Linklaters

March 2011

Technology Media and Telecommunications.

Data Protection and Freedom of Information

EU - Commission outlines latest plans for Directive reform

On the occasion of a meeting organised by the Privacy Platform, led by MEP Sophie in 't Veld on 16 March 2011, the EU Commission Vice-President Viviane Reding set out her latest plans for the reform of the data protection legal framework. The changes mainly relate to the online world and, in particular, social networking and photo sharing sites, but provide some guidance about the Commission's wider thinking.

Four pillars of reform

The plans are based around four pillars.

> *Le droit à l'oubli* – Although the current legislation already contains rules in that respect (including the right for deletion and the obligation not to retain data for longer than necessary), the proposed "right to be forgotten" has undoubtedly generated a lot of attention. The Commission intends to draw up a comprehensive set of rules to deal with privacy risks online including an explicit right for users to withdraw consent to the processing of their personal data and explicit obligation on data controllers to prove they need to retain data. The issue is therefore to focus the burden of proof onto data controllers.

> *Transparency* - Already a fundamental part of data protection legislation, the Commission intends to extend these rights to allow individuals to control the use of their data. This is likely to require the provision of additional information about data protection rights, how third parties might use their data, the details of the relevant data protection authority and the risks faced by providing their data. This information must also be provided in a clear and intelligible way - easy to find, easy to understand.

> *Privacy by default* - The Commission considers many existing privacy settings are not sufficient to demonstrate consent as they require considerable effort to use. These settings should instead be pre-set to prevent any unfair, unexpected or unreasonable processing of data.

Contents

> *Extra-territorial effect* - Perhaps the most interesting suggestion is that data protection laws should be given extra-territorial effect and apply to any processing of data related to EU citizens and non-EU citizens living in the European Union where the data controller is targeting those citizens. How the data protection authorities will enforce these rules is not expressly set out.

Does this apply beyond The Social Network?

While these four pillars initially look attractive they do raise a number of questions, particularly if these principles are applied outside of the social networking sphere. For example, it seems sensible for the right to be forgotten to apply to information an individual posts about themselves. If individuals put the information up, they should be able to take it down. However, it raises more difficult issues about censorship and freedom of speech when the information is posted by a third party. Should the individual's data protection rights always trump the third party's rights to freedom of speech or is this a value based judgment? If it is a value based judgment then who makes that decision and on which basis?

The position becomes even more difficult outside the social networking sphere. Do individuals have a right to be forgotten in newspaper archives or credit reference agencies? Given the current framework already contains an obligation not to retain personal data any longer than necessary, there seems little justification for any further expansion. Equally, the suggestion that individuals should always have the right to withdraw consent raises wider issues and would limit the circumstances in which data controllers will want to rely on consent as a legal ground for processing personal data.

The proposed additional rules on transparency also need careful consideration. Many individuals do not read privacy policies so obligations to include additional information could be counter-productive. Good privacy policies should be short and to the point so there is a clear tension in mandating the disclosure of additional information. The key issue is also educational, especially for heavy online users such as children and teenagers, who should be informed by the relevant public authorities (e.g. in schools) in an intelligible manner about the best practices over the Internet, in the same way as car drivers need to take exams before they get their licence and are on the streets.

The Commission will, no doubt, expect some resistance to these proposals but may well feel encouraged by the recent Communication by the European Council and the entrenchment of data protection rights in the EU Charter of Fundamental Rights. There is certainly much to suggest a more muscular data protection framework is on the way.

Viviane Reding's speech is available here

By Tanguy Van Overstraeten, Brussels, and Peter Church, London

Belgium - Mobile mapping recommendation: Google Street View's to do list?

In a recent Recommendation, the Belgian data protection authority (the "**Privacy Commission**") has reviewed issues associated with "mobile mapping" and imposed a number of requirements on operators providing such services including conducting a privacy assessment and providing it to the Privacy Commission six weeks prior to the launch of the service. The Recommendation demonstrates the increasing importance of the principle of privacy by design.

Mobile mapping and privacy issues

The Recommendation applies to mobile mapping which it defines as "a technology by which a vehicle equipped with cameras and/or a scanner can digitally record data about a specific road, including by the taking of 360° pictures". It does not refer to any companies by name although Google's Street View is an obvious example. The Privacy Commission also provides examples of the potential uses of mobile mapping, such as public road safety, tourism or navigation.

