KIRKLAND & ELLIS
INTERNATIONAL

INTELLECTUAL PROPERTY
AND TECHNOLOGY

EUROPEAN UPDATE

IN THIS ISSUE:

Editor: Pierre-André Dubois
Authors:
Pierre-André Dubois
Joanna Shepherd
Kathleen McCallie

AUTUMN 2002

Welcome to Kirkland's *European Update*

We are pleased to present you with the first edition of a new Kirkland & Ellis publication, European IP Update. With our growing European-based IP and IT practices serving the needs of our clients in various fields, including software supply, e-commerce, financial services, telecommunications, and biotechnology, we want to provide our clients with timely and informative news on important legislative and judicial developments. Our European IP Update will attempt to cover a broad range of topics across Europe.

Depending on what developments we consider of interest to our clients, the focus of our European IP Update may vary from issue to issue. Our first issue reviews a number of developments in the fields of e-commerce and privacy, some of which are likely to force companies operating in Europe to change their business practices. We hope that you will enjoy reading our European IP Update.

Pierre-André Dubois

The EU's New Privacy and Electronic Communications Directive - Major Implications for E-Commerce and the Telecommunications Sector

With the European Union's ("EU") new Directive on privacy and electronic communications (2002/58/EC)(the "Directive") coming into force, the EU's position in relation to electronic communications and individual privacy has been, to a large extent, clarified. Although, on the face of it the Directive tries to find a compromise between an individual's right to privacy and established Internet and telecommunications business methods, the Directive creates a number of restrictions which will require most e-commerce and telecommunication providers to modify substantially their business practices. The precise way the Directive will be implemented in the national laws of each Member State will likely vary to some extent, and Member States have until 31 October 2003 to do so.

Cookies

The Directive limits the use of web bugs, hidden identifiers and other similar devices stored on a user's terminal (generally, but not limited to, "cookies"). This is likely to be one of the more controversial elements of the Directive (although the final text of the Directive did not adopt the original draconian proposal of rendering the use of cookies totally illegal). Although cookies may be used for legitimate purposes and are a useful tool for on-line businesses, enhancing the website experience, cookies also represent a potential invasion of a user's privacy.

The Directive takes a very protective approach restricting the use of cookies to circumstances where: (i) the user has been provided with clear and comprehensive information about the purposes for which the cookie is used, and the user has had

... the Directive creates a number of restrictions which will require most e-commerce and telecommunication providers to modify substantially their business practices.

the opportunity to refuse to have the cookie stored on their hard disk (i.e. "opt -out") before the cookie is served; or (ii) the use of the cookie is for the sole purpose of carrying out or facilitating the transmission of an electronic communication or in order to provide a service explicitly requested by the user. Although website providers may still make access to website content by a user conditional on the acceptance of a cookie,

website providers will need to ensure that they provide a sufficiently detailed explanation of the use of cookies and instigate an "opt-out" process allowing users to refuse to accept cookies.

This restriction on the use of cookies and the ability of users to "opt-out" may discourage some users in using certain websites and may deny on-line businesses a legitimate and useful tool in analyzing the effectiveness of their sites and advertising. Website operators will need to develop user-friendly policies with respect to their use of cookies which will provide all necessary information to the users, but, at the same time, reassure users that their consent to the use of cookies will not result in a massive invasion of their privacy. Some operators may therefore need to find a fine balance between collecting less data by way of cookies (hence, making their disclosure to users more attractive) and continuing to use their current technology (which, in certain cases, may scare users away as a result of the required disclosure).

Unsolicited commercial communications

Essentially the Directive only permits businesses to send unsolicited automated or electronic direct marketing communications or "spam" (such as faxes, e-mails and SMS messages) to recipients who have consented in advance to receive such communications (i.e. persons who have "opted-in"). However, businesses are permitted to use their customers' e-mail addresses to send their customers direct marketing e-mails in relation to that business' similar products and services provided that such customers are given a clear and distinct opportunity to object, free of charge and in an easy manner, to such use of their e-mail contact details when their e-mail contact details are collected and each time a direct-marketing e-mail is sent.

