e-commercelaw&policy

FEATURED ARTICLE
09/09

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Disclosure of personal data for criminal investigations

A Belgian criminal court recently fined Yahoo! Inc. for failing to disclose the personal data of its email users - under criminal investigation for fraud - to the Belgian Public Prosecutor. Cedric Burton, an Associate at Hunton & Williams LLP, examines the difficulties multinational companies operating in several jurisdictions face, especially in Belgium, where the Code of Criminal Procedures requires that the operator of an e-communication company cooperate with the Public Prosecutor within the framework of a criminal investigation.

On 2 March, the Belgian Criminal Court of Termonde[1] fined Yahoo! Inc. (hereafter 'Yahoo') €55,000 for refusing to disclose to the Belgian Public Prosecutor the personal data of its e-mail users who were under criminal investigation for fraud. The Court also imposed a daily penalty of €10,000 for each day Yahoo refused to disclose the data. The case was immediately appealed by Yahoo on 3 March, and the appeal hearings are expected by the end of the year.

This case illustrates the difficulties that multinational companies active in several jurisdictions may face and the complex issue of applicable law. This analysis will:

- describe briefly the legal framework applicable to this type of situation in Belgium;
- examine the context, some of the arguments put forward by Yahoo and selected parts of the court's ruling; and
- provide the reader with some comments on the court's reasoning and companies faced with the same type of situation with some recommendations.

Legal framework

The Belgian Code of Criminal Procedures[2] requires that the operator of an electronic communication network or the provider of an electronic communication service (hereafter 'providers') cooperates with the Public Prosecutor within the framework of a criminal investigation. Following a written and justified[3] request from the Public Prosecutor, providers must grant access to their database in order to allow the Public Prosecutor to identify a subscriber or user suspected of criminal activities[4]. Likewise, the provider must disclose to the Public Prosecutor the data necessary to identify the subscriber or the user[5]. Refusal to disclose the data may be sanctioned by a fine ranging from €143 to €55,000.

Context of the case

Within the framework of an investigation for fraud, the Public Prosecutor of Termonde sought to obtain the disclosure of detailed account information in order to identify e-mail users using pseudonyms on their Yahoo e-mail accounts for the purpose of committing internet fraud in Belgium. The Public Prosecutor was seeking identification data, including the IP address, date of creation of the account, user profile and any other information which might help identify the e-mail user.

The Public Prosecutor's request was made via the regular channels of communication provided by Yahoo and in accordance with the guidelines mentioned in the help section of Yahoo's webpages, in particular the e-mail addresses provided on the website for inquiries about security. Following this request, some exchange of correspondence between Yahoo and the Public Prosecutor took place. In particular, Yahoo requested the demand to be written - this was complied with by the Public Prosecutor. However, and despite the Public Prosecutor's compliance with Yahoo's instructions, Yahoo still refused to disclose the requested information and to cooperate with the Public Prosecutor. Consequently, the Public Prosecutor referred the case to the Criminal Court of Termonde.

Trial and Yahoo's main arguments

During the trial, Yahoo first argued that the US Electronic Communications Privacy Act (hereafter ECPA), not Belgian law, was applicable. In Yahoo's opinion, Belgian law did not apply because

Yahoo has no legal entity in Belgium and does not store any customer data in Belgium. Therefore, following the reasoning of Yahoo, a request for access from a US judicial authority was necessary to obtain the identification data. According to Yahoo, the Public Prosecutor should have issued a formal request via the US Department of Justice in accordance with the procedures established by the Treaty on Mutual Legal Assistance on Criminal Matters signed between the United States and Belgium on 1 January 2000. Secondly, Yahoo challenged the applicability of Article 46bis of the Belgian Code of Criminal Procedures to the facts in issue. In Yahoo's opinion, supplying webmail services does not constitute the provision of electronic communication services or the operation of an electronic communication network as defined in the Belgian Electronic Communication Act.

Ruling of the case

Notwithstanding Yahoo's arguments, the Belgian Criminal Court held that Belgian law applied. It stated that even though the ECPA could apply, it did not prevent the application of Belgian Criminal Law, which is applicable to companies that are virtually present on Belgian territory via the internet, in particular when they provide virtual services to Belgian citizens. The Court considered that when a company engages in business on Belgian territory via the internet, it is virtually present on Belgian territory and therefore subject to Belgian criminal law. In the court's opinion, non-application of Belgian law to this case would render Belgian law ineffectual and allow companies to circumvent Belgian criminal law.

The Court also rejected Yahoo's argument that providing webmail services was not within the scope of Article 46bis of the Belgian Code of Criminal Procedures. The Court asserted that the definition of the Code of Criminal Procedures is independent from other legal provisions such as the Belgian Electronic Communication Act. In other words, following the Court's reasoning, Article 46bis must receive a 'stand-alone' interpretation. For that reason, Yahoo is considered by the Court to be a provider of electronic communication services and, as such, falls within the scope of Article 46bis of the Belgian Code of Criminal Procedures.