In the Privacy Commission's opinion, this particular technology raises privacy issues because its relies on the use of cameras in public places. The captured images may contain representations of individuals or property that can be recognised and therefore constitute personal data and even sensitive personal data (e.g. if someone is captured exiting a particular medical practice). As mobile mapping involves the processing of such personal data, the Belgian data protection law applies, which raises a number of interesting considerations.

Application of data privacy laws

A first consideration is that it is impossible to determine whether an image is or is not sensitive data. This derives from the context. As such, the Privacy Commission does not offer any specific solution to this issue.

The Privacy Commission also insists on the importance of specifying the purposes for mobile mapping applications. The determination of the purpose should be made at an early stage, as that purpose must be notified to the Privacy Commission prior to the start of any personal data processing. Moreover, any further processing must remain compatible with that original purpose with the effect that data collected for a particular mobile mapping application may not be used for other related applications.

The Privacy Commission also reiterates that processing of personal data is only lawful if it can rely on a legal basis set out in Belgian data protection law. The Privacy Commission recognises that it is impracticable to obtain consent from the data subjects, so the data controller will have to rely mostly on the "legitimate interest of the data controller" legal ground.

Accordingly, the Recommendation makes it clear that the level of privacy protection will depend on the purpose of the mobile mapping. For example, the level of protection for a regular 2D map with no image of persons or

properties will be lower than for a Street View like application. The Privacy Commission explicitly refers to the concept of privacy by design emphasising that it expects the data controller to "think before it acts". In particular, taking into account that mobile mapping applications are not designed to process personal data (the processing thereof being more of a by-product of such activity), the Privacy Commission recommends that such processing should be avoided as much as possible by using appropriate technical measures (e.g. by automatic blurring, etc.).

The Privacy Commission also considers the data controller's obligation to inform data subjects about the processing of their data and suggests a number of pragmatic solutions such as publishing information in the local press and online, using the mobile mapping vehicle itself to inform the public, training the operator of the camera to reply to questions from data subjects and providing him with an information notice he could hand out to the public.

Privacy assessment

The conclusion to the Recommendation insists that a privacy assessment should take place prior to the start of the mobile mapping processing operations. Moreover, once the application is up and running, data controllers should continue monitoring any potential privacy aspects in the light of new technological developments. In this respect, the Privacy Commission requires data controllers to inform the Privacy Commission before launching such a service and make their privacy assessment available to the Privacy Commission at the latest six weeks prior to that launch.

By Guillaume Couneson and Tanguy Van Overstraeten, Brussels

Denmark - The Cloud is brought down to earth

There is an inherent tension between the delivery of cloud-based computing services and data protection laws. How can an organisation allow personal information to travel freely and seamlessly from server to server around the world whilst still ensuring it is subject to an adequate level of protection? How can that organisation ensure the security of this information if it doesn't know where it is or even who holds it?

A recent ruling by the Danish Data Protection Agency (*Datatilsynet*) provides an example of the problems that can arise in practice and the regulatory hurdles facing the cloud computing industry.

Odense Municipality

The Danish Odense Municipality asked for an advance opinion from the Datatilsynet about its proposed use of the Google Apps online office suite. This suite of products was to be used within schools and would, amongst other things, process sensitive personal data about health, social problems and other private matters about pupils.

As a public body, the Municipality is subject to not only the general security obligations in the Danish data protection act but also the more stringent security requirements set out in the Danish

Executive Order on security measures for the protection of personal data processed by the public administration.

The Datatilsynet undertook a review of the proposed use of Google Apps. Despite its generally positive view of new technologies and cloud computing, the Datatilsynet concluded that it was not appropriate to use Google Apps to process confidential and sensitive data about pupils. There were five main reasons for this conclusion.

Inadequate terms and conditions

The Google Apps suite was to be provided by Google Ireland Limited as data processor for the Municipality. Under the Danish data protection act, the Municipality must have a written contract with Google obliging it to only act on the Municipality's instructions and to take appropriate technical and organisational security measures. These obligations are reflected in Sections 1.4 and 1.5 of the terms offered to the Municipality (though interestingly, these don't appear to reflect the current terms and conditions offered by Google):

> "*1.4 … Customer therefore instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same…*
>
> *1.5 …For the purposes of this Agreement … the parties agree that Customer shall be the data controller and Google shall be a data processor. Google shall take and implement appropriate technical and organisational measures to protect such personal data against*

accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access."