Companies relying on direct marketing by electronic means should make sure, pending implementation of the Directive, that they have on record consent from their customers who are receiving direct-marketing communications in connection with the goods and/or services such customers usually purchase or subscribe to.

Traffic and location data

The Directive also imposes stringent restrictions on the storage and use of traffic and location data. These restrictions will have significant impact on the way the telecommunications sector conducts its business. These restrictions are also likely to have an impact on web operators, web advertisers and those who provide or use tracking technologies. "Traffic data" is data processed to enable the sending, delivery and billing of communications and includes any naming, numbering or addressing information provided by the sender of the communication, data referring to the routing, duration and timing of a communication and the protocol used, whilst "location data" is data relating to the geographical location of the user's terminal equipment (for instance, the location of a user's mobile phone handset or an IP address).

Traffic data

Under the Directive, a service provider is only permitted to process (e.g. collect, store and/or use) traffic data to: (i) enable billing and inter-connection payments to be processed (in this case, the service provider may only process such data up to the end of the period during which a bill may lawfully be challenged or payment pursued, and, once this period has expired, the service provider must either delete or anonymize the data); and (ii) to the extent that such processing is necessary for the transmission of communications, detection of individual technical failures or errors in the transmission of a communication, and to detect and prevent fraud. In order to process the traffic data for any other purposes (such as electronic marketing and/or the provision of additional services), a service provider must obtain "informed consent" from the person to whom the traffic data relates (the "data subject") to the use of the data for the other purposes, and the data subject must be given the opportunity to withdraw their consent to the processing of the traffic data at any time.

In order to demonstrate that it has obtained "informed consent," the service provider must provide the data subject with full information in relation to the types of traffic data processed, the duration of the processing and the purposes for which the data is processed before obtaining consent. Furthermore, the service provider may only retain traffic data obtained with informed consent for the duration necessary for the provision of the additional services and/or marketing, and once the services and/or marketing have been provided, the service provider must erase the traffic data or render it anonymous.

Location data

The Directive applies even more stringent restrictions in relation to the processing of location data. A service provider is only permitted to process anonymized location data if the relevant user/subscriber has given informed consent to the extent and duration of the processing of such location data necessary for the provision of a service requested by him. Again, in order to obtain "informed consent," a service provider must inform users or subscribers, prior to obtaining their consent, of the type of location data that will be processed, the purposes and duration of the processing and whether the location data will be transmitted to a third party for the purpose of providing the services requested by the users/subscribers. Furthermore, the service provider must provide users/subscribers with: (i) the opportunity to withdraw their consent to the processing of location data at any time; and (ii) a simple and free-of-charge means of temporarily refusing the processing of location data for each connection to the network or transmission of a communication.

The restrictions around the processing of location data will most likely require many operators of e-commerce sites to change the way they operate or to clearly advise users that, for example, the user's IP address is being processed.

Under existing law, there was uncertainty in at least some EU countries whether an IP address would amount to personal data protected under data-protection laws. Clearly, this Directive now elevates IP addresses to the status of personal data.

It is worth mentioning that Member States may create exceptions by law to the restrictions on the processing of traffic and location data when necessary for national security, defense and the investigation of criminal offenses. Any such exceptions, however, will need to be appropriate and proportionate under the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Implications of the Directive

Although Member States are not obliged to enact the Directive into national laws until next year, it would be wise, in light of the stringent protections in the Directive for those in the telecommunications and e-commerce sectors who trade in the EU to begin to reflect the requirements of the Directive in the operation of their businesses. In particular, the design of communication networks and systems should limit the amount of personal data processed to that strictly necessary for billing unless the service provider has or is planning to obtain informed consent from a data subject. Furthermore, service providers should ensure that any activities (other than provision of the communication service and billing) are based on anonymized aggregated location data. All web operators should examine their current practices with respect to cookies and consider whether changes need to be made to the operation of their sites and start to develop opt-out policies. Finally, all companies relying on direct marketing should immediately examine their customer database to see what consents have been obtained historically.

