy

Due to a procedural mistake by the claimant, the Court was not able to also rule on the compatibility of the provision with the right of privacy embodied in Article 22 of the Constitution. The claimant only raised this argument at a late stage in the proceedings, and so it was dismissed by the Court.

However, relying on the more general constitutional principles of equality and non-discrimination, the Court nevertheless upheld the right to privacy in its decision, emphasising that any limitations to the right of privacy of data subjects must be based on an objective and relevant criterion and must be proportional to the objective pursued by the legislator.

This decision demonstrates the importance of the right to privacy for the Court and its willingness to challenge legislation that unduly curtails the fundamental right of citizens to review the use of their personal data by the government, in this case the Ministry of Finance.

By Guillaume Couneson and Emma Ottoy, Brussels

Belgium - Privacy Commission consultation on cookies

In April 2014, the Belgian Privacy Commission issued a consultation containing draft recommendations on the use of cookies in Belgium. The recommendations are detailed (over 60 pages) and of particular importance as they constitute the first official guidance on cookies in Belgium. They can also be considered as "best practice" on the use of cookies pending the release of the final recommendations.

Cookies and consent

Under Belgian law, cookies are regulated by two sets of legal provisions. As cookies are considered to contain information related to identified or identifiable individuals (i.e. users of computers on which they are placed), they constitute personal data and are subject to the Belgian Data Protection Act (the "**DP Act**").

In addition, cookies are regulated by Article 129 of the Belgian e-Communications Act of 13 June 2005 (the "**e-Communications Act**"), which transposes Article 5(3) of the amended e-Privacy Directive into Belgian law. This requires users' prior consent to the use of cookies, unless the cookie is "strictly necessary" for the provision of a service explicitly requested by the user. To obtain consent, the user must be provided with clear and comprehensive information regarding the purposes of the cookie and the user's rights.

However, neither the DP Act nor the e-Communications Act explains how the information should be provided and how consent should be obtained.

Draft Recommendations

The draft recommendations of the Privacy Commission clarifies these issues with a number of guidelines:

> detailing the mandatory information to be provided to users, which is essentially the same as normally required under the DP Act;

> requiring the provision of this information in a user-friendly manner in a way making it accessible at any time on the relevant website;

> imposing the consent to be freely given (i.e. without negative consequences in case of refusal), specific (i.e. ideally given per type of cookie and not in general for all cookies) and informed (i.e. obtained after the provision of all relevant information);

> allowing implied consent stemming from certain positive actions by a website visitor, to the extent such actions establish the consent with sufficient certainty;

> allowing consent to remain valid for further cookies sent by the same provider, when installed for the same purposes; and

> imposing that cookies not be retained for longer than necessary to achieve their purpose.

Interestingly, the draft recommendation then goes on to list the various purposes for which cookies may be used and describes the steps required to ensure compliance with the DP Act and the e-Communications Act per type of cookie. The draft also provides examples of "technical cookies" falling under the exceptions of Article 129, as well as examples of compliant cookie policies.

Next steps

The consultation launched by the Privacy Commission ended in the summer. The Commission is due to release a final version of its recommendations in due course, taking into account the input collected during the consultation. So far, however, the Privacy Commission has not done so.

As a result, the draft recommendation remains the sole official guidance to date. Although some changes are expected in the final version, the draft recommendation can already be considered as a list of "best practices" to be taken into account when drafting cookie policies or assessing the compliance of their use.

By Tanguy Van Overstraeten and Guillaume Couneson, Brussels

France – Supreme Court reaffirms need for data protection notification

In October 2014, the French Supreme Court (*Cour de Cassation*) ruled that evidence from an email monitoring system was not admissible because that system had not been notified to the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*). This follows previous decisions by the Cour de Cassation and emphasises the need for companies to notify their data processing in order for it to be lawful.

Excessive personal use

The case arose after an employee was dismissed for excessive personal use of her corporate mailbox (Cass. Soc. 8 October 2014, n°13-14991). The email monitoring system showed that the employee had sent and received more than 600 personal emails within a month.

When the case reached the Court of Appeal, it decided that evidence from the email monitoring system was admissible because:

> the employer had informed his employees of the monitoring and the possible sanctions should the monitoring reveal excessive personal use;

> the evidence was limited to the date, sender, recipient, and matter of the emails, and did not include their content; and

> even if the data processing had not been notified to the CNIL at the time the information was collected, the employer had subsequently made a notification.

