e-commercelaw&policy

THE E-COMMERCE NEWSLETTER FOR LAWYERS
JANUARY 2013 VOLUME 15 ISSUE 1 **WWW.E-COMLAW.COM**

China tightens online data regulations

China approved on 28 December new laws allowing the deletion of 'illegal' information online and requiring internet users to provide their real names to ISPs.

"China does not currently have a well-formed legal framework regulating the use and abuse of personal data," said Tim Smith, Partner at Rouse, Beijing. "These regulations do provide some user protection, for instance requiring service providers to keep personal information confidential."

The regulations are said to protect personal data and prevent the spread of false information. Commentators have raised serious concerns however that citizens will now cease posting freely online.

"The real name system may help mitigate the dissemination of lies, but this is not a justified excuse for its adoption under law, as it cannot strike a good balance with free expression and corruption reporting," said Wei Zhang, Partner at Jun He. Smith believes however that "This is more likely to be seen as a challenge to the openness of these platforms for [personal expression]. Whistle-blowers have other ways to raise concerns."

IN THIS ISSUE

FTC ends Google probe as EC investigation continues

The Federal Trade Commission (FTC) ended on 3 January its investigation into Google's alleged anti-competitive search practices, finding that Google does not illegally manipulate its search results. Rather, the FTC found that changes to Google's search design are attempts to improve user experience.

The FTC's decision contrasts with the recent reaction by EU Competition Commissioner Joaquin Almunia regarding the European Commission's own ongoing investigation into Google's allegedly anti-competitive search practices. Almunia told the Financial Times that his "conviction is [Google is] diverting traffic" to its search services, at the expense of competitors.

"The FTC did not institute a formal action because Google's suggestion that consumer appreciation is the true measure of the benefit of a design change seemed to sit well with the agency," said Rachel Hirsch, Associate at Ifrah Law. "The settlement, while a loss to Google's competitors, is a win for consumers, at least in the FTC's book." Howard M. Ullman, Of Counsel at Orrick, adds that "The FTC concluded that the evidence did not establish that Google's algorithms were anti-competitive, but were supported by adequate pro-competitive justifications."

The FTC has entered into a voluntary agreement with Google, with the search giant agreeing to allow rivals to opt out of 'scraping,' the copying of content from competitors for search results. Google also cannot now pursue injunctions on standard-essential patents (SEPs) if the licensee is willing to adhere to FRAND terms.

"Google has incentive to honour the agreements," said W. Joseph Price, Associate at Kelley Drye. "Google knows that voluntary agreements do not occur in a vacuum. In the US and elsewhere, there are pending investigations; it would benefit Google to keep the option of voluntary agreements on the table."

"I would expect competitors to be pretty vigilant in seeking to ensure Google honours [these] terms," explains Paul Stone, Partner at Charles Russell. "There may be some issues around determining whether a company seeking access to SEPs is a 'willing licensee' if Google considers the price being offered is not a fair one."

The EC's investigation continues, with some commentators forecasting a different conclusion to that of the FTC. "Many online marketers feel let down by the FTC and would hope the EC takes more aggressive measures," said Hirsch.

EC's new digital priorities fall short of addressing all the issues

The European Commission adopted seven priorities for the Digital Agenda on 18 December, priorities which include investment in high speed broadband and a cyber-security strategy, but do not address all of the concerns.

"The digital single market is far from being achieved in Europe from a consumer's point of view," said Marc Lemperiere, Of Counsel at Bignon Lebray Avocats. "Cross border purchases are very low. Although several directives and regulations have been adopted to this effect, it is surprising that the EC is not addressing this issue directly in its priorities." Vanessa Barnett, Partner at Charles Russell, agrees, "Further efforts need to be made to address the fragmented nature of the current regulatory environment which is stifling cross-border online trade."

The EC's priorities follow a review of the Digital Agenda for Europe, which aims to maximise the potential of ICT. "The digital sector is constantly evolving so it makes sense that the priorities set in 2010 should be updated," said Mark Webber, Partner at Osborne Clarke. However, continues Webber, whether one review after three years is enough is questionable.

"The priorities do not address taxation," adds Lemperiere. "In a context of public finance tightening, Member States want to better tax sales made on their territory over the internet."

"If one has a look at what China is doing with its five year plan," concludes Marc Holtorf, Partner at Clifford Chance, "one certainly doubts that EU efforts are sufficient."

ecommercelaw&policy

THE E-COMMERCE NEWSLETTER FOR LAWYERS
VOLUME 15 ISSUE 1 JANUARY 2013
WWW.E-COMLAW.COM

Editorial: Undisclosed sniffing

The FTC recently reached an agreement with advertising company Epic Marketplace over allegations that the company used 'history sniffing' technology to illegally gather data about the web browsing habits of millions of consumers.

Epic Marketplace, which has a presence on 45,000 websites, used online behavioral advertising to target ads to consumers by placing a cookie on consumers' computers to monitor their web browsing behaviour and therefore accurately gauge their interests.

The problem arose from claims made in Epic's privacy policy, which stated that the company would only collect information from consumers about visits to sites within its network. However, the FTC alleged that in fact Epic was collecting information about consumers' entire web browsing behaviour and assigned consumers interest segments based on the sites they visited. 'Among the domains that Epic "sniffed" were pages relating to fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy,' states the FTC complaint.

However, it was not the practice of history sniffing itself, however sensitive the data collected, that violated Section 5(a) of the Federal Trade Commission Act. It was the 'deceptive acts or practices' that resulted when Epic failed to inform consumers about its use of the technology in its privacy policy.

The agreement reached by both parties, although Epic refused to admit any wrongdoing, mandates that Epic destroy all information it gathered unlawfully and prohibits any misrepresentations about data privacy in future. Interestingly the agreement also bans Epic from any future use of such technology.

Companies should take heed and ensure that their online privacy policies reflect actual practices, because it was not the practices themselves that Epic was held to account for, but there insufficient disclosure.

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Associate Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Editorial Assistant Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions David Guati
david.guati@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com
Print The Premier Print Group

E-Commerce Law & Policy
is published monthly by
Cecile Park Publishing Limited
17 The Timber Yard, Drysdale Street,
London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

CECILE PARK PUBLICATIONS

E-Commerce Law & Policy
Monthly: launched February 1999
E-Commerce Law & Policy is a unique source of analysis and commentary on global developments in e-business legislation. The journal was nominated for the prestigious British & Irish Association of Law Librarians (BIALL) Serial Publication of the Year Award in 2001, 2004 and 2006.
PRICE: £480 (£500 overseas).

E-Commerce Law Reports
Six issues a year: launched May 2001
The reports are authoritative, topical and relevant, the definitive practitioners guide to e-commerce cases. Each case is summarised, with commentary by practising lawyers from leading firms specialising in e-commerce.
PRICE: £480 (£500 overseas).

E-Finance & Payments Law & Policy
Monthly: launched October 2006
E-Finance & Payments Law & Policy provides all those involved in this fast evolving sector with practical information on legal, regulatory and policy developments.
PRICE £600 (£620 overseas).

Data Protection Law & Policy
Monthly: launched February 2004
Data Protection Law & Policy is dedicated to making sure that businesses and public services alike can find their way through the regulatory maze to win the rewards of effective, well-regulated use of data.
PRICE £450 (£470 overseas / £345 Govt).

World Online Gambling Law Report
Monthly: launched April 2002
World Online Gambling Law Report provides up-to-date information and opinion on the key issues confronting the industry.
PRICE £600 (£620 overseas).