United Kingdom ISPs Face Significant Duties and Costs Under New RIPA Order

United Kingdom internet service providers ("ISPs") are now required to maintain specific communication and data interception capabilities so that they are able to comply with e-mail and other communication interception warrants issued by law enforcement authorities. This is because the Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 (the "Order") came into force as of 1 August 2002. The Order provides crucial details lacking in the United Kingdom's controversial Regulation of Investigatory Powers Act 2000 (the "RIPA") as to ISPs' obligations to provide "reasonable assistance" to United Kingdom law-enforcement authorities in effecting warrants to intercept e-mail messages and other communications. However, while the Order clarifies ISPs' interception duties under the RIPA, it also imposes potentially significant financial and organizational costs.

Interception Capability Requirements Spelled Out

United Kingdom-based ISPs, subject to the limited exceptions noted below, are required under the Order to:

- maintain a mechanism for implementing communication interceptions within one working day of being informed that an interception warrant has been appropriately authorized;
- intercept all communications and related data authorized by an interception warrant and make near real-time transmission of same to the law enforcement agency that issued the warrant;
- ensure that the intercepted communication and related data can be correlated;
- ensure that the communication hand-over interface they provide to law enforcement agencies complies with any requirements stated by the Secretary of State;
- ensure that, "where reasonable," appropriate filtering technology is provided so that only the traffic data associated with the relevant account is intercepted;
- ensure interception capability reliability at least equal to their overall reliability;
- ensure that the intercept capabilities are auditable in order to confirm that intercepted communications and related data are actually from, or intended for, the subject being investigated (or originate from, or are intended to be transmitted to, the premises named in the applicable warrant); and

... it is unclear whether certain sections of the RIPA actually comply with the European Convention on Human Rights and the Data Protection Act 1998.

- comply with all the above obligations in a manner that minimizes the chances that the person whose communications are being intercepted (or other unauthorized persons) becomes aware of the interception.

ISPs are exempt from the above requirements only if they do not provide (or do not intend to provide) their services to over 10,000 users in the United Kingdom, or if their services are limited to the banking, insurance, investment or other financial services sectors.

Failure to comply with these obligations carries civil penalties. However, where an ISP believes that an interception warrant is too extensive or costly to comply with, it may refer the matter for review by the National Technical Advisory Board. This is a body established by the RIPA and made up of industry and Government representatives.

Potentially Enormous Cost and Operational Consequences

The obligations mandated by the Order will necessitate substantial investment by ISPs in specialized software, hardware, staff-training programs and new to company policies. The RIPA requires the Secretary of State to ensure that United Kingdom ISPs receive a "fair contribution" to offset the costs of complying with interception warrants or maintaining intercept capability. However, the RIPA itself is vague on what a "fair contribution" is; certainly, it will not entirely compensate ISPs for costs incurred in complying with their obligations under the Order or the RIPA generally.

A Government-sponsored report estimated that large ISPs could spend over £1,000,000 implementing interception capability frameworks, which are only one portion of the obligations imposed by the RIPA. This cost estimate has been criticized by some as being too low: a report issued by the British Chambers of Commerce estimated that ISPs' interception framework ongoing costs could range from between £3,500,000 and £12,000,000 per annum due to necessary reinvestment as ISPs networks evolve. Evidence that RIPA compliance costs could be far higher than initially anticipated may be borne out by the fact that the Government set aside £20,000,000 for communications service-provider expenses due to RIPA obligations for the years 2001 to 2004 — yet £14,000,000 of that support was spent in just 2001 alone, before the Order even came into effect.

Prior to the RIPA's passage, a number of United Kingdom ISPs threatened to move their e-mail servers overseas to less restrictive jurisdictions in order to avoid this law. Other United Kingdom-based ISPs are considering emerging anonymising and encryption services to avoid RIPA obligations. Some ISPs and other organizations also argue that it is unclear whether certain sections of the RIPA actually comply with the European Convention on Human Rights and the Data Protection Act 1998. It remains to be seen whether any of these strategies and arguments will be effective, legally viable or commercially practical. One has to remember that, while a proportionality test will be applied by a court assessing the validity of the RIPA or the Order, protection of civil liberties under European and UK law can be overridden by national security and criminal investigation requirements, hence providing some justification for the Order.