Supreme Court declares information inadmissible

However, the Cour de Cassation overturned the Court of Appeal's decision. The fact that the employees had been informed of the monitoring did not exempt the employer from notifying the processing to the CNIL. The email monitoring system had not been notified at the time when the data forming the evidence was collected and was therefore an unlawful source of evidence, which had to be discarded by the Court.

This is similar to a decision taken ten years ago in which the Cour de Cassation held that the refusal by the employee to use the badging system at the entrance and exit of a factory could not justify his dismissal since that processing had not been notified to the CNIL at the time of the dismissal (Cass. Soc. 6 April 2004, n°01-45227).

In both cases, the employer made a belated notification. This could have been seen as a means to remedy the earlier breach and to cooperate with the CNIL. However, it was not sufficient for the Cour de Cassation, which applied article 22 of the French data protection act (Loi Informatique et Libertés) strictly and required notification be filed prior to carrying out the processing.

The decision also follows the Cour de Cassation's decision which invalidated the sale of a customer database because the seller had failed to notify such processing to the CNIL (Cass. Com. 25 June 2013, n°12-17037).

These cases demonstrate the court's role in ensuring compliance with the Loi Informatique et Libertés by depriving data processing or transfer of data of legal effect. This is in addition to the role of the CNIL which can investigate a failure to notify and apply administrative sanctions and also has the potential to impose criminal prosecution, which is punishable by up to five years' imprisonment.

The General Data Protection Regulation

The latest decision by the Cour de Cassation confirms the strict approach of French courts towards filing requirements. This may seem awkward at a time when the EU proposals for a new General Data Protection Regulation intend to remove a lot of the existing formalities. However, pending the potential adoption of the Regulation, it remains crucial for companies to fully comply with their obligation to notify any data processing to the CNIL in advance.

By Alexandre Entraygues and Clotilde Chabre, Paris

Poland – Privacy amendments to encourage entrepreneurs

In November 2014, the Polish Parliament adopted the Act on Facilitating Economic Activity in order to encourage entrepreneurship. The relevant provisions of the Act come into force on 1 January 2015 and are bound to relax a range of laws including the Polish Act on the Protection of Personal Data.

Appointment of information security administrator to be voluntary

The Act on Facilitating Economic Activity (the "**Act**") applies to entrepreneurs, i.e. any natural or legal persons carrying out commercial activities in their own name.

The Act amends the Polish Act on the Protection of Personal Data so that the appointment of information security administrator by data controllers is no longer mandatory. However, the appointment of an information security administrator does provide some benefits for entrepreneurs (e.g. such as the notification exemption below). At the same time, the Act imposes new obligations on information security administrators, such as the requirement to undertake internal compliance audits when mandated by the Polish Data Protection Authority.

The Act introduces certain eligibility criteria to be met by a person appointed as an information security administrator – most importantly they must have adequate knowledge of the protection of personal data. To ensure sufficient independence and autonomy, the information security administrator must report directly into the director of the entity by whom s/he has been appointed.

Exemptions from registration

The Act also provides that companies which appoint an information security administrator will be exempt from the obligation to register their personal data filing systems if they notify the Polish Data Protection Authority of such an appointment. Entrepreneurs will also be relieved from the obligation to:

> keep their notification up to date in relation to changes made to their personal data filing systems; and

> notify hard copy personal data filing systems.

However, the information security administrator must himself maintain a register of personal data filing systems processed by a data controller. In addition, the exemptions set out above will not apply to personal data filing systems containing sensitive personal data (e.g. data concerning health or data related to convictions).

The Polish Data Protection Authority will keep a register of information security administrators.

Facilitation of data transfers outside the EEA

The Act also relaxes some of the rules on the transfer personal data outside the EEA. Currently, the prior approval by the Polish Data Protection Authority

is needed in a vast array of circumstances. Once the amendments provided for in the Act enter into force, approval will not be necessary for transfers based on model contractual clauses or approved by the Polish Data Protection Authority so-called Binding Corporate Rules.

By Ewa Kurowska-Tober, Warsaw

Russia – New data localisation law: Current state of play

Russia recently amended its laws to require the personal data of Russian citizens, including those collected on the Internet, to be stored in databases in Russia. These amendments have caused considerable concern following suggestions by the Russian President administration that duplicates of databases containing the personal data of Russian citizens are not allowed outside of Russia. There has also been a proposal to bring the implementation date forward from September 2016 to January 2015, though this proposal appears to have stalled. We consider the current state of play.

What are the new data localisation requirements?