World Sports Law Report
Monthly: launched September 2003
World Sports Law Report is designed to address the key legal and business issues that face those involved in the sports industry.
PRICE £600 (£620 overseas).

DataGuidance
Launched December 2007
The global platform for data protection and privacy compliance.
www.dataguidance.com

Consumer protection when 'purchasing' digital content

The UK Government is collating responses to its consultation on a Consumer Bill of Rights, which aims to clarify and modernise consumers' rights in relation to goods, services and digital content. H. Kristjan Larusson and Hayley Davis, of Taylor Vinters, discuss the Government's approach to ensuring that consumer rights, particularly in regards to digital content, fully protect the consumer.

Consumer protection has been noted as most lacking in the digital arena, where consumers are often unclear of their rights and remedies. Digital content is most easily identified as any item 'produced and supplied in digital form.'[1] This article aims to assess the current problems with analogue ideas of consumer protection in an increasingly digital economy, and whether the Consumer Bill of Rights (CBR) can adequately bridge the gap between traditional goods and services and digital content.

Current issues

UK consumer law is currently laid out across a number of different Acts and regulations. The CBR does not seek to drastically change the existing legal position for consumers. Instead, the Bill intends to clarify the legal position, by providing a clear code of rights to enable consumers to have the confidence to challenge businesses when they purchase poor quality goods, services or digital content in the 'modern marketplace.'

The concept of software under the existing law illustrates the uncertainty in the digital arena. The leading case on defining whether software constitutes 'goods' for the purposes of statutory consumer protection dates back to 1996[2], before the burgeoning popularity of downloading and streaming digital content. The case drew a distinction between the software itself, which could not be considered 'goods' and the disk on which the software was supplied, which was included within the definition of 'goods.' This dichotomy resulted in consumers having to prove whether the fault was with the software or the physical disk. Consequently, as the law stands, a consumer who purchases a film or game in a shop will, most likely, have greater protection than a consumer who accesses the same film or game online.

When consumers buy something, regardless of whether it is goods or services, certain terms are implied into the contract between the parties. The importance of distinguishing whether goods or services have been purchased relates to these implied terms and the extent of the resulting rights afforded to a consumer. For example, seven terms are implied into a contract for the purchase of goods (under the Sale of Goods Act 1979), compared to only one implied term for service contracts (under the Supply of Goods and Services Act 1982). There is a conceptual difficulty with classifying intangible digital content, which does not easily fall within either category. As a result, it is unclear what rights are available to consumers in relation to digital content and what recompense is available if things go wrong. This uncertainty in the legal status of digital content, has led to digital content being dealt with separately under the CBR.

Under the CBR, digital content will be treated broadly along the same lines as the newly proposed law on the supply of goods, with a distinction drawn between the delivery of the content (service), and the content itself (goods). This distinction may still be problematic for digital content and ignores the fact that digital content is usually subject to a licence rather than sale. The Government consultation acknowledges that digital content is usually regulated by End User Licence Agreements (EULAs), allowing the owners of the digital content to impose their own terms on consumers, but fails to explore the interrelation between the new consumer rights and EULAs.

The suggestion that the CBR may override any contrary terms included in a EULA is a worrying development for content owners, particularly coupled with the recent decision in Usedsoft GmbH v. Oracle International Corp[3]. In a decision that seems somewhat counter-intuitive, the CJEU held that the right to distribute a copy of a computer program, which had been downloaded from the internet with the permission of the content owner, was exhausted if the content owner had also granted the customer the right to use the copy for an unlimited period of time, provided that consideration had been paid. Such a decision would appear to treat this transaction as a sale and hence treat the software as goods. This decision was given under the EU Software Directive and it may be that subsequent decisions made under the Consumer Rights Directive would clarify digital goods and services classification.

Any proposal will have to overcome the lack of awareness of consumer rights over digital content. Educating the public as to their new rights will be easier if the rights themselves and methods of challenge are clear.

In addition, the rights of redress for digital consumers must be worthwhile. A survey by consumer watchdog, Which?, found that 62%

of people had not taken any action after being disappointed by a downloaded purchase[4]. This may depend on the nature of the digital content: if a customer downloads an app for £0.99 that falls short of the expected quality, they may simply chalk it up to experience, although the same is unlikely to occur where that customer purchases expensive, but faulty software. However, a customer's right of redress must be the same and must be dealt with in a uniform way by content providers, irrespective of the value or nature of the digital content. Content providers will need to be aware of the additional problems that can be experienced in the delivery and purchase of digital content, including technical incompatibility and access problems.

The Government's proposals

The Government seeks to provide consumers with a series of statutory guarantees, which replace the current implied terms and clearly state the quality standards digital content must meet, together with remedies available in the event of breach of these guarantees. Traders would not be able to exclude or limit their liability in relation to these statutory rights, and it is envisaged that these rights will apply to digital content provided outside of the UK to UK-based consumers.

Under the proposals, digital content must meet any description given and be of satisfactory quality. It must meet a reasonable person's expectations, although this is to be based on an objective assessment rather than the consumer's opinion, and consumers must allow for minor glitches that may be resolved in due course. Furthermore, a trader supplying digital content must have the right to supply that content and hence not put the consumers in a position where they may be in breach of copyright.

Any proposal will have to overcome the lack of awareness of consumer rights over digital content. Educating the public as to their new rights will be made easier if the rights themselves and methods of challenge are clear and intelligible to all.

There are some important issues that the Government will face. A key issue is the uncertainty in relation to guarantees over what is being purchased. For example, most 'sales' of digital content resemble more of a licence than a 'sale.' This may cause issues when aligning the treatment of digital content with that of goods. An issue associated with this is the degree of title or rights afforded to the consumer under the contract. For example the consumer is unlikely to receive full title to the digital content, including the copyright to such.

The consultation asks whether consumers of digital content should be given the right to reject the content. The OFT's response to the consultation is uncertain in its approach, initially stressing the importance of having the right to reject in relation to 'small value items,' presumably as opposed to 'high value items.' However, later on, the OFT can only be understood as meaning that it believes that such a right should exist in general in relation to all items, regardless of their value[5].

Further, as recognised by the OFT, the right to reject directly relates to the issue of the 'obligation to delete' and the real danger of consumers abusing the right to reject by keeping or making additional copies of the product and receiving a refund, but continuing to use the product. Therefore the right to reject could significantly impact online business. In an attempt by content owners to hinder such potentially fraudulent activity, it could also trigger the return to draconian digital rights management software attached to digital content. One can seriously doubt that there will ever be a 'technically acceptable solution to allow such content to be safely removed from the user's device once a refund has been received'[6], which would adequately deal with this danger. Hence this issue requires additional legal, technical and empirical studies before a conclusion can be reached.

Conclusion

Online commerce in digital content remains in flux. The current speed of innovation and the regular introduction of new technologies and business models, probably render this inevitable. The law governing the digital arena can only follow this development and will probably never catch up, or at least not until online commerce has reached a 'stable condition.' Therefore, and despite the emphasis on technology-neutral legal principles as set out in the Government consultation, the law governing digital content and consumer protection will also remain in flux, where legal certainty can only be achieved to a certain degree.

H. Kristjan Larusson Associate
Hayley Davis Solicitor
Taylor Vinters
kristjan.larusson@taylorvinters.com
hayley.davis@taylorvinters.com

With thanks to Emma Whiting for her assistance in preparing this article.