Liability of Intermediary Service Providers Finally Clarified in the UK

With the coming into force on 21 August 2002, of the Electronic Commerce (EC Directive) Regulations 2002 (the "Regulations"), the civil and criminal liability in the United Kingdom of intermediary service providers ("ISPs") (which would include any operator of a website having an establishment or place of business in the United Kingdom) has been, to a large extent, clarified. While one will have to await decisions from the courts on the precise interpretation of the Regulations, ISPs can already take comfort from the Regulations that, in many cases, it will now be difficult for them to be found liable for unlawful materials published as a result of most transmission and hosting activities.

Transmission

Where an ISP plays a passive role as a mere conduit of information for content providers or as a provider of access to a communications network, the ISP will not be liable in damages or for criminal offences as a result of a transmission where it did not:

(a) initiate the transmission;

(b) select the receiver of the transmission; and

(c) select or modify the information contained in the transmission.

... one of the key tests is whether the ISP has "actual knowledge" of the alleged unlawful materials or activities.

Transmissions automatically initiated by an ISP at the request of a recipient of a service will not count as the initiation of a transmission. Similarly, a transmission selected as an automatic response to a request from the recipient of the service (e.g. a user's request to have an e-mail forwarded to a mailing-list broker) will not count as selection of the receiver of a transmission. Finally, manipulations of a technical nature that take place in the course of transmission (e.g. the automatic addition of headers to e-mails) do not count as selection or modification of the information provided that the integrity of the information contained in the transmission is not altered.

Hosting

Similarly, when an ISP is providing hosting services, the ISP will not be liable in damages or for criminal offences as a result of such hosting where:

(i) the ISP does not have actual knowledge that an activity or information was unlawful and is not aware of any circumstances or facts from which it would have been apparent to the ISP that the activity or information was unlawful; or

(ii) upon obtaining such knowledge or awareness, the ISP acts expeditiously to remove or disable access to the information; or

(iii) the recipient of the service was not acting under the authority or control of the ISP.

In order to avoid liability, one of the key tests is whether the ISP has "actual knowledge" of the alleged unlawful materials or activities. What will constitute "actual knowledge" will be a question of fact to be decided in each case. However, in order to be able to state that it did not have "actual knowledge," the ISP (who has an obligation under the Regulations to provide its contact information on its website or documents relating to its operation) must act on any notice received alleging that an unlawful activity has taken place. Once such notice has been received, the ISP should immediately take action to deal with the unlawful materials, for example, by pulling them down from the website. In a case decided by the English courts a few years ago under the Defamation Act 1996 (which contains provisions similar to those of the Regulations with respect to defamation), an English court found that an ISP was liable for defamation after the ISP had had several warnings about a message board containing some defamatory materials, but had failed to act on those warnings. An ISP does not, however, have an obligation to report the unlawful activities to the competent authorities or the owner of the relevant IP rights. However, depending on the nature of the illegal activity, a reporting obligation may arise under certain criminal statutes (for example, money laundering, or terrorist activities).

While the Regulations do not provide for a positive obligation on an ISP to monitor the contents of a website, it is advisable for ISPs to establish clear rules of conduct with respect to the operations of any chat rooms or message boards, as well as to monitor from time to time the contents of such sites so as to be able to react rapidly to any illegal materials posted on a site. Evidently, if in the course of monitoring a message board, an ISP discovers unlawful materials, it would then need to act diligently to prevent any loss of the defense set out in the Regulations as a result of deemed knowledge.

Caching

Where an ISP caches copies of the recipient of a service's information (for example, copies of a website) in the provision of the service, the ISP will not be liable in damages or for criminal offences when the caching is automatic, immediate, temporary and for the sole purpose of providing a more efficient service. However, this protection is subject to the satisfaction of a number of conditions, including that the ISP comply with conditions on access to the information. Furthermore, in order to obtain protection, ISPs must ensure that as soon as they have "actual knowledge" that the initial source of the information has been removed from the network or access to the information has been disabled, the information is then deleted from their caches.