Yahoo's non-disclosure of the information requested by the Public Prosecutor was a violation of Article 46bis of the Belgian Code of Criminal Procedures

As a result, the Criminal Court of Termonde held that Yahoo's non-disclosure of the information requested by the Public Prosecutor was a violation of Article 46bis of the Belgian Code of Criminal Procedures, and fined Yahoo €55,000, with an additional penalty of €10,000 imposed on a daily basis for non-compliance with the court order. Yahoo immediately appealed the decision. The appeal hearings are expected before the end of 2009.

Comments

At least two aspects of the Court's reasoning can be challenged:

- the applicability of Belgian Criminal law; and
- the scope of Article 46bis of the Belgian Code of Criminal Procedures. First, regarding the applicability of Belgian Criminal Law, the criterion of 'virtual presence on the territory' used by the Belgian Court can be questioned. It may be argued that Yahoo does not really focus on the Belgian market. Yahoo's services are accessible to Belgian users but there is no specific Belgian site for Yahoo webmail (i.e., there is no 'Yahoo.be' webmail designating mail originating from Belgium), no Yahoo Belgian entity and no data stored in Belgium. Without solving the complex issue of applicable law, the criterion used by the Belgian Court seems open to criticism and will most likely be challenged on appeal.

Second, it is doubtful that Yahoo would be considered to be a provider of electronic communication services or an operator of electronic communication networks. With regards to the supplying of webmail accounts, Yahoo would most likely be considered to be an information society service provider[6] and not a provider or an operator of electronic communication services or network as defined in the Belgian Electronic Communication Act[7]. In sum, the reasoning of the Court is questionable and will be strongly challenged on appeal.

In any event, this case illustrates the complex relationship between the issue of applicable law and online activities, and the tendency of judges to apply their national rules when faced with criminal activities occurring on the internet. Traditionally, Belgian law is broadly applied to criminal activities whenever there is a link to Belgium. Belgian courts are also somewhat territorial and protective of their citizens and usually find themselves competent when a case is referred to them.

This case also illustrates the growing tensions between national laws and the global character of the internet. The internet creates important opportunities for businesses, in particular in terms of the number of individuals who can be reached via online services. It is an invaluable tool, but companies must be careful when offering services to individuals located in foreign countries. The opening of a website to the citizens of a foreign country can have far reaching

consequences, in particular when it comes to litigation, since this can potentially trigger the application of conflicting national law requirements.

Recommendations

Companies planning to offer online services to individuals in foreign countries should consider the question of applicable law, analyse the specific national legal requirements and define a strategy. To some extent, this aspect can be regulated in website terms of use and privacy notices. Nevertheless, some areas of law, in particular criminal law, may not be circumvented contractually and are not harmonised at the European level. As a result, companies may have to comply with every applicable national law requirement which, in turn, may create situations where companies are faced with a complex set of conflicting obligations.

A practical approach to this type of situation could be to mitigate the legal risks by developing, where possible, pan-European policies, and by using the highest standard or strictest requirement as a common denominator. Even though this approach could considerably reduce the legal risks, it will not solve all potential issues. Therefore, since neither the contractual nor pan-European/global approach is fully satisfactory, the only safe solution for companies might be to limit the number of individuals who can access their online services by using technical means (e.g., scroll-down menu with a restricted list of countries, using a credit card number, a zip code, or a declaration 'sur l'honneur'). Even if none of these technical requirements is flawless, they will significantly reduce the legal risks.

In any event, regardless of the applicable law, it is recommended that companies follow up on requests (from data subjects, authorities or a public prosecutor's office) made via the various communications channels provided on their websites. To achieve this goal, appropriate policies and procedures should be developed and implemented within the company. For example, companies should consider implementing procedures that ensure that questions, requests and concerns are actually dealt with. In addition, under Belgian law, providers of electronic communication services and operators of electronic communication networks are legally required to designate someone responsible for handling such requests from the Public Prosecutor. It may also be advisable to implement additional measures depending on the technical set-up of the service and of the company. In any case, it is crucial that the measures outlined above are coordinated closely between the legal and IT departments to ensure their smooth implementation.

Cédric Burton Associate
Hunton & Williams LLP, Brussels
c.burton@hunton.com

This article is not to be taken as legal advice and represents only the views of its author.