1. Article 2(11) of the Consumer Right Directive 2011/83/EU.
2. International Computers Ltd v St Albans District Council [1996] 4 All ER 481.
3. UsedSoft GmbH v Oracle International Corp, Case C-128/11, 24 April 2012.
4. http://conversation.which.co.uk/technology/download-refund-disappointing-faulty-app-store-itunes-android-market/
5. 'Enhancing Consumer Confidence by Clarifying Consumer Law: consultation on the supply of goods, services and digital content - The OFT's response to the Government's consultation', http://www.oft.gov.uk/shared_oft/reports/oft_response_to_consultations/OFT1453resp.pdf
6. Para.5.32 of the OFT's response.

The COPPA Final Rule: an analysis of the 2012 revisions

After two years of analysis, public workshops, and public comments, the Federal Trade Commission announced its revised Final Rule in late December 2012. Effective 1 July 2013, the Final Rule revises the existing Children's Online Privacy Protection Act (COPPA) in many ways. John P. Feldman, a Partner at Reed Smith LLP, discusses these changes.

The most important changes are: definitional changes; changes to notice provisions; changes to methods and exceptions to consent requirements; changes to confidentiality requirements; and changes to the safe-harbour provisions. The revisions to the COPPA Rule signal an increase in enforcement activity at the FTC. They also raise the stakes for those operators who offer content for kids. Such operators will now be strictly liable for the acts of others under some circumstances. Marketers should review their procedures and consider internal protocols that will enable them to prove to the FTC that they are operating in compliance with exceptions to the notice and consent requirements.

Collection of information

The FTC expanded the definition of 'collects or collection' to include a concept of implied collection. Where the original definition in the COPPA Rule included 'requesting that children submit personal information online,' the new definition expands the scope to include 'requesting, prompting, or encouraging a child to submit personal information online.'

The Commission has chosen to use this opportunity to 'allocate and clarify' responsibilities under COPPA. Under the revised Final Rule, a child-directed content provider is strictly liable for personal information collected by third parties through its site. The Commission takes the position that any benefit arising from a third party's presence on a child-directed site justifies placing responsibility on the operator if the third party collects information from a child.

A plug-in or advertising network that collects personal information from users of both general and child-directed sites will be liable for a COPPA violation only if it has actual knowledge that it is collecting personal information from a specific child.

'Personal Information'

There were several changes regarding the definition of 'personal information.' First, personal information will now include a screen or user name if it functions as online contact information. An anonymous screen name will be deemed personal information if one can use it to contact the person on a website or online service. Second, the definition of 'persistent identifiers' has been modified to prohibit online behavioural marketing targeting children. In the original Rule, the Commission would consider a persistent identifier such as a cookie to be personal information if it was associated with individually identifiable information. The FTC now is focusing on a business practice it abhors: online behavioural marketing.

The definition of 'support for internal operations' sets forth seven activities. They are:

1. To maintain or analyse the functioning of the website or online service;
2. To perform network communications;
3. To authenticate users of, or personalise the content on, the website or online service;
4. To serve contextual advertising on the website or online service;
5. To protect the security or integrity of the user, website, or online service;
6. To ensure legal or regulatory compliance; or
7. To fulfill a request of a child permitted under one of the exceptions to the COPPA Rule.

'Personal information' has been expanded to cover photographs, videos and audio files regardless of whether they could permit 'physical or online contacting.' Fourth, personal information now expressly includes geolocation data.

'Disclosure' means the release of personal information collected by an operator from a child in identifiable form for any purpose except where an operator gives such information to a person who provides 'support for the internal operations of the website or online service.' It is important to keep a documented file as to the purpose of any disclosure of personal information that contains or may contain children's data to meet any applicable exception related to the internal operational use of the data.

A service directed at children

A website or online service is directed to children if it falls into two basic categories: (1) extrinsic evidence suggests that it is directed to children or (2) the website or online service has actual knowledge that the service is collecting information from users of another website or online service directed to children. A website or online service that appears to be directed to children will not be deemed to be such a site if:

a. it does not 'target children as its primary audience';

b. it does not collect personal

information from any visitor prior to collecting age information; and

c. it prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under 13 years of age without complying with the notice and parental consent requirements under the Rule.

Clear and conspicuous notice

The Final Rule provides clear guidance as to what will constitute clear and conspicuous notice. When an operator seeks to obtain a parent's affirmative consent to the collection, use, or disclosure of a child's personal information, the notice must set forth:

a. That the operator has collected the parent's online content information from the child in order to obtain the parent's consent. If so, the notice has to include the name of the child or the parent.

b. That the parent's consent is required for the collection, use, or disclosure of such information. The notice has to also state this in the converse: that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent.

c. The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, assuming the parent gives consent.

d. A link to the operator's online notice of its privacy practices.

e. The means by which a parent can provide verifiable consent.

f. That if the parent does not provide consent within a reasonable time from the date of the notice, the result will be that the operator will delete the parent's online contact information from its records.

The Commission has 'strengthened' the confidentiality, security, and integrity provisions of the rule to require operators to inquire about the practices of service providers and third parties with whom it does business.

When an operator seeks to obtain the parent's online contact information merely so that it can voluntarily communicate with the parent about a child's participation on a website, and there is no collection, use, or disclosure of personal information from or about a child, the notice must set forth:

a. That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information.

b. That the parent's online contact information will not be used or disclosed for any other purpose.

c. That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so.

d. A link to the operator's online notice of its privacy practices.

When an operator seeks to send the parent notice that it is complying with the COPPA Rule exception for multiple communications with a child (§ 315(c)(4)), the notice must set forth:

a. That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child.

b. That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator.

c. That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child.

d. That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so.

e. That if the parent fails to respond to the direct notice, the operator may use the online contact information collected from the child for the purpose stated in the notice.

f. A link to the operator's online notice of its privacy practices.

When an operator is sending a notice to a parent to let him or her know information concerning the child's safety, the notice must set forth:

a. That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of the child.

b. That the information will not be used or disclosed for any purpose unrelated to the child's safety.

c. That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so.

d. That if the parent fails to respond to this notice, the operator may use the information for the purpose stated in the direct notice.

e. A link to the operator's online notice of its privacy practices.

In the Final Rule, the FTC retained the 'email-plus' sliding scale approach that permits a quasi-verifiable approach in situations where the operator does not disclose children's personal information. When the operator is collecting and using personal

information for internal purposes only (such as to fulfill prizes), he can use an email 'coupled with additional steps to provide assurances that the person providing the consent is the parent. Additional steps include: sending a confirmatory email to the parent following receipt of the consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.'

Exceptions

With regard to the COPPA exceptions set forth in § 315(c), the Commission has made a few substantive changes.

1. § 315(c)(1) - It remains permissible to collect the name or online contact information of a parent or child to be used for the sole purpose of obtaining parental consent.
2. § 315(c)(2) - There is a new exception that gives operators the option to collect a parent's online contact information for the purpose of providing notice to, or updating, the parent about the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information.
3. § 315(c)(3) - It remains permissible to collect on a one-time basis online contact information from a child in response to a child's request. This will maintain the ability to send notifications regarding a contest or sweepstakes, forward-to-a-friend emails, birthday messages, or similar communications.
4. § 315(c)(4) - It remains permissible to notify a parent via email that the operator has collected a child's online contact information to contact a child multiple times (such as to provide a child with a newsletter). Notifying the parent by postal mail is no longer permissible.
5. § 315(c)(5) - It remains permissible to collect both the child's and the parent's online contact information where it is necessary to protect the safety of the child and where the information is not used for any other purpose.
6. § 315(c)(6) - It remains permissible to collect a child's name and online contact information in order to protect the security or integrity of the website or online service; take precautions against liability; respond to judicial process; and to the extent permitted by other provisions of law.
7. § 315(c)(7) - There is no notice or consent required by virtue of the collection of a persistent identifier where it is used solely to provide 'support for the internal operations of the website or online service.'
8. § 315(c)(8) - This new exception relates to the definition of a 'website or online service directed to children.' This new provision relates to social media platforms with age-screening processes that collect persistent identifiers to establish a personal link to a site, such as to 'like' a page.