The Datatilsynet decided that Section 1.4 was insufficient as it merely instructed Google to process data in accordance with its own policies, which it might choose to vary unilaterally. It considered that this obligation was "*devoid of content in purely material terms*".

The security obligations were unacceptable. Section 1.5 satisfies the general obligation to ensure the data is kept secure. However, it does not satisfy the additional requirement arising under the Executive Order to flow the obligations in that Order down to Google. The use of generic security obligations in Section 1.5 of the terms and conditions was therefore insufficient.

Inability to ensure security

Perhaps more fundamentally, the Danish data protection act requires the Municipality to ensure that the data processor complies with its security obligations in practice, which is likely to require some sort of audit or inspection of that processor's facilities.

This is a problem with a cloud-based solution as information is likely to flow freely between data centres. In this case, the Datatilsynet concluded that the Municipality was unaware of where its data was physically located and, on that basis, it questioned whether the Municipality would "*be able to actively ensure that the required security measures are upheld at the data centres*". This was the case even though the Google Apps were subject to a SAS 70 Type II audit, meaning that independent auditors have controlled and verified Google security practices.

Specific security requirements in the Executive Order

The Municipality was also unable to demonstrate that the Google Apps service complied with a number of specific security obligations in the Executive Order. These include:

> inadequate provisions to delete personal data. While Google had strict procedures in place to overwrite and/or dispose of old hard drives, this was not sufficient to meet the stricter technical requirements of the Executive Order which require data to be overwritten multiple times in accordance with a recognised standard, e.g. DOD 5220.22-M;

> insufficient evidence that data is encrypted when transmitted between Google's data centres. This was a particular issue given that sensitive personal data would be transmitted as part of this process;

> inadequate monitoring and control of unsuccessful login attempts. There was no evidence that unsuccessful login attempts (which may be evidence of an attempt to hack the system) were logged or that access would be blocked following repeated failures to access the system; and

> inadequate usage/audit logs. It was unclear how the Municipality would comply with the requirements in the Executive Order to keep usage/audit logs on the processing of personal data.

Risk assessment

In light of these conclusions, it is unsurprising that the Datatilsynet also concluded that the Municipality had failed to carry out a proper risk assessment, as required in the Executive Order. Of particular concern was the fact Google did not encrypt data "at rest" on its servers. In particular, Google's position is:

> "*Encryption is a commonly accepted way to protect data and Google regularly considers encryption for each of its applications. However, while encryption secures data, it also negatively impacts the speed of search and collaboration. For this reason, Google consciously decided not to encrypt Google Apps data at rest on its systems. The data is, however, 'obfuscated' or masked using proprietary algorithms.*"

The Datatilsynet suggested that a better approach would be to adopt the approach outlined by ENISA in its publication, *Cloud computing - Benefits, risks and recommendations for information security*. This contains a comprehensive list of risks posed by cloud computing services and a detailed list of security questions to ask a cloud computing provider.

Transfers outside the EEA

The Datatilsynet final concern related to international transfers of personal data. The Google Apps services was said to be provided from Google data centres in the EEA and the US. The data centres in the EEA do not involve the transfer of personal data to a third country and Google has joined the US Safe Habor. This should be sufficient to meet any data protection concerns. However, the Datatilsynet was still concerned that transfers to other third counties might take place and, if so, may not be justified.

Dark clouds ahead?

The Datatilsynet's opinion provides a useful practical example of the data protection issues that arise from the use of cloud computing and a warning that European data protection regulators may scrutinise such offerings in detail. Google and other companies offering cloud computing solutions will, no doubt, be considering the implications of this decision. There are a range of options available to them, including to:

> adopt a "gold standard" approach and seek to comply with all data privacy laws across the EU. This highest common denominator approach would be difficult and expensive given the stringent requirements imposed by some European Member States, such as the Spanish security regulations which *inter alia* require the encryption of sensitive personal data. This approach would also have to be supported by a thorough audit programme to provide comfort to data controllers that their data would be kept secure in practice;

> adopt a jurisdiction by jurisdiction approach and provide greater protection to some jurisdictions. For example, Danish public authorities could be provided with an enhanced package of protections to allow them to comply with the Danish Executive Order. However, this is the antithesis of a commoditised utility computing model and the additional costs of complying with multiple national standards may make it more expensive than adopting a gold standard; or

> maintain their current offering and leave it up to their customers to determine if its offering complies with local data protection laws.