In July 2014, the President of the Russian Federation signed Federal Law "On amendments to certain legislative acts of the Russian Federation for clarification of personal data processing information and telecommunication networks" (No.242-FZ) (the "**data localisation law**").

The data localisation law amends the existing Russian Federal Law "On Personal Data" (No.152-FZ) and two other laws. It applies to all data operators collecting personal data about Russian citizens through electronic communications, including the Internet. Operators recording that data must ensure the storage of that data takes place in databases located in the territory of the Russian Federation. There are certain limited exceptions where the processing is:

> carried out pursuant to Russian laws or an international treaty;

> necessary for the administration of justice or enforcement proceedings;

> necessary for the execution of duties by the Russian state and municipal bodies; or

> for journalistic, media, scientific, literary or creative purposes.

The law was enacted in a very short time to better protect the personal data of Russian citizens, particularly in light of recent political developments.

Do they prevent data being exported out of Russia?

The data localisation law does not contain any explicit restriction on the transfer of personal data outside of Russia; it simply requires that data are kept in Russia.

However, in September 2014, the administration of the Russian President circulated a commentary on the data localisation law that suggested it should be applied restrictively and that the processing of personal data about Russian citizens should **only** take place in Russia and that data could not be duplicated in other countries. The commentary also suggested the data localisation law would also apply to personal data collected before the law comes into effect.

This commentary is non-binding and subsequent comments do not appear to support this restrictive approach. For example, in November 2014, the head of Russia's data protection authority (*Roskomnadzor*) suggested that

transfers of personal data outside of Russia should instead be subject to the existing provisions of the Federal Law "On Personal Data" (No.152-FZ). The existing law permits the transfer of personal data outside of Russia if certain conditions are met such as the transfer being subject to the prior written consent of the data subject and the transfer being to a country that is party to the Council of Europe Convention on Personal Data.

Who does the law apply to?

The data localisation law applies to all data operators. This is a concept that combines aspects of a data controller and data processor under European data protection law.

It therefore catches all entities in Russia collecting personal data through electronic communications (including subsidiaries or branches of foreign companies) regardless of the sector the data operator operates in. It is not clear if the law is also intended to apply to foreign companies without a local presence in Russia, though there may be further clarification in due course.

Other provisions - A new right to be forgotten

The data localisation law may also help to create a "right to be forgotten" by amending the Federal Law "On Information, Informational Technology and Protection of Information" (No. 149-FZ).

Initially a "right to be forgotten" is set out in the existing Russian Federal Law "On Personal Data" (No.152-FZ) in accordance with which a data subject has the right to require that the operator deletes personal data which are processed in breach of the law. But this provision needs a practical implementation mechanism which will be provided by the data localisation law.

Pursuant to a court order, a Russian citizen can approach the Roskomnadzor with an application requesting that their personal data should be deleted from a website. The Roskomnadzor will then contact the hosting provider for the relevant website and ask it to remove that content.

If the hosting provider does not remove the content, the Roskomnadzor can add it to a "Register of personal data violators" and ask telecoms operators to block access to that hosting provider's website in the future.

When will these changes come into effect?

The data localisation law is supposed to enter into force on 1 September 2016.

There is a draft law in the Duma to move the implementation date forward to 1 January 2015. However, this amendment appears to have stalled in the face of significant concerns about whether compliance by this deadline is practical. It is possible that there will be a further attempt to move the deadline forward, but it seems unlikely that the implementation date would be until mid-2015 at the earliest.

By Galina Tereschenko, Moscow

Singapore – MAS consultation on outsourcing arrangements

In September 2014, the Monetary Authority of Singapore issued a consultation on new standards and guidelines to ensure that financial institutions have sound risk management practices for outsourcing arrangements, which will include cloud services. We consider the impact of these proposals.

Consultation and binding force

The consultation is part of the Monetary Authority of Singapore's ("**MAS**") efforts to raise the standards of financial institutions' risk management practices. It is proposing to:

> issue a new notice on outsourcing management standards (the "**Notice**"); and

> revise the existing Guidelines on Outsourcing (last updated on 1 July 2005) (the "**Guidelines**").

The introduction of the Notice would be significant as it would be legally binding. This is unlike the current regulatory regime (i.e. the Guidelines) which provides for "best practice" standards.

The risks to financial institutions for non-compliance will therefore be greater, including the imposition of criminal sanctions. The public consultation has now closed and there has been no indication by the MAS as to if and when the revised Guidelines and Notice will come into force.

Some of the more significant changes proposed under the new Notice are set out below. The revisions to the Guidelines provide financial institutions with guidance to ensure compliance with the obligations under the Notice.