Security

The Commission has 'strengthened' the confidentiality, security, and integrity provisions of the rule to require operators to inquire about the practices of service providers and third parties with whom it does business. Operators must inquire about such entities' data security capabilities and, 'either by contract or otherwise,' receive assurances from such entities about how they will treat the personal information they receive. Similarly, the Commission has added a new provision that states that an operator of a website or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected.

COPPA establishes 'safe-harbours' for participants in Commission-approved COPPA self-regulatory programs. This program has worked very well. However, demonstrating its distrust of self-regulation even as it publicly praises it, the Commission has modified the COPPA Rule to impose greater governmental oversight onto 'self-regulation.'

John P. Feldman Partner
Reed Smith LLP, Washington, DC, office
jfeldman@reedsmith.com

Free's ad-blocker ignites the net neutrality debate in France

Free, one of the three main French Internet Service Providers, exacerbated the net neutrality debate with its 3 January announcement that it was installing an ad-blocker on its Revolution Freebox. This application would block some advertising on end users' equipment. Marc Lempérière, Of Counsel at Bignon Lebray Avocats, discusses the implications of such a move and the on-going net neutrality debate in France.

The initiative seems to be part of Free's dispute with Google over their peering agreement and therefore has broader implications than only the rights of Internet Service Providers (ISPs) to filter content. Free suspended the initiative within days, but the announcement has brought the net neutrality debate into the spotlight.

Net neutrality refers to a principle whereby all electronic communications networks must carry all data streams in a neutral fashion, regardless of their nature, content, sender or recipient. This principle is not only a legal principle, but was one of the causes of the development of the internet, since it lowered barriers to entry, making possible the constant innovation that characterises this ecosystem. Although it is considered one of the founding principles of the internet, to date none of the EU Member States (except the Netherlands) have adopted restrictive legal provisions for protecting net neutrality.

In 2012, the French government indicated that it felt no urgency to adopt a law on the subject. The high profile of Free and its ad-blocker is likely to create urgency, however. In such a case, the French government will be able to rely on the work, which has been carried out by the French Parliament, various ministries and the ARCEP (Authority for Regulation of Electronic and Postal Telecommunications). Indeed, two bills (2010, 2012) and a report (2011) have already been filed with the *Assemblée Nationale* and the ARCEP issued a report on net neutrality in September 2012. Although the two bills will probably not become law, they and the other preliminary work in this area identify two main issues: the legal protection of net neutrality and the technical measures needed to ensure protection without threatening the development or financing of internet initiatives.

Consecrating neutrality

Although the ARCEP declined to recommend whether web neutrality needed to be legally defined, both bills proposed that a formal definition be adopted and enforced in France.

The 2010 bill states that the principle of net neutrality 'must be understood as the interdiction of discrimination related to the content, the senders or the recipients of digital exchange of data.' The 2012 bill is more detailed, defining the principle as 'the capacity for internet users (i) to send and receive the content of their choice, use services or operate applications of their choice, to connect equipment or use programmes of their choice, provided they do not damage the network (ii) with a quality of service that is sufficient, transparent and nondiscriminatory and (iii) without prejudice to the obligation pronounced following a judicial procedure or measures required because of security reasons and by unforeseeable congestion situations.' The 2012 definition is expressed in terms of rights for internet users, rather than obligations for the various actors who make possible the functioning of the internet. The 2012 definition would allow ISPs to discriminate between data on the basis of content, sender and recipient, provided the rights of internet users are respected.

The 2012 bill also proposes to limit the powers of the French government to constrain net neutrality by ordering the blocking of websites. French public authorities can currently block websites under three different laws:

- Firstly, in accordance with the 2004 law implementing EC Directive 2000/31 concerning E-Commerce and some provisions of EC Directive 2002/58 on Privacy and Electronic Communications, French judicial authorities can require ISPs or suppliers of hosting services to take measures to prevent damages caused by content of online services.
- Secondly, the President of the agency that regulates online gambling (ARJEL) can ask the *Tribunal de Grande Instance* of Paris to compel ISPs to block access to websites that repeatedly breach online gambling regulations, despite an injunction that such activity cease. At the time of adoption, French ISPs vigorously denounced the risks posed to net neutrality.
- Thirdly, in case of breach of copyright caused by an online telecommunication service, the HADOPI law allows copyright owners and organisations to request from the *Tribunal de Grande Instance* that measures be taken to prevent such breach. Regarding this law, the *Conseil Constitutionnel* ruled that, in view of the role of internet access in the exercise of freedom of expression and communication, only a judge could sanction interrupting this access and force the government to modify the procedure that allows

the HADOPI authority to block subscriptions to ISPs.

The bill makes clear that only a court may require that access to online communication services be blocked, thereby strengthening the protection of net neutrality against measures unilaterally decided by governmental authorities.

Protecting quality and universality

The 2010 bill, proposed by the Socialist party, imposed four obligations on ISPs in order to ensure their compliance with the principles of web neutrality. ISPs:

- Must allow users to connect as many items of equipment to on-line services as they wish;
- Cannot restrict capacities of transmission without explicit agreement of ARCEP or a court;
- Must communicate for free the technical modalities of interconnection with their network; and
- Can only transmit a stream of data as a priority if all streams of data support the same use, no matter what their protocol and other means of transmission benefit from the same priority or upon decision of judicial authority.

Repeated breach of the provisions could be sanctioned by ARCEP with fines of up to €10,000,000. Interestingly, article 4 of this bill would have allowed the ARCEP to sanction practices implemented by Free, while the French government, under current legislation, could only react by organising a meeting between ISPs and Content Access Providers (CAPs). In contrast, the 2012 bill only requires the ARCEP to implement a monitoring body concerning the compliance of ISPs with net neutrality.

The ARCEP, in its September 2012 report, stated that it was ensuring net neutrality through:

- Using competition and transparency to promote the principle of neutrality. The ARCEP argued that 'the greater the pressure created by competing high-quality access products, the less incentive an ISP will have to diminish the quality of its own service.' ARCEP noted that transparency could be improved in the French market and is working to establish a framework for informing users of the specific features of their internet services.
- Increased monitoring of the quality of internet access services. The ARCEP conducts an annual quality-of-service survey that already includes indicators for internet access. It has expanded its measurement of fixed networks to include internet access indicators.
- Regulation of traffic management. The ARCEP re-affirmed its belief that traffic management practices can be used only if they are relevant, efficient, proportionate, transparent and do not discriminate. However, the ARCEP also acknowledged that specialised services supplied with a controlled quality of service may rely on traffic management techniques, provided they do not diminish the quality of the internet and comply with competition law and sector specific regulation.
- Monitoring of interconnection agreements and disputes. The ARCEP noted that the structure of interconnections agreements and the interconnection market was changing rapidly. Among the trends is the fact that the frontier between ISPs and CAPs is becoming less clear, since CAPs are deploying their own network infrastructure while ISPs are diversifying into CAPs' activities. ARCEP noted that developments may threaten net neutrality, with ISPs being tempted, for instance, to discriminate in favour of the traffic they generate, but it also made it clear that ARCEP was not planning regulatory involvement in this market, which has developed without intervention.

