crowell moring

CLIENT ALERT

European TMT & Privacy Bulletin - October 2013

Oct.15.2013

Sections of this issue:

ISP Liability and Media Law

Electronic Communications & IT

Privacy & Data Protection

ISP LIABILITY AND MEDIA LAW

Belgian Copyright Collecting Society SABAM Claims Copyright Levy from Internet Access Providers

Belgian copyright collecting society SABAM claims 3.4 percent of the country's largest Internet access providers' subscription fees. According to SABAM, enabling subscribers to access the Internet and transmit copyright-protected content over the Internet qualifies as a communication to the public within the meaning of copyright legislation. IAPs should therefore pay a copyright levy, SABAM states. It lodged legal proceedings with the Brussels court of first instance to enforce this claim. SABAM's claim is highly contested, not only by the Internet Service Providers Association ISPA but also by the Belgian Ministry for the Economy and by legal commentators.

1) SABAM, the Belgian collecting society for copyrights, claims 3.4 percent of the subscription fees of Belgium's largest IAPs to compensate for their role in enabling their subscribers to access the Internet and use it to share copyright-protected content.

In a press release, SABAM justifies its claim by stating that the IAPs' Internet subscriptions are partly used by subscribers to make use of its protected repertoire. In SABAM's reasoning, part of the IAPs' profit must therefore be transferred to SABAM.

SABAM also refers to recent case law from the EU Court of Justice. According to Sabam the ECJ expanded the notion of "communication to the public" of copyright protected works in the *Airfield* and *Premier League* cases. The IAPs' transmission of copyright protected content over their networks, on behalf of their subscribers, would qualify as a communication to the public.

2) As several years of discussions with the IAPs did not result in an agreement over this so-called "Internet Tax," SABAM now initiated legal proceedings with the Brussels court of first instance against Telenet, Belgacom, Tecteo and Brutele (VOO).

However, the Belgian Ministry for the Economy already made it very clear that it objects to a copyright levy by IAPs as sought by SABAM. The Ministry even initiated a warning procedure against SABAM under article 77 of the Belgian Copyright Act. SABAM's efforts to contest this failed, both in summary proceedings and in proceedings on the merits.

3) SABAM's claim to impose a copyright levy upon IAPs is highly disputed, not only by the Belgian government, but also by legal commentators and the Internet Service Providers Association ISPA.

Indeed, EU Directive 2000/31/EC on Electronic Commerce clearly exempts IAPs offering mere conduit services, i.e. the transmission of information provided by a subscriber or the provision of access to a communication network, from liability for the content transmitted through their network. Seeking a copyright levy from IAPs in circumstances where they do not initiate the transmission of the content, do not select or modify the content and do not select the receiver thereof, would be contrary to this exemption of liability.

4) It is nevertheless possible that this case will lead to another referral for a preliminary ruling to the EU Court of Justice. However, it seems in any event doubtful that SABAM will find in this approach a new stream of income.

For more information, contact: Karel Janssens

ISP LIABILITY AND MEDIA LAW

Connected Continent Proposal of the European Commission

On 11 September 2013, the European Commission (Commission) announced its intention to take a new step towards a European single market for electronic communications by adopting the Proposal for a Regulation laying down measures concerning the European single market for electronic communications and to achieve a Connected Continent. The plan for a Connected Continent was launched by Commission President Barroso in his 2013 State of the Union speech.

The proposed regulation firstly intends to make it easier for companies to invest in new networks or services and to expand their services across borders. In this light, the Commission proposes a one-stop-shop solution, allowing European electronic communication providers to operate in all Member States with a single authorization granted by the national regulatory authority of one of the member states.

The proposal also provides for the coordination of the use of radio spectrum to ensure more 4G mobile access and Wi-Fi. While the Member States would remain in charge of spectrum allocation, the proposal wants to create a more coherent framework to instigate the emergence of integrated multi-territorial networks and services. It does however not create a pan-European spectrum license. The proposal lists criteria and conditions that have to be taken into account by the national authorities granting spectrum licenses. It also harmonizes certain authorization conditions, such as the duration of the rights of use, and takes a careful step at coordinating the authorization procedures.

Another aspect of the proposed package is the encouragement of competition between companies by providing standardized wholesale products. It is more specifically aimed at the introduction of a standardized European virtual broadband access product and a European Assured Service Quality connectivity product. The goal hereof is to expand the business-to-business market by facilitating market entry and the provision of cross-border services.

The proposal also claims to be strengthening net neutrality in the EU, namely the right to full and open internet. It is aimed at guaranteeing speed and quality for the internet. However, the proposal does not exclude that companies differentiate their offers and compete on enhanced quality of service when this does not impair the quality of the open internet. Hence, it is uncertain whether the net neutrality proposals will require major adjustments to current network management practices.

Furthermore, the proposal introduces new EU-wide consumer rights. Unlike in the current Universal Service Directive, that only provides minimums and options, these rights would be harmonized across Europe and directly enforceable. The proposal prescribes, inter alia, transparency obligations regarding contract information, and provisions aimed at facilitating switching between suppliers.

Lastly, the proposal also targets roaming premiums, building on the 2012 Roaming Regulation that already subjected operators to wholesale price cuts. For incoming calls, the proposal intends to ban charges as of 1 July 2014. Companies could choose to offer phone plans that apply in all Member States at a price driven by domestic competition, so called 'Roam Like At Home.' In that case they would be largely free of European regulation. If they do not, customers will have the right to opt to take roaming services from a cheaper local company or a rival company in their home country that offers cheaper roaming rates. This complete ban of roaming premiums does not apply for outgoing calls. As for fixed calls made to another EU country, the proposal states the companies cannot charge more than they do for long-distance domestic calls. For mobile calls, the limit is set at € 0,19 per minute (plus VAT).

The proposal now has to be approved, but the road towards this approval seems long and difficult. The proposal has been received with mixed reactions, including rather negative reactions of Members of the European Parliament. The governments of the Member States also still have an opportunity to make amendments. On top of this all, the EU lawmakers are under time pressure since the elections for the EU Parliament will be held in May 2014. During the Commission's presentation of the proposal in the European Parliament on September 11 it however already became clear that it is unlikely that the law will be adopted before the elections.

For more information, contact: Emmelie Wijckmans

ELECTRONIC COMMUNICATIONS & IT

Belgium Implements EU Data Retention Directive

With the Act of July 30, 2013 and the Royal Decree of September 19, 2013, Belgium (finally) implemented the EU Data Retention Directive of March 15, 2006 (Directive 2006/24/EC). The Belgian legislation, however, imposes more far-reaching obligations upon telecom operators and its entry into force does not go unnoticed.

Background

1) Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive) requires telecom operators to retain traffic and location data for various services in order to serve the investigation, detection and prosecution of serious crime.

2) In Belgium, article 126 of the Act of June 13, 2005 on Electronic Communication (hereafter "AEC") forms the legal basis for telecom operators' data retention obligations. Although member states had to implement the Data Retention Directive by September 15, 2007 (to be postponed to March 15, 2009 with respect to Internet services), it was only with the Act of July 30, 2013 that the Belgian government modified article 126 and (partially) implemented the Data Retention Directive. With the Royal Decree of September 19, 2013, implementing article 126 AEC, Belgium completed its implementation of the Data Retention Directive.

Data to be retained

3) In accordance with the Royal Decree of September 