Google appears to be adopting the final option. One of its security and privacy FAQs is "*Is my organization compliant with the European Commission Directive on Data Protection if we use Google Apps?*" The answer refers to Google US Safe Harbor registration and then states "*Generally, an organization must decide whether its use of Google Apps is compliant with any regulations it may be subject to.*"

The Datatilsynet opinion is available here

By Emma Linnér, Stockholm

France - CNIL seeks to boost cloud computing

In a decision in January 2011 (published on 16 February 2011), the French Data Protection Authority (*CNIL*) relaxed the data protection obligations imposed on non-EEA data controllers using data processors in France.

Scope of the decision

The current rules on applicable law mean that when a data controller outside of the EEA transfers personal data to a data processor in France, it makes use of "means" in France and therefore will be subject to the French Data Protection Act.

The CNIL has decided that the data protection rules should be relaxed in such a situation, as such processing only entails minimum risks for data subjects whose data have initially been collected outside of the EEA. The relaxed rules apply to personal data relating to payroll and employee management and client and prospect management which are transferred by a data controller based outside of the EEA to France for processing and then sent back to the data controller.

Lifted obligations

The following obligations will no longer apply:

> *Notification* – The CNIL has decided to exempt the above processing operations from filing any prior notifications.

> *Transfer authorisation* – There is no need to obtain a transfer authorisation from the CNIL for the above processing operations, as the CNIL considers the transfer back to the controller outside of the EEA to be necessary for the performance of a contract between the data controller and the data subject or in its interest.

> *Fair processing information* – The CNIL has also considered that employees and clients need not be informed about the processing of their data in France where the provision of such information would require disproportionate effort.

Remaining obligations

However, other obligations of the French Data Protection Act remain applicable, including:

> *Security* – The agreement between the data controller and the French data processor must include provisions regarding the protection of security and confidentiality of the data at stake as well as a provision confirming that the data processor must only act upon the instructions of the data controller. An access control policy and a security policy protecting against data disclosure must also be in place.

> *Designation of a French representative* -The non-EEA data controller must still designate a French representative that will replace him in the performance of its obligations under the French Data Protection Act. In

addition, the non-EEAdata controller remains liable for any breach of the French Data Protection Act.

This recent decision from the CNIL should help the development of French-based cloud computing services, though arguably the benefit may be limited as it may be difficult to confirm that all of the data processed using that cloud infrastructure fall within the purposes set out above. The decision is also very interesting as it gives a flavour of changes the CNIL is envisaging in the context of the current review of Data Protection Directive.

The decision is available here.

By Sylvie Rousseau and Grégory Sroussi, Paris

France - Amendments to the scope of whistleblowing hotlines

In October 2010, the CNIL modified its authorisation regime for whistleblowing hotlines to comply with a decision issued by the French Court of Cassation in 2009 (see *TMT News: Courts silence "illegal" whistleblowing schemes*). The effect of these modifications is discussed briefly below.

Authorisation of whistleblowing hotlines

In France, a whistleblowing hotline must be authorised by either:

> obtaining specific prior approval from the CNIL following the filing of a formal application for approval; or

> self-certifying that the whistleblowing hotline complies with the pre-defined set of rules recognised by the CNIL (authorisation AU-004).

Modifications

The CNIL's recent decision modifies the self-certified scheme in two ways.

> *Vital interest of a company cannot be relied upon* - The CNIL has confirmed that reporting under self-certified whistleblowing hotlines is limited and cannot be extended beyond the scope of the specifically authorised scope, even in situations where reporting would be in the vital interest of the data controller.

> *Two additions to the authorised reporting scope* - The new rules expand the scope of the self-certified hotlines by allowing reporting: (a) to prevent anti-competitive practices; and (b) where needed to comply with the Japanese Financial Instruments and Exchange Act. This is in addition to the original scope, which allows reports on finance, accounting, banking, corruption and compliance with Section 301(4) of the Sarbanes-Oxley Act.

There is a six-month grace period from the publication of the new rules (i.e. until 8 May 2010) to amend any existing company hotline, if necessary.

The new authorisation regime is available here.

By Sylvie Rousseau and Grégory Sroussi, Paris

France - CNIL issues guidelines on data security and offshoring

The CNIL has recently issued two key guidelines on data security and offshoring for companies processing personal data.