Interestingly, article 4 of this bill would have allowed the ARCEP to sanction practices implemented by Free, while the French government, under current legislation, could only react by organising a meeting between ISPs and Content Access Providers (CAPs).

Conclusion

It seems that - in France, at least - net neutrality is becoming less a general principle than a right of consumers. This interpretation could, despite additional obligations, be quite favourable for providers. It would offer them more leverage against CAPs by threatening to discriminate against traffic arising from their sites, as Free has allegedly attempted to do against Google. Indeed, ISPs and CAPs are debating sharing the financing of new infrastructure with ISPs. ISPs allege that, since they are the main beneficiaries of the existing infrastructure, CAPs should contribute to development. Most analysis of Free's ad-blocker initiative has argued that Free was using its infrastructure to leverage its power to discriminate between senders of data and to slow traffic (in this case from YouTube, a Google subsidiary), to try to impose a paying peering agreement on Google that would be more favourable to Free.

It seems a consensus concerning net neutrality is emerging among French authorities. Ms. Fleur Pellerin, the French Minister for the Digital Economy, has refused to make any accusations against Free, but has stated that Free's ad-blocker raised issues concerning the sharing of value between CAPs and ISPs. It must be noted that many CAPs are located in tax havens. The French government has long sought to more efficiently tax income generated by these CAPs. Therefore, as the net neutrality debate continues, it must be asked whether the French government will remain fully neutral.

Marc Lempérière Of Counsel
Bignon Lebray Avocats
mlemperiere@bignonlebray.com

The rights and wrongs of social media evidence

With over a billion people communicating via social media sites such as Facebook, Twitter and LinkedIn, the appeal of user posts and messages as sources of criminal intelligence has never been stronger. Mark Johnson, Founder of the Risk Management Group, discusses the value of evidence gathered from social networking sources.

The diversity of social media enhances its value as a source of information, but just as this vast seam of data is starting to be efficiently mined, a number of inhibitors are being identified. New US legislation in the form of AB 1844, questions about privacy, flaws in the processes employed by providers for validating users' identities, as well as attribution and geo-location challenges, may all conspire to undermine the reliability of social media evidence.

Social media complexity

Legal and ethical thinking in relation to digital or open source online intelligence gathering is still playing catch up with the evolving social media product and service mix. One can spot this in the language used, for example in the way that social network services (SNS) are treated as being homogeneous when, in fact, they have specialised characteristics.

The term 'social media' is broader than 'networking' and includes blogging, micro-blogging (e.g. Twitter), file sharing, gaming, life streaming, authoring and a multitude of other activities, any of which represents a source of intelligence that could be used by the Police and other agencies. This complex mix requires a finely crafted set of guidelines because each facet of social media has the potential to confront investigators with unique points for consideration.

It is also important that we appreciate the sheer scale of social media data. Facebook reports that its data storage is growing by half a Petabyte every two days. To put this into context, one Petabyte equates to 13.5 years worth of high definition video.

Privacy and user identities

Google has long been in the privacy spotlight and the company is not well served by recent missteps or by public statements by CEO, Eric Schmidt. In October 2012 the firm admitted that its Street View vehicles had collected personal data by tapping into the unsecured Wi-Fi connections of private citizens. Why the cars would even be equipped to do this in the first place is unclear. Then in September 2012 Google confirmed that an employee had been fired for accessing the personal data of users, four of whom were children, casting doubt on its internal security and data protection mechanisms.

The matter of Lord McAlpine's public trial-by-tweet serves to underline some important points concerning issues of online identity, privacy, journalistic ethics and defamation via social media:

- Social media is immensely powerful through its ability to influence opinions, but that power does not imply accuracy and, according to Jonathan Coad of Lewis Silkin, users have a clear legal and social responsibility to ensure that whatever they publish, regardless of the medium, is true and accurate if it infringes the human rights of others.
- The complete lack of editorial control within social media means that, at present, anyone can publish anything to a global audience without effective oversight.
- Establishing the identity of those posting on social media sites can be challenging. Well-known brands and individuals are the most likely to be correctly identified. Other users suffer no such restrictions and accounts are regularly created using fabricated identities.

The true figure is unknown, but by comparing disclosures made by sites like Facebook with our own findings, we estimate that perhaps 5% of all profiles are wholly or partly fabricated. It may well be that as awareness of the risk of monitoring increases, only a diminishing minority of criminals will sign up for a social media account using their real names. In fact, far from being a vast bucket of reliable data, social media could just as easily become the most effective way to communicate and plan anonymously.

To demonstrate this particular area of weakness, The Risk Management Group conducted a series of experiments on behalf of UK insurers Legal & General as an input to the firm's Digital Criminal Report 2012. We were able to create eight fake Facebook profiles, each of which attracted hundreds of friends. Fake accounts were also setup on LinkedIn and Twitter as a part of this trial. Every one of these fake accounts remains live twelve months later.

While it is true that payphones, pre-paid mobile devices and email provide similar levels of anonymity, the degree to which new social media forms can be used for mass broadcast is unprecedented. As we enter an era characterised by the 'news broadcast organisation of one,' it becomes ever more important that we are able to validate the identity of each broadcaster. As Jonathan Coad said, paraphrasing Lord Justice Leveson, we face the risk of

mob rule online and our society needs to make a choice between responsible online behaviour governed by long established legal principles for the protection of human rights, and the rule of the online mob.

Implications of US AB1844

While some push for greater accountability for posts online, we are also seeing increasing pressure for better protection of online privacy. In September 2012 Sarah J. Banola and Stephen Kaus of Cooper White & Cooper published an article that addressed the possible implications of the signing into California law of AB 1844: 'AB 1844 prohibits employers from requiring job applicants or employees to allow access to their personal social media sites, except if access is reasonably required to investigate allegations of employee misconduct or violation of laws or regulations. Governor Brown announced his action on various social media sites, including Twitter, Facebook, Google+, LinkedIn and MySpace.'

AB 1844 may well herald a shift in attitudes towards the uses to which social media data may reasonably be put. Data that has hitherto been regarded as 'open source,' and therefore fair game, may well come to be regarded as personal and private.

Defamation to incrimination

Twitter provides us with a perfect example of this social media diversity. Unlike Facebook, where users 'friend' each other and form what can effectively become closed user groups, Twitter is by design a broadcast medium. The vast majority of Twitter's 100 million users fully expect to have their posts read by strangers. However, the failure of providers like Twitter to validate user identities allow users to create fictional or forged identities with ease, in order to conceal their true identity but occasionally in order to defame, impersonate or incriminate. This is something that cannot readily be done in the telecommunications or corporate email domains without acts such as credit card or identity theft, hacking or social engineering.

AB 1844 may well herald a shift in attitudes towards the uses to which social media data may reasonably be put. Data that have hitherto been regarded as 'open source,' and therefore fair game, may well come to be regarded as personal and private.

In the absence of proper identity validation techniques for the whole of the user base, most social media evidence is suspect so corroborating evidence is essential. However, even corroboration is becoming more difficult to achieve as users move away from the desktop computer onto mobile devices, many of them using anonymous pre-paid SIM cards or operating across public WiFi networks.