One area which is not directly addressed by the Regulations, nor in current European Directives, is the activities of search engines and tools. This is an area which will require further legislative guidance. However, it is difficult to see how an ISP would be able to seek a defense based on the Regulations since most of the terms and conditions of most websites contain a notice precluding information from being stored in an electronic retrieval system. For the time being, the activities of search engines and tools will be subject to general principles of tort law (including the tort of trespass), as well as applicable principles of copyright and trademark law.

Community Patents - Still a Possibility?

On 30 August 2002, the European Commission moved further towards the implementation of the Community Patent by adopting a draft working document clarifying jurisdictional issues regarding the Community Patent. However, this positive step suffered a recent setback when the EU Council of Ministers for Competitiveness failed to agree on some of the legal issues surrounding the potential implementation of the Community Patent.

Currently in Europe, it is not possible for an applicant to obtain a single unitary patent covering the whole of the EU. Instead, in order to get patent protection in the EU, an applicant must obtain a bundle of national patent rights under either the European Patent Convention ("EPC") or the Patent Cooperation Treaty ("PCT").

An applicant can obtain patent protection under the EPC by filing a single application in a state party to the EPC designating the countries in which protection is sought. The United Kingdom and most other Western European countries are party to the EPC. Assuming the application proceeds to grant, the application would result in a European patent. Essentially, a European patent is a bundle of national patent rights in those countries designated, each national patent being subject to the national law of the relevant country. Alternatively, an applicant could file an application under the PCT in a state party to the PCT (currently the United Kingdom and 76 other countries), designating the countries in which protection is required. Again, assuming the application proceeds to grant, this would result in a bundle of national patent rights in those countries designated, each national patent being subject to the national law of the relevant country. As under both systems, a successful application results in a bundle of national patents. Where any validity and/or infringement issues arise, the patent holder has to deal with these on a country-by-country basis, incurring costly and time-consuming parallel litigation. Furthermore, as each country's national patent legislation and case law varies, it is quite common to find that a patent for a particular invention is valid and infringed in one country, but invalid and not infringed in another.

For a number of years, the EU has been considering implementing the so-called "Community Patent," a unitary patent that would cover all Member States of the EU and that would stand or fall for the whole of the EU. One of the EU's principal areas of concern in implementing the Community Patent is to ensure certainty and unity of the law relating the Community Patent and consistency of case law throughout the EU. The working document adopted by the Commission proposes a centralized EU jurisdiction for resolution of Community Patent validity and/or infringement issues with specialist patent courts to guarantee high-quality decisions through a quick, inexpensive and uniform procedure. The working document envisages the establishment of a first-instance judicial panel, the "Community Patent Court," composed of two legal members and one technical member. The Community Patent Court would have jurisdiction to deal with infringement and validity issues only; other legal issues, such as compulsory licenses, would fall under the jurisdiction of other EU courts. The working document also envisages that once a coherent body of case law on the interpretation and application of the Community Patent Regulation has been established, regional Community Patent Courts would be developed.

While the adoption of this working document by the European Commission represented a significant step towards the establishment of a Community Patent, interested parties will now need to await the further meeting of the EU Council of Ministers to see whether Member States will agree to a compromise following the disagreement at the last EU Council of Ministers for Competitiveness.

For more information visit www.kirkland.com or contact:

London
Pierre-André Dubois
Tel: +44 (0)20 7816 8830
pdubois@kirkland.com

Chicago
William A. Streff, Jr., P.C.
Tel: +1 312 861 2126
wstreff@kirkland.com

Gregg Kirchhoefer
Tel: +1 312 861 2177
gkirchhoefer@kirkland.com

Los Angeles
Robert G. Krupka, P.C.
Tel: +1 213 680 8456
rkrupka@kirkland.com

New York
Lisa A. Samenfeld
Tel: +1 212 446 4968
lsamenfeld@kirkland.com

San Francisco
Stephen P. H. Johnson
Tel: +1 415 439 1439
sjohnson@kirkland.com

Washington, D.C.
Edward C. Donovan
Tel: +1 202 879 5289
edonovan@kirkland.com