Minimum standard for "material outsourcing arrangements"

The Notice imposes minimum standards for financial institutions in the management of all its "material outsourcing arrangements". This is defined as an outsourcing arrangement which:

> has the potential to materially impact an institution's business operations, reputation or profitability or adversely affect any institution's ability to manage risk and comply with applicable laws, in the event of a service failure or security breach; or

> involves customer information and, in the event of any unauthorised access or disclosure, loss or theft of customer information, may materially impact an institution's customers.

The minimum standards include establishing adequate risk management frameworks, systems, policies and processes to control and monitor the material outsourcing arrangements, and maintaining a central register of all material outsourcing arrangements.

Due diligence on service providers

The Notice obliges financial institutions to conduct due diligence on service providers in considering, renegotiating or renewing any material outsourcing arrangements. This must be documented and re-performed on an annual basis.

The due diligence should include assessing the service provider's corporate governance, risk management, security controls, audit, and financial strength and resources.

Audit rights

Under the Notice, service providers must not only give financial institutions the right to conduct audits, but must also allow the MAS to conduct audits where necessary or expedient.

A financial institution must also indemnify the MAS for any losses to the service provider arising out of any action taken to access and inspect the service provider.

Protection of customer data

Where an outsourcing arrangement involves disclosure of customer data to the service provider, a financial institution is required under the Notice to protect that data, including:

> ensuring that the service provider isolates and clearly identifies the customer data belonging to the financial institution;

> engaging service providers that operate in jurisdictions which generally uphold confidentiality provisions and agreements;

> the inclusion of confidentiality provisions which address access to the information by the employees of the service provider, and restrictions against disclosure of such information; and

> imposing notification requirements on the service provider to notify the financial institution in the event of disclosure of customer information to third parties.

Termination and exit obligations

Certain termination provisions must be included in outsourcing arrangements, including the right for a financial institution to terminate the agreement in the event that the service provider undergoes a change of ownership, becomes insolvent or there has been a "*deterioration in the ability of the service provider to perform the service as contracted*".

There are also notification obligations imposed on the financial institution to keep the MAS informed of such events.

Who is subject to these rules?

The Notice and Guidelines will apply to "financial institutions", as defined in section 27A of the Monetary Authority of Singapore Act (Cap. 186) (the

"**Act**"). This definition is wide and includes not only all institutions approved as a financial institution under the Act, but extends to:

> any licensed money-changer or remitter, and any insurance intermediary registered or regulated under the Insurance Act (Cap. 142);

> any licensed financial adviser under the Financial Advisers Act (Cap. 110);

> any licensed trust company under the Trust Companies Act (Cap. 336);

> any holder of a stored value facility under the Payment Systems (Oversight) Act (Cap. 222A);

> any trustee-manager of a business trust that is registered under the Business Trusts Act (Cap. 31A); and

> any securities exchange, futures exchange, recognised market operator, licensed trade repository, licensed foreign trade repository, approved clearing house or recognised clearing house under the Securities and Futures Act (Cap. 289).

Impact on cloud and existing agreements

The proposed changes have potentially far-reaching consequences on the outsourcing portfolio of both financial institutions and service providers alike.

Some of these obligations (such as the audit requirements) are extremely intrusive. This is particularly the case for some commodity cloud providers who do not generally provide audit rights and instead ask customers to rely on their own security audits and certification. These proposals may therefore exclude some of such cloud providers from the market for financial services outsourcing in Singapore.

Should the Notice be issued, all affected parties will have a six month transitional period from the date of issuance to ensure compliance before the Notice comes into effect. Existing contracts will not need to be updated in accordance with the obligations, but any outsourcing agreements entered into or renewed on or after this six month transitional period will need to comply with the applicable provisions of the Notice.

By Adrian Fisher and Joel Cheang,Singapore

UK – New private copying, quotation and parody copyright exceptions

Three new exceptions to copyright infringement entered into force in the UK on 1 October 2014: (i) private copying; (ii) quotation; and (iii) caricature, parody and pastiche. These new exceptions, which expand the ways in which copyright material can be used in the UK, mark a further step in implementing the reforms recommended in the 2011 Hargreaves Report to promote innovation and drive economic growth. Most of these changes bring the law up to date with widespread common practice. However the new parody exception may give marketing teams additional scope for creativity.