Data security guidelines

In October 2010, the CNIL issued a Personal Data Security Guide addressed to those using information technology systems (including developers and system administrators). It is intended to assist them to evaluate the level of security offered by those systems and provide guidelines on the measures to be adopted in order to protect personal data.

The guide is a user-friendly risk management guide, composed of 17 sections covering issues such as user authentication, the use of encryption and safe means of exchanging data with other organisations. Each of section structured in three key parts: “elementary precautions”, “things not to do” and “how to learn more”.

Offshoring guidelines

In October 2011, the CNIL also issued a set of guidelines to assist data controllers to transfer data in a compliant manner in the context of outsourcing to non-EU countries. The guidance recognises that it is important to first identify the capacity in which the parties process data. The following criteria have been identified by the CNIL as helping to distinguish between the role of controller and processor:

> *Instruction level* - the level of prior instructions provided by the customer;

> *Control level* - the extent to which the customer can control the services and the processor’s use of the data;

> *Transparency* - the level of transparency of the customer with respect to the provision of services. In particular, does the supplier present itself under its name or its customer’s name? Can the supplier re-use the data for its own purposes?

> *Expertise* - the level of expertise of the supplier has over the means used to conduct the processing.

The guidance also reminds data controllers that they have a responsibility to notify the CNIL of data processing activities (including transfers). Various data transfer scenarios are envisaged by the CNIL and helpful guidelines are provided on the set of standard contractual clauses to be used in each relevant situation.

Finally, the CNIL also supported the use of Binding Corporate Rules in the event of intra-group data transfers. Indeed, the CNIL promotes the implementation of such BCRs in all major French companies. In order to facilitate the adoption of BCRs, the CNIL has established “BCR Clubs”, on a sector basis, designed to help companies drafting BCRs in their sector of

activity. These clubs currently cover aeronautic, banking and insurance, information technology, law firms and retail.

The offshoring guidelines are also helpful in that they extend the scope of some of the notification exemptions and simplify the data transfer authorisation process.

The CNIL's security guidance is available here and its offshoring guidance is available here.

By Sylvie Rousseau and Grégory Sroussi, Paris

Media & Telecoms

Belgium - Additional access obligations in the broadcasting market

In December 2010, the Belgian Institute for Postal services and Telecommunications (*BIPT*) and the broadcasting regulators issued draft decisions imposing access obligations on the main cable operators in Belgium and triple play obligations on the incumbent, Belgacom.

Access obligations on cable operators

The BIPT and the three broadcasting regulators, the CSA, Medienrat and the VRM, respectively competent for the French-speaking, German-speaking and Flemish communities, issued four draft decrees applicable to the cable broadcasting markets in Belgium. Due to the geographic segmentation of cable broadcasting, the relevant markets are limited to the zones where the incumbent cable operators (i.e. Brutélé, Tecteo, Telenet, Numéricable and A.I.E.S.H.) are active.

The four draft decrees oblige cable operators to provide any alternative operator so requesting with access to their platforms for digital television. In addition, cable operators will be obliged to provide such an alternative operator with an offer to their analogue television services and internet access for resale. The purpose of this initiative is to create an incentive for more competition in the broadcasting market and in particular the cable market in Belgium.

Triple play obligations

In addition, the BIPT released a draft analysis of the broadband markets for consultation. This analysis led to the BIPT's draft decision confirming the obligations that have already been imposed on incumbent operator, Belgacom (i.e. unbundling of the local loop and the provision of bitstream access). Furthermore, the BIPT proposes imposing an additional obligation upon Belgacom, i.e. providing access to the multi-cast functionality, which would enable alternative operators to offer more "triple play" services.

According to the BIPT and the competent broadcasting regulators, these changes should not only result in more competition in the relevant Belgian cable markets but they should also offer a transparent and structured framework to regulate the various commercial "triple play" offers.

The deadline set for the relevant stakeholders to provide comments to the regulators in relation to the draft decrees was 18 February 2011. The regulators are now considering these comments and plan to come up with a final and definitive version of the draft decrees by this summer.

By Didier Wallaert, Brussels

Outsourcing

UK - When does negligence become gross negligence?

The term gross negligence is commonly used in English law agreements to denote situations in which a party will not benefit from an exclusion clauses nor be indemnified for his conduct. As such, it is an important term but one on which there has been divergent authorities. The recent case of *Camarata Property v Credit Suisse Securities* [2011] EWHC 479 suggests that gross negligence means more than simple negligence but the difference is not easy to define or even describe.