An informative discussion of the issues related to privacy is provided in a paper written by UK lawyers Micheal O'Floinn and David Ormerod. Questions are raised about expectations of privacy and the need for authorities to justify the actions taken to capture and record SNS communications. Coad, on the other hand, contends that virtually all social media discourse is public, in the sense that it generally occurs between three or more people. The presence of that third party is the element required to make a defamatory remark actionable because it has been published. The question is whether the maker of a defamatory remark can simultaneously claim any expectation of privacy. Logic would suggest not.

This still leaves the matter of messages sent between individual users of social media sites, which are not posted on the public 'wall' and which can only be accessed by logging onto the account of either sender or the receiver or via lawful intercept mechanisms. These would seem to be similar to email messages and they might require different treatment. We therefore have a range of social media message formats to consider:

- Broadcast messages, such as the McAlpine-related tweets or unsecured Facebook posts.
- Group messages within sites, in instances when privacy settings are activated.
- Private messages sent between individuals within sites, which can only be viewed by logging onto the account of one of the parties.

Conclusion

Ethical questions, privacy concerns, identity validation flaws, technical data collection and retention challenges and the difficulties of corroboration all raise serious questions about the value of social media evidence. This is not to say that those publishing defamatory remarks or plotting criminal offences via social media should not be held to account, but rather to acknowledge that as social media users become increasingly aware of monitoring we can expect to see a corresponding increase in the use of fake profiles, as well as increasing use of privacy settings or private messaging. Unless social media service providers take steps to strengthen their user identity checks (here the horse may have already bolted) the value of social media data as evidence is likely to decrease sharply over time.

The real value of social media monitoring is to be found in analysis of the general. Social media can tell us what people are thinking, where they are and how they might intend to behave. In the longer term, social media is far more important as a source of social intelligence than as evidence.

Mark Johnson Founder
The Risk Management Group
Elena Jacobs Solicitor
LLM Solicitors
mark.johnson@trmg.biz

Mobile application developers: a target of regulators

Regulatory enforcement on mobile apps

Lawmakers and regulators are targeting mobile application ('mobile apps') makers, specifically their information and data privacy practices, hard. Government has good reasons to do so as some mobile app developers have clearly been lax in their compliance with existing privacy laws and regulations and handling of consumer data. Furthermore, mobile phones and handsets are much more personally identified with a specific person than computers, so app developers do not have the same level of deniability around the issue of data collection and whether data collected through a mobile handset is personally identifiable. Finally, collection of personally identifiable information ('PII') of children under 13 years old is subject to specific federal law; the FTC is keen on enforcing this.

Industry may argue that regulations will stifle and should not interfere with its development, and that the players are often small business entrepreneurs creating jobs. While these arguments fail to support lack of compliance with established legal doctrines, a more persuasive argument may well be that some of the laws and regulations are not entirely clear, and that compliance therefore is not a simple or inexpensive matter. Established tech behemoths operating in the mobile app space, on the other hand, may welcome complicated legal compliance regimes, as they can support large legal/privacy compliance departments. What is important is to understand the regulatory environment and where enforcement is currently focused.

California Attorney General actions

The California Online Privacy Protection Act[1] requires that companies conspicuously post a privacy policy on their websites. It may be difficult for mobile apps to post a privacy policy, simply because such documentation is not generally incorporated into the consumer's app experience.

California's Attorney General ('AG'), Kamala Harris, takes the position that mobile apps are covered by California's law, like websites. The first action in her strategy to enforce this was in February 2012, when the AG reached the agreement with six major online app platform companies[2] that the state law applies to mobile apps. Then, in October and November 2012, AG Harris sent warning letters to many mobile app developers that were considered non-compliant with the state law[3]. In December 2012, AG Harris lodged allegations against Delta Air Lines for, according to the Complaint, failing to comply with California's law in its treatment of its mobile app[4].

The Complaint against Delta alleges two primary violations of state law. First, the Delta app allegedly failed to conspicuously post or make reasonably accessible a privacy policy in or around the mobile app. The AG warned Delta that if it failed to bring the mobile app into compliance within 30 days, it could be subject to enforcement. Second, although Delta's traditional website does have a posted privacy policy, it allegedly fails to address the Fly Delta mobile app and to list the personally identifiable information collected through the app, as required by law. Specifically, Delta's mobile app collected geo-location data, credit/debit card account information, date of birth information, passport information, and other information, that was not addressed in the privacy policy. Many of these data points are not specified in the statutory definition of PII, but could be considered as such if maintained in a form that could be combined with an identifier in the statute, such as a full name. The Complaint alleges that Delta, therefore, failed to comply with its own posted privacy policy by collecting certain forms of data that are not addressed in the privacy policy.

Mobile app developers need to ensure compliance with California's privacy policy law because it provides a general baseline for privacy compliance for the entire US.

Published guidance

In September 2012, the FTC published a guide for app developers called 'Marketing Your Mobile App: Get it Right from the Start:'[5] guidance regarding how the FTC may apply its Section 5 authority to police deceptive and unfair practices in the mobile app arena and helpful for providing baseline understandings in the areas of advertising and privacy. Advertising guidance includes (1) telling the truth about what a mobile app can do, and (2) disclosing key information clearly and conspicuously.

The FTC has advised industry to (1) utilise 'privacy by design' by incorporating privacy protection into practice from the outset of development, (2) be transparent by providing privacy notices that are easy to find and understand, (3) offer easy to locate choices about the app's privacy practices, (4) honour privacy promises - note that sites and apps will be held to the exact letter of their privacy policies, (5) be aware of COPPA and otherwise take special care to protect kids' privacy, (6) collect sensitive information such as medical, financial, or precise geo-location information, only with consent, and (7) keep user data secure.

Those who operate within the mobile app ecosystem must be aware of the laws, rules, and regulations that govern their actions and practices. Failure to comply with applicable law will not be met with a slap on the wrist.

Barry M. Benjamin Partner
Kilpatrick Townsend & Stockton, New York
Bbenjamin@kilpatricktownsend.com

1. The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).
2. Amazon, Apple, Google, Hewlett-Packard, Microsoft, Research in Motion.
3. http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance
4. People v. Delta Air Lines Inc., Cal. Super. Ct., No. CGC-12-526741, filed 12/6/12.
5. http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

Combating IP infringement in Thailand: posed amendments

The sale of pirated products and counterfeit goods via the internet is a significant problem in Thailand, so much so that the Thai government is set on clarifiying the current legislation and increasing the power of rights holders with new provisions within the Draft Copyright Act. Nuttaphol Arammuang, Attorney-at-Law at Tilleke & Gibbins, discusses the current Computer Crimes Act and pending Copyright Act.

The Thai government is searching for new solutions to battle intellectual property infringement on the internet, both utilising existing laws and enacting new legislation. To this end, the Cabinet recently approved a draft of the proposed amendment of the Copyright Act which provides additional measures to copyright owners in combating online piracy.

The existing legal framework

Since existing IP laws in Thailand do not explicitly sanction the sale of counterfeit goods online, IP owners have, up until now, been unable to take aggressive action against these online sellers. In practice, IP owners have tried to tackle this type of infringement by conducting investigations to uncover the source of the fake goods, followed by raid actions under the current Trademark Act B.E. 2534, the Copyright Act B.E. 2537, and the Patent Act B.E. 2522.

This approach, however, is increasingly hampered by the fact that online traders do not typically store their goods on their premises. Instead, traders purchase the counterfeit products from sellers after receiving purchase orders from their customers.