Private copying

This new exception, effected by way of a new section 28B Copyright, Designs and Patents Act 1988 ("**CDPA**"), permits individuals to make personal copies of any copyright works (other than computer programs) for private, non-commercial use, provided the original was acquired lawfully and permanently. This change allows copying for purposes such as format shifting (e.g. digital storage of music purchased on CDs), back-up, and storage on a private cloud, provided the copier owns the original. However, an individual cannot transfer a personal copy to anyone else, except on a private and temporary basis, or give away the original whilst retaining any personal copies.

Comment - The Information Society Directive (2001/29/EC) (Article 5(2)(b)) permits Member States to implement this exception, on condition that rights holders receive "fair compensation". In other EU countries, similar exceptions are supported by levies on copying equipment, but no equivalent system is proposed in the UK. Given that this fairly limited exception brings the law up to date with what consumers are doing already, the UK Government may have considered that this widely accepted practice is already priced into the purchase of copyright works.

Quotation

The new quotation exception extends the existing fair dealing exceptions for "criticism or review" at section 30 CDPA. It allows quotation ("whether for criticism, review or otherwise"), provided that:

> it is fair dealing;

> there is sufficient acknowledgement;

> it uses no more than is required; and

> the original work has been made available to the public.

Comment - There is no statutory definition of "fair dealing", but the English courts have established that it is an objective test: how would a fair-minded and honest person have dealt with the work? Relevant factors include the amount of the copyright work that has been used and whether that use affects the market for the original, e.g. by competing with it.

The UK Intellectual Property Office's guidance suggests that short quotations of a copyright work in an academic paper or history book are permitted under this exception, but long extracts are not. Interestingly, it also suggests that, in exceptional circumstances, quoting a photograph will be allowed, provided the use does not conflict with the copyright owner's normal exploitation of it.

Parody

Use of copyright material is now permitted for the purpose of "caricature, parody or pastiche", under a new section 30A CDPA. Again, any such use will have to be "fair dealing" to benefit from the exception.

Comment - While the legislation does not attempt to further define caricature, parody or pastiche, the CJEU has very recently provided some helpful guidance as to the meaning of "parody". In *Deckmyn v Vandersteen* (C-201/13), the CJEU ruled that the only essential characteristics of a parody are:

> to evoke an existing work while being noticeably different from it; and

> to constitute an expression of humour or mockery.

The CJEU also said that the purpose of all exceptions to copyright infringement is to strike a fair balance between the interests of rights holders and those who want to use copyright material. Further, if a parody conveys a discriminatory message, the holders of rights in the parodied work may have a legitimate interest in ensuring that their work is not associated with that message. As such, it will be for the national courts to perform the necessary balancing act between copyright infringement and freedom of expression in each case.

The treatment of parodies in the UK is now more similar to their treatment under US law, where parodies may be permitted under the general "fair use" doctrine.

This new exception is likely to be welcomed by many (including parodists such as Cassetteboy, a duo known for their online "mash-up" parodies, and those wishing to use video parody, via social media or otherwise). However, anyone wishing to take advantage of this exception should remember that it has no impact on either the laws of defamation or the author's moral right to object to derogatory treatment of their work.

By Kathy Berry, London

UK – Supreme Court considers remedial and irremediable breaches

The Supreme Court's decision in *Telchadder v Wickland* [2014] UKSC 57 provides a useful analysis of when a breach of contract is capable of remedy and how you can remedy breach of a negative obligation. We consider its application to commercial contracts.

Mobile homes

The Mobile Homes Act 1983 was introduced to protect permanent occupiers of mobile homes from unethical site operators. There are nearly 85,000 such households in the UK and a substantial proportion of residents are elderly.

The protection includes implying the following contractual term into their occupation agreement:

> "*The owner shall be entitled to terminate the agreement forthwith if, on the application of the owner, the appropriate judicial body –*
>
> *(a) is satisfied that the occupier has breached a term of the agreement and, after service of a notice to remedy the breach, has not complied with the notice within a reasonable time; and*
>
> *(b) considers it reasonable for the agreement to be terminated*"

Mr Telchadder occupied a mobile home on Meadowview Park, Little Clacton. His occupation agreement was subject to this implied contractual term. Reflecting the fact that residents of mobile homes live in close proximity to each other, his occupation agreement also obliged him not to annoy or disturb other residents and not to carry offensive weapons.

Nasty surprises

Problems arose when Mr Telchadder, described by Lord Wilson as "eccentric", startled another resident by jumping out from behind a tree wearing camouflage netting. The site owner, Wickland Holdings Limited, sent a notice in August 2006 warning it would seek to terminate his agreement if he repeated this behaviour.