Auto-redemption notes

The litigation arose out of the claimant's purchase of 5 year auto-redemption notes issued by Lehman Brothers Treasure Co BV. These notes were subject to significant losses when Lehman Brothers collapsed. The claimant alleged it had sought advice from the defendant bank about that notes and the advice received was negligent and in breach of its contractual obligations.

The bank refuted these claims and also relied on the exclusion clauses in its contract with the claimant. These stated that it was not liable for any advice it provided unless that liability arose "*directly as a consequence of the gross negligence, fraud or wilful default of us or any of our directors, officers, or employees*":

A further clause excluded any liability for decline in the value of the investments purchased or solvency of a counterparty unless "*the liability arises directly as a consequence of the gross negligence (or, in the case of liabilities arising from our custody activities, negligence), fraud or wilful default of us or any of our directors, officers, or employees*".

Accordingly, the bank argued that even if it was negligent, it was not liable as it had not been grossly negligent (no claim being advanced on the basis of fraud or wilful default). To unpick this, the court had to consider the divergent cases on the meaning of gross negligence.

Nothing more than simple negligence?

The claimant, unsurprisingly, relied on authorities that commented on the difficulty in distinguishing simple negligence and gross negligence, or, put another way, the difficulty in deciding on what "gross" means in this context. In light of these difficulties, they concluded that there was no relevant distinction in the cases before them.

One example, is *Tradigrain SA v Internek* [2007] EWCA Civ 154 in which the Court of Appeal had to consider a German law agreement containing the term gross negligence. The Court found this term had a recognised meaning under German law comprising: (a) an objective element involving a failure to exercise ordinary care where there is a clear risk of harm (the kind of situation which "makes one clap one's hand to one's head and ask 'How can it happen?'"); and (b) a subjective element in the form of an absence of anything which renders the act or omission excusable. However, it did not

have a recognised meaning under an English law contract as gross negligence "*has never been accepted by English civil law as a concept distinct from simple negligence*".

A modern approach to interpretation?

Andrew Smith J took a rather different tack in the current case and decided the question was not whether gross negligence was a familiar concept in English civil law but instead what this term meant in the bank's terms and conditions. A particularly important point was the presence of both "negligence" and "gross negligence" in those terms and conditions, a factor that indicated some distinction must be intended.

However, the difference is one of degree and not kind (indicating that gross negligence is not wholly divorced from simple negligence). While this difference is not easy to define or even describe with any precision, it is likely be capable of embracing not only conduct undertaken with actual appreciation of the risks involved, but also serious regard or indifference to an obvious risk.

Whether a more authoritative view on this term will be forthcoming remains to be seen. Certainly the last time this issue came before the Court of Appeal they decided that the debate about its meaning was a "*somewhat sterile and semantic one*" (*Springwell v JP Morgan* [2010] EWCA Civ 1221) though the interpretation in this case seems to reflect the natural and ordinary meaning of the words and be more in line with Lord Hoffmann's urging to discard the old intellectual baggage of legal interpretation.

In any event, in this case the point was moot. The Court decided the defendant bank could not have predicted Lehman's collapse so was neither negligent nor grossly negligent.

Camarata Property v Credit Suisse [2011] EWHC 479 is available here.

By Peter Church, London

UK - Court considers the risk of interoperability with legacy systems

A substantial part of many systems development projects is the integration of the new system with the customer's legacy systems. A dispute over this issue was considered in the recent case of *McCain Foods v Eco-Tec (Europe) Limited [2011]* EWHC 66 in which the supplier alleged that problems with its equipment arose because it interacted badly with the customer's legacy systems. The court had to decide who assumed responsibility for this risk.

The facts

McCain and Eco-Tec entered into an equipment purchase agreement pursuant to which Eco-Tec supplied McCain with a "scrubber", which was designed to remove hydrogen sulphide from biogas produced by McCain's waste water treatment processes. McCain intended to use the clean biogas in the generation of electricity which was in turn to be used in powering its plants. This would have entitled McCain as an Ofgem accredited generator of renewable electricity to claim "Renewables Obligation Certificates".

The equipment purchase agreement included a specification which set out the purpose for which the "scrubber" would be used and provided that:

> "*The [Eco-Tec] scrubber will be situated in the pipework between the [McCain] blowers which are existing and therefore define the scrubber operating conditions*"

The "blower" was part of McCain's legacy systems. When it became apparent that the Eco-Tec scrubber did not fulfil its intended purpose, McCain brought a claim for breach of contract, alleging that Eco-Tec had supplied equipment that failed to meet the agreed specification. In reply, Eco-Tec argued that the failure of the scrubber to perform as required was attributable to faults in the McCain legacy blower.