1. Tribunal correctionnel de Termonde, No. DE 20.95.16/08/25, available upon request to the Public Prosecutor.
2. Code belge d'instruction criminelle.
3. The written request must be justified owing to the proportionality obligation with regard to a data subject's privacy underlying any investigation.
4. Article 46bis §1 of the Criminal Code.
5. Article 46bis §2 of the Belgian Code of Criminal Procedures.
6. See the e-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market) and its implementation into Belgian law: article 2, 1° of the Belgian e-Commerce Act - Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, M.B., 17 mars 2003.
7. Loi du 13 juin 2005 relative aux communications électroniques, M.B., 20 juin 2005.

cecile park publishing

Head Office UK Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
tel +44 (0)20 7012 1380 fax +44 (0)20 7729 6093 info@e-comlaw.com
www.e-comlaw.com

Registered number 2676976 Registered address 141 Wardour Street, London W1F 0UT VAT registration 577806103

e-commerce law & policy

Many leading companies, including Amazon, BT, eBay, FSA, Orange, Vodafone, Standard Life, and Microsoft have subscribed to ECLP to aid them in solving the business and legal issues they face online.
ECLP, was nominated in 2000 and again in 2004 for the British & Irish Association of Law Librarian's Legal Publication of the Year.
A twelve month subscription is £420 (overseas £440) for twelve issues and includes single user access to our online database.

e-commerce law reports

You can now find in one place all the key cases, with analysis and comment, that affect online, mobile and interactive business. ECLR tracks cases and regulatory adjudications from around the world.
Leading organisations, including Clifford Chance, Herbert Smith, Baker & McKenzie, Hammonds, Coudert Brothers, Orange and Royal Mail are subscribers.
A twelve month subscription is £420 (overseas £440) for six issues and includes single user access to our online database.

data protection law & policy

You can now find in one place the most practical analysis, and advice, on how to address the many problems - and some opportunities - thrown up by data protection and freedom of information legislation.
DPLP's monthly reports update an online archive, which is an invaluable research tool for all those who are involved in data protection. Data acquisition, SMS marketing, subject access, Freedom of Information, data retention, use of CCTV, data sharing and data transfer abroad are all subjects that have featured recently.
Leading organisations, including the Office of the Information Commissioner, Allen & Overy, Hammonds, Lovells, BT, Orange, West Berkshire Council, McCann Fitzgerald, Devon County Council and Experian are subscribers.
A twelve month subscription is £390 (public sector £285, overseas £410) for twelve issues and includes single user access to our online database.

world online gambling law report

You can now find in one place analysis of the key legal, financial and regulatory issues facing all those involved in online gambling and practical advice on how to address them. The monthly reports update an online archive, which is an invaluable research tool for all those involved in online gambling.
Poker, payment systems, white labelling, jurisdiction, betting exchanges, regulation, testing, interactive TV and mobile gaming are all subjects that have featured in WOGLR recently.
Leading organisations, including Ladbrokes, William Hill, Coral, Sportingbet, BskyB, DCMS, PMU, Orange and Clifford Chance are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

world sports law report

WSLR tracks the latest developments from insolvency rules in football, to EU Competition policy on the sale of media rights, to doping and probity. The monthly reports update an online archive, which is an invaluable research tool for all involved in sport.
Database rights, sponsorship, guerilla marketing, the Court of Arbitration in Sport, sports agents, image rights, jurisdiction,domain names,ticketing and privacy are subjects that have featured in WSLR recently.
Leading organisations, including the England & Wales Cricket Board, the British Horse Board, Hammonds, Fladgate Fielder, Clarke Willmott and Skadden Arps Meagre & Flom are subscribers.
A twelve month subscription is £520 (overseas £540) for twelve issues and includes single user access to our online database.

priority order form

FAX +44 (0)20 7729 6093
CALL +44 (0)20 7012 1380
EMAIL dan.towse@e-comlaw.com
ONLINE www.e-comlaw.com
POST Cecile Park Publishing 17 The Timber Yard, Drysdale Street, London N1 6ND

☐ Please enrol me as a subscriber to **e-commerce law & policy** at £420 (overseas £440)
☐ Please enrol me as a subscriber to **e-commerce law reports** at £320 (overseas £440)
☐ Please enrol me as a subscriber to **data protection law & policy** at £390 (public sector £285, overseas £410)
☐ Please enrol me as a subscriber to **world online gambling law report** at £520 (overseas £540)
☐ Please enrol me as a subscriber to **world sports law report** at £520 (overseas £540)

All subscriptions last for one year. You will be contacted at the end of that period to renew your subscription.

Name			
Job Title			
Department		Company	
Address			
Address			
City		State	
Country		Postcode	
Telephone		Fax	
Email			

1
Please **invoice me** Purchase order number
Signature Date

2
I enclose a **cheque** for the amount of
made payable to *'Cecile Park Publishing Limited'*

3
Please debit my **credit card** VISA ☐ MASTERCARD ☐
Card No. Expiry Date
Signature Date
VAT No. (if ordering from an EC country)

Periodically we may allow companies, whose products or services might be of interest, to send you information.
Please tick here if you would like to hear from other companies about products or services that may add value to your subscription. ☐