Things remained calm for a further three years until 2009 when Mr Telchadder's behaviour deteriorated. He harassed and intimidated other residents, including telling another resident: "*I'll f*&king kill you as well – I've got shotguns and air rifles*". The police were called, though did not press charges, and the local magistrate issued a restraining order against him.

Wickland sought to terminate his occupation agreement on the basis of the notice served in August 2006. It did not attempt to terminate on the basis these new breaches were serious and irremediable. The Southend County Court held that Wickland was entitled to terminate the occupation agreement. This decision was upheld by the Court of Appeal, so Mr Telchadder appealed to the Supreme Court.

It considered three questions:

> was jumping out from behind a tree wearing camouflage netting in 2006 a breach capable of remedy?

> if it was capable of remedy, how could Mr Telchadder remedy the breach "within a reasonable time"?

> if the breach was not capable of remedy, was Wickland still required to send a notice requiring remedy?

Breaches capable of remedy

Breach of a positive obligation is most obviously capable of remedy. For example, if Mr Telchadder had failed to pay his pitch fee or pay to insure his mobile home, he could ordinarily remedy it by making belated payment. Ordinarily…but not always. For example, if the mobile home burnt down prior to the insurance being reinstated, the breach would become irremediable.

The difficulty here is that jumping out on another resident, Miss Puncher, and startling her was a breach of a negative obligation not to annoy or disturb other residents. Taken literally, this type of breach is always irremediable. There is nothing Mr Telchadder could do to "unstartle" Miss Puncher.

The Supreme Court decided that the correct test is to determine if the mischief caused by the breach of negative obligation can be redressed. In this case, the startling of Miss Puncher was not particularly grave and could be redressed by Mr Telchadder avoiding further anti-social behaviour.

However, the ability of a party to remedy a breach of a negative obligation does depend on the facts. If Mr Telchadder committed a more serious breach, for example by physically attacking Miss Puncher, that breach may not have been capable of remedy.

Remedy "within a reasonable time"

The next question was how Mr Telchadder could comply with the notice "within a reasonable time". Again, this requirement fits better with a positive obligation such as making payment.

In relation to a negative obligation, the majority of the Court decided the word "within" must be read as "for" – i.e. Mr Telchadder would have to avoid further anti-social behaviour "for" a reasonable time.

The Court did not specify what a "reasonable time" would be in this case but it was certainly less than three years. Accordingly, the 2006 notice had ceased to have any effect. It could not be used to terminate Mr Telchadder's occupation agreement in 2009.

The decision has a number of interesting implications. For example, the dissenting judgment by Lord Carnwarth and Lord Reed suggested this could lead to a "cat and mouse" game in which residents continually breach their agreement and are served with a notice; comply for a reasonable period; and thereupon commit further breaches. However, Lord Wilson described this concern as "unreal" and, in any event, the "reasonable time" to comply with a subsequent breach would be much longer than for the first.

More difficult is the application of these principles to commercial agreements which expressly set out the time for remedy. For example, an agreement might allow a party to terminate where the other:

> "*commits a material breach of its obligations and (where the breach is capable of being remedied) that breach has not been remedied within 30 days after receipt of notice*".

The problem here is that the party breaching their negative obligation can simply desist from further breaches for 30 days after which the slate is wiped clean. They would then be free to start the cycle again by committing further breaches and desisting for a further 30-day period. In practice, one assumes this is both unlikely and, as suggested by Lord Toulson, those initially remedial breaches may rapidly become irremediable.

Is a notice to remedy required if the breach is irremediable?

One curious aspect of the Mobile Homes Act 1983 is that the implied term does not address irremediable breaches. On a literal reading, Wickland must serve a notice regardless of the type of breach. The majority decided this would be "nonsensical". There would be no purpose in serving a notice to remedy a breach which is incapable of remedy.

A note of warning

The Supreme Court's decision provides a useful insight into the operation of termination clauses and the ability of parties to remedy breaches of contract.

The decision is likely to be of wider application. However, it is important to note the context in which it was given. The implied terms under the Mobile Homes Act 1983 were designed to protect a vulnerable section of the pubic, and take an unusual form. Even where an unremedied or irremediable breach takes place, the site owner can only terminate where the court considers it "reasonable" to do so. This is a very different position to most commercial contracts and give ample grounds for the Courts to distinguish this case should they feel it necessary.

Telchadder v Wickland Holdings Ltd [2014] UKSC 57 is available here.

By Peter Church, London

Author: Peter Church

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

A19096415/0.5a/08 Dec 2014