Who bears the risk for the legacy systems?

McCain argued that the specification in the equipment purchase agreement clearly transferred this risk to Eco-Tec who was obliged to supply a system that could meet the performance requirements in the specification while being located between, and operating at the same time as, the McCain blower. In response, Eco-Tec argued that the specification did not impose any contractual obligation on Eco-Tec and, instead, just provided the detail of operating conditions within which the equipment was to function.

In finding in favour of McCain, the court remarked:

> "*… the Specification provided for the location of the scrubber and the presence of the McCain blowers. The "scrubber operating conditions" including the pre-existing blower … the equipment was required "to conform to… specifications." If it was unable to be commissioned because of the presence of the McCain blower, which appears to have been the case, that was a breach by Eco-Tec of the requirements of the Specification ... If risk for that breach was to be*

excluded, Eco-Tec could have sought to negotiate that exclusion. They did not do so."

Eco-Tec also sought to rely on a clause which stated that the System was to be "*integrated with any other component(s) described or referred to herein, whether or not such components are provided by Seller, or components will together perform in accordance with the performance standards set out herein*." It argued that the effect of the clause was that the responsibility for coordinating components fell on all of McCain's systems suppliers together. The court rejected that limited interpretation. If that were the intended effect of the clause, then Eco-Tec should have drafted it accordingly.

Recoverable heads of loss

McCain claimed that it had suffered a series of losses which were recoverable from Eco-Tec, including:

> the cost of procuring replacement equipment;

> revenue lost through the inability to claim a Renewables Obligation Certificate; and

> the costs of sourcing electricity elsewhere instead of using electricity that should have been generated by the system provided by Eco-Tec.

In its defence, Eco-Tec sought to rely on a provision which excluded liability for "*indirect, special, incidental and consequential damages*". By reference to well-established authorities (such as *Hotel Services v Hilton International* [2000] BLR 235), the court held that these losses arose naturally from the failure of the scrubber to meet the agreed specification so were all direct losses and therefore recoverable.

Implications for system development agreements

The *McCain* case highlights the important of explicitly allocating risk (and therefore liability) for a failure of a supplier's newly-developed system to interoperate with a customer's legacy systems. From a customer's perspective, it also confirms that a system development agreement should, at a minimum, note the existence of any legacy systems, describe the relevant legacy system components and their function and clearly set out who is responsible for the integration process.

For suppliers, the case underlines the risk associated with accepting an absolute obligation to supply a system that interoperates with legacy systems in circumstances where that interoperation is not assured, or where there has been no obligation to undertake due diligence of those legacy systems. In the *McCain* case, the wording of the equipment purchase agreement was such that even if Eco-Tec had been able to satisfy the court that the McCain legacy equipment was defective, the court would still have found that the risk for a failure in interoperability fell to Eco-Tec.

McCain Foods v Eco-Tec (Europe) [2011] EWHC 66 is available here.

By Ben Buckley, London

UK - Cowboy builders, negligence and your IT suppliers

The ability to bring a claim in tort, as well as contract, provides a number of benefits. Damages are measured on a different basis, claims are (in theory) not limited to contracting parties and the limitation period may be longer. However, while concurrent claims are possible under English law, it is not clear if a duty of care will always arise. The Court of Appeal's decision in *Robinson v P.E. Jones (Contractors) Limited* [2011] EWCA Civ 9 casts some light on this issue and we consider its implications for the information technology and outsourcing industry.

A blocked chimney at 12 Magnolia Rise

The case arose from the construction of a house in 1992. The house owner asked the builder to add an additional chimney flue to one of the rooms of the house so that he could install a gas fire. Twelve years later, the house owner arranged for British Gas to service the fire and discovered the chimney flue was defective. Expert evidence suggested the flue had not been constructed in accordance with good building practice or building regulations.

The cost of any remedial work would be substantial so the house owner brought an action against the builder in 2006. Given the passage of time, any claim in contract was barred under the Limitations Act 1980. However, a claim in negligence, which runs from the date the house owner became aware of the negligence, was not.