The Computer Crimes Act

The Computer Crimes Act B.E. 2550 was enacted to provide legal sanctions against wrongful access to or 'hacking into' computer data. In searching for solutions to battle IP infringement online, recent meetings between government officials and members of the private sector have resulted in an innovative approach that relies on the existing Computer Crimes Act.

In the absence of specific legislation to address these activities, the DIP has suggested to IP owners that they may be able to enforce their rights by applying Sections 14 and 20 of the Computer Crimes Act.

Section 14

Whoever commits the following offences shall be liable for imprisonment for a term not exceeding five years, or a fine not exceeding THB 100,000, or both:

(1) Entering wholly or partially spurious computer data or false computer data into a computer system, in a manner that is likely to cause injury.

Section 20

In the case where the commission of an offence under this Act involves the distribution of computer data that may affect the security of the Kingdom, as prescribed in Book II, Title I or Title I/I of the Penal Code, which may be inconsistent with public order or good morals, the competent official may apply for a motion to the court to order that the distribution of such computer data be blocked.

In 2011, these sections were applied to a case related to food and medical products before Thailand's Criminal Court. In Red Case Sor. 33/2554, the defendant advertised the sale of food, medicine, and medical equipment using information that was deceptive to consumers. The court deemed this act an offence under Section 14(1) of the Computer Crimes Act, issuing an order to block the distribution activities undertaken by the website.

As this judgement shows, Sections 14 and 20 grant the court the authority to block the distribution of forged computer data or false computer data upon the request of an officer, if the court finds that such content may be inconsistent with public order or good morals. Unfortunately, the Computer Crimes Act is not clear in defining whether offering counterfeit goods for sale on a website can be considered 'forged computer data.' Although some government officials claim that this law sets out the right to take action against websites that offer fake goods for sale online, others opine that fake goods offered on a website cannot be deemed 'forged computer data.'

In seeking a solution to this problem, representatives from the Ministry of Information and Communication Technology (MICT), the DIP, and the private sector met in March 2012. The Director-General of the DIP stated that she encouraged IP representatives or IP owners to submit a formal letter to the MICT requesting to shut down these websites under Section 14. When an IP owner proceeds with a formal letter, this will provide a test case to determine whether Section 14 of the Computer Crimes Act can be used to shut down websites that offer fake goods for sale.

In light of these developments, a new procedure was proposed during the meetings. If all parties implement the new procedure, it could enable IP owners to shut down websites selling counterfeit or pirated goods in as little as two weeks. Clearly, this would be a major development for long-suffering IP owners who have battled online piracy for years.

Proposed amendment

In addition to the potential actions under the current Computer Crimes Act, IP owners can also look forward to new enforcement options under upcoming amendments to Thailand's copyright law.

On 9 October 2012, the Cabinet approved a proposed amendment of the Copyright Act (Draft Act), which had been presented for approval by the Council of State. The Draft Act provides additional provisions for the current Copyright Act, such as protecting information rights management and technological measures and empowering the court to order a person who infringes on a copyright or performers rights to pay damages in a higher amount, not to exceed double the amount. Among other things, the Draft Act provides additional measures for copyright owners to combat online piracy through the court system.

The Draft Act defines 'service provider' in the same terms as the Computer Crimes Act. According to the law, the term 'service provider' means: 1. A person who provides services to others regarding the provision of access to the internet or any other connectivity through a computer system, whether such services are provided in their own name or in the name or for the benefit of other persons. 2. A person who provides computer data storage services for others.

The Draft Act enables a copyright owner to file a motion requesting the court to order a service provider to suspend the alleged infringing act or temporarily remove the work allegedly made by copyright infringement from the system of the service provider.

Section 32/3 paragraph 1

In the case where there is evidence to believe that there is copyright infringement in a computer system of a service provider, the copyright owner may petition the court for cessation of such infringement.

This type of petition needs to clearly set forth specific information and evidence, as well as the relief requested. Once the court receives a petition, the court shall make inquiries. If the court views that it is appropriate to be permitted as requested, the court shall order the service provider to suspend the alleged infringing act or temporarily remove the work allegedly made by copyright infringement from the service provider's computer system, for a period of time specified by the court. The court order will be enforced immediately, and the service provider will be notified. In this case, the copyright owner has an obligation to initiate a lawsuit against the infringer within a period of time ordered by the court.

The Draft Act also prescribes exceptions for service providers who can prove that they did not have direct control of their computer system, did not commit the infringement themselves, or did not order anyone to commit the infringement. Also, the service will be free from any liability for the damages caused by complying with the court's order.

Section 32/3 paragraph 5

In the case where the service provider does not control or initiate copyright infringement and infringement of performers' rights in a computer system of the service provider, or cause someone to commit copyright infringement and infringement of performers' rights, and the service provider has complied with the court order under paragraph four, the service provider is not liable for the alleged infringing act that had been committed prior to the court order and after the court order terminates.

Section 32/3 paragraph 6

The service provider is not liable for any damage caused by any act done in compliance with the court order under paragraph four.

Pursuant to approval by the Cabinet, the Draft Act will be proposed to Parliament, which consists of the House of Representatives and the Senate, for further consideration and approval.

Although the debate regarding the application of the Computer Crimes Act on IP cases is ongoing and the Draft Copyright Act is still pending, it is evident that the Thai government intends to implement more stringent measures in the near future to inhibit the stream of illicit gains enjoyed by illegal online retailing operations.

Stringent measures

Although the debate regarding the application of the Computer Crimes Act on IP cases is ongoing and the Draft Copyright Act is still pending, it is evident that the Thai government intends to implement more stringent measures in the near future to inhibit the stream of illicit gains enjoyed by illegal online retailing operations.

At this stage, when an IP owner decides to test the approach proposed by the DIP and a court order is requested, practitioners will eagerly await the outcome for any developments in this area of the law. If the Computer Crimes Act is deemed practicable, it will provide an efficient route for IP owners to shut these websites down, without incurring additional investigation costs.

However, if the court decides that the activities of illegal online retailers specifically, offering counterfeit goods for sale on a website do not constitute 'forged computer data' under Section 14, it will then be necessary for all stakeholders to push ahead with further amendments to existing IP laws.

Nuttaphol Arammuang
Attorney-at-Law
Tilleke & Gibbins
nuttaphol.a@tilleke.com

The need for harmonised data retention regulation

Data security v. data privacy

As is well-known, law enforcement agencies throughout the world are pushing for laws more invasive that force Internet Service Providers (ISPs) and telecom providers to continuously collect and store data documenting the online activities of users. In turn, under a general point of view, data protection laws typically compel companies to limit the collection of personal information for a specific purpose (e.g. billing purposes), and to keep the data for only a specific period of time before destroying or anonymising it. Therefore, security requires retention and privacy fights against retention! But the main concern we can find is that we are still missing organic and harmonised regulation of data retention.

In this regard we can say that even the European Union (EU) has failed in such an intent. In fact, Directive 2006/24/EC - the so called 'Data Retention Directive' - which is the most prominent example of a mandatory data retention framework, instead of harmonising the EU internal market, has created a patchwork of national blanket retention legislation, significantly larger than what would have existed without the same Directive.