Concurrent liability in tort for economic loss

The main issue for the Court of Appeal was whether the builder owed a duty of care to the house owner in respect of economic loss. The starting point for this analysis is that:

> a concurrent duty in tort can exist irrespective of whether there is a contractual relationship between the parties. Where it does exist, the plaintiff is free to choose the remedy which appears to be most advantageous (*Henderson v Merrett [1995] 2 AC 145*); and

> this was a claim for economic loss not personal injury or damage to tangible property. Different rules apply to those claims and a duty of care is much more likely to arise.

With these points in mind, Lord Justice Jackson decided that the relationship between a builder and his client is primarily governed by the contract between those parties and that contract "*is the primary determinant of each party's obligations and remedies*".

A wider duty embracing liability for economic loss is only likely to arise if there has been an assumption of responsibility by the builder. This type of assumption of responsibility is likely when professional persons provide services; "*they give advice, prepare reports, draw up accounts, produce plans and so forth. They expect their clients and possibly others to act in reliance upon their work product, often with financial or economic consequences*".

However, there was nothing to suggest a professional relationship between the parties. This was a normal building contract requiring the builder to complete the construction of the house to an agreed specification, containing specific warranties of quality and agreed remedies. Accordingly, the builder was not under any duty of care to prevent the house owner from suffering economic loss. It "*would be inconsistent with the whole scheme of this contract, if the law were to impose upon the defendant duties of care in tort far exceeding the defendant's contractual liabilities*".

Effect of exclusion clauses

Any duty would, in any event, have been avoided by the terms of the contract between the parties which stated that:

> "*8. The Vendor shall not be liable for any defect .. which is not within the terms of the Certificate of the National House-Building Council ….*
>
> *10. The Vendor and the Purchaser shall forthwith enter in to the National House-Building Council's standard form of Agreement No. HB5 (1986) … The Vendor shall not be liable to the Purchaser … in respect of any defect error or omission in the execution or the completion of the work save to the extent and for the period that it is liable under the provisions of the NHBC Agreement..*"

Lord Justice Jackson decided the only sensible interpretation of these clauses was that the parties agreed to exclude any liability in negligence. This was despite the fact there is no reference to the word "negligence" in either clause. This is thus a further example of judicial retreat from a strict application of the principles in *Canada Steamship v The King* [1952] AC 192.

The clauses were also both found to be reasonable under the Unfair Contract Terms Act 1977. The house owner would have protection under the NHBC Agreement and, while this was not total, it does provide a very substantial benefit, including protecting against insolvency of the builder.

Impact on the information technology and outsourcing industry

These are important issues as there are a number of benefits to bringing an alternative case in tort:

> the measure of damages is different in tort. It is based on the position the customer would be in "but for" the breach. In some cases, a claim in tort can lead to a higher award in damages than a claim in contract, particularly where the customer has struck a bad bargain;

> the limitation period for claims in tort is different. In this case, the house owner's claim in contract was time-barred but his claim for negligence was not; and

> in certain circumstances, the customer may be able to "reach around" the contract and make direct claims against the supplier's sub-contractors (who may not be able to benefit from the limitations and exclusions in the supplier's contract). However, where the claim is for economic loss, such claims will always be difficult as they are likely to circumvent the contractual framework agreed between the parties, see *BSkyB v EDS: Time to reassess the risks of outsourcing?*

The decision is likely to narrow the situations in which tortious claims can be made against information technology or outsourced services providers. In particular, it will be necessary to show there is a professional relationship with that client or the service provider has otherwise assumed a duty of care.

At one end of the spectrum are those providing consultancy services. It is very likely that a duty of care will exist as this is a professional relationship and the consultant will expect their clients and possibly others to act in reliance upon their advice. At the other end of the spectrum are more mundane services such as data entry or coding. It is less likely that a duty of care would exist and the courts are much more likely to see the contract as the primary determinant of each party's obligations and remedies.

The case also provides a useful reminder that it is possible to avoid a duty of care through appropriate contractual provisions. While it will now be harder to establish such a duty, there may be some benefit in putting the matter beyond doubt.

Robinson v P.E. Jones (Contractors) Limited [2011] EWCA Civ 9 is available here.

By Will Robinson, London

Authors: Peter Church

Contacts

For further information please contact:

Tanguy Van Overstraeten
Partner

(+32) 2501 9405

tvanover@linklaters.com

Peter Church
Managing PSL

(+44) 20 7456 4395

peter.church@linklaters.com

One Silk Street

London EC2Y 8HQ

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

Linklaters.com