By means of the Data Retention Directive, the EU required Member States to enact laws in compliance with such a Directive, by requiring telecom companies to store a variety of data for six to 24 months. As a consequence, Member States have implemented such laws, most opting for the shorter time frames of six or 12 months. In Italy, for instance, the Legislative Decree 196/2003 - 'Italian Personal Data Protection Code' - opted for a data retention period equal to six months for billing purposes and 12 or 24 months for justice purposes (the latter referring to electronic communications traffic data and telephone traffic data).

However, although many countries have transposed the Data Retention Directive into their national legislation, the same Directive has met with stiff opposition, where Constitutional Courts, in some countries, have issued decisions striking down national data retention laws for violating human rights; those nations fighting the Data Retention Directive are Cyprus, the Czech Republic, Germany, Greece and Romania.

The reason why some EU Member States did not accept the Data Retention Directive's content is because mandatory data retention may create huge potential for abuse and could not then ensure the protection of individuals' rights and freedoms, presenting a serious risk of infringement.

Moreover, another concern to be taken into consideration are instances where data processing is carried out across more than one country, especially where one of those countries is located outside the EU. In other words, it is necessary to look to those situations where data flow may cross different geographic borders and jurisdictions. These situations mainly occur when a Data Controller avails itself of a cloud computing service.

As is well-known, we have entered into the cloud computing age, where personal data is increasingly being stored and transmitted across international borders by means of cloud infrastructures. As a consequence, the growth of cloud computing has inevitably multiplied the risk of personal data breach, by involving more cases of liability for Data Controllers.

In such a case, as explained above, concern is greatest where a part of the data processing is carried out in an EU Member State and, at the same time, another part of the same processing is carried out in a country outside the EU. For instance, the United States currently has no mandatory data retention law, but the government may obtain access to the stored data under the Stored Communication Act (SCA), enacted as part of the Electronic Communications Privacy Act. In fact, the SCA requires mandatory data preservation, requiring providers to preserve stored data for up to 180 days on government request. Therefore, what would be the applicable law, for instance, where the data collection occurs in Italy and its storage occurs in the US? To better understand the concern, it could be helpful to remember a concrete case that recently involved the Italian Data Protection Authority (the Garante). On 15 October 2010, the Garante issued an interesting decision on the Google Street View service, by means of which the Garante stated that it is not the relevant legislative force in the country where the data is transferred for storage purposes.

Having said that, it is evident that there are still outstanding issues with regard to data retention. In fact, as we have seen above, the main problem is that it is still missing an organic and harmonised data retention regulation, not only on a world-wide level, but on an EU level.

Although we know that this is a challenging project, which inevitably needs extensive cooperation of a large number of states around the world, our hope is that, sooner or later, a comprehensive regulation will be adopted that may overcome frictions existing in the data retention field. Such a regulation should establish the due and necessary balance between privacy and security, in order to avoid any possibility of infringing on individuals' rights and freedoms, by providing lawmakers, ISPs, users and any further parties involved with positive and definite rules. But at the same time, the regulation in question shall settle all contrasts inevitably existing between the laws of different states throughout the world and resulting from the possible application, in a concrete case, of more than one law.

Maybe, the comprehensive reform of the Directive 1995/46/EC proposed by the European Commission in January 2012, to strengthen online privacy rights and boost Europe's digital economy, could be the right opportunity to lay the foundations of an important change to privacy and data protection rules, even in the case of data retention.

Rocco Panetta Partner
Panetta & Associati
Studio Legale
r.panetta@panetta.net

Key e-commerce cases

Read the full reports in E-Commerce Law Reports Volume 12 Issue 6

Game cloning

Electronic Arts v. Zynga

EA accused Zynga of infringing its copyright in The Sims Social. EA contends that Zynga's The Ville, copies protectable elements of The Sims Social, achieved in part through Zynga's hiring of former EA executives who had access to proprietary information. EA claims the infringement includes, among other things, aspects of its character creation feature, the look and feel of the starter homes and choice of decorative elements, the characters' household activities and bodily needs, and the 'unique visual manner and style' in which characters socialise with each other.

Zynga hit back with a counterclaim against EA, alleging that EA improperly tried to stifle competition by forcing Zynga to stop hiring EA employees. Zynga also went on the offensive in its answer to EA's complaint, in which it takes the position that The Sims Social belongs to a 'longstanding and well-developed genre known as "life simulation" games.' Zynga goes on to allege in its answer that The Ville is merely the latest of Zynga's many life simulation games and that The Sims Social contains many of the same 'common functional elements' and *scenes a faire* as these games.

What does this mean for the ongoing litigation between EA and Zynga? Combined with the risk - for both sides - of allowing a court to determine whether the line between lawful copying and infringement has been crossed, it certainly seems less likely that this case will go the distance.

Jennifer Kelly Partner
Theis Finlev Associate
Fenwick & West LLP
JKelly@fenwick.com

Email ownership

Fairstar Heavy Transport v. Adkins and Claranet Ltd

Fairstar, a marine heavy transport company, obtained a court order restraining Mr Adkins from 'knowingly deleting or otherwise interfering with e-mails sent or received by Mr. Adkins whilst acting on behalf of Fairstar.' Mr Adkins was the former CEO of Fairstar.

Fairstar was the subject of a hostile takeover by one of its competitors, resulting in the termination of Mr Adkins' services. During his appointment by Fairstar it was alleged that all of Mr Adkins' emails were automatically forwarded from Fairstar's email server and deleted, which meant that they lost details crucial to a deal.

The application made by Fairstar before Mr Justice Edwards-Stuart was for an order that an independent expert be allowed to inspect the emails sent and received by Mr. Adkins. Fairstar's case was based solely on a proprietary interest in the content of the emails, on the basis that Fairstar was entitled to the content of the emails.

Edwards-Stuart J confined himself to dealing with the issue of whether 'Fairstar have a proprietary claim to the content of the emails held by Mr. Adkins (and/or Claranet) insofar as they were received or sent by Mr Adkins acting on behalf of Fairstar.'

Edward-Stuart J's judgement was that previous authority pointed strongly against there being a proprietary interest in information, and thus the content of emails, and he could find no practical basis for finding so. He would however 'not go so far as to say this area of law is settled.'

Dawn Osborne Partner
Scott Perry Paralegal
Palmer Biggs Legal
dawn.osborne@pblegal.co.uk

The Stored Communications Act

Jennings v. Broome

Mrs. Jennings believed that her husband was involved in an adulterous affair, and while he did not deny the affair, he would not identify the object of his affections. Mrs. Jennings then confided in Ms. Broome, who used to work for Mr. Jennings, and guessed the correct security screen answers to Mr. Jenning's email account and obtained the tell-all emails. Mr. Jennings then filed suit against Ms. Broome claiming that his email account had been accessed unlawfully under the federal Stored Communications Act.

The case came up to the South Carolina Supreme Court, which examined the sole question of whether Ms. Broome's actions in accessing Mr. Jennings's Yahoo! account without his authorisation constituted a violation of the federal Stored Communications Act.

A group of South Carolina Justices ultimately held that the Stored Communications Act offered Mr. Jennings no relief. Clearly, in this situation, Ms. Boome had intentionally accessed Mr. Jennings's account without authorisation and obtained access to his emails. However, the Court determined that the emails were not in 'electronic storage' within the meaning of the Act.

The extent to which the Stored Communications Act and other provisions of the broader Electronic Privacy Communication Act (EPCA) are outdated has led to very recent efforts to update the text to recognise both the changing technological world in which we now live, as well as evolved concepts of expected privacy rights in electronic communications.

Melinda Levitt Partner
Foley & Lardner LLP
MLevitt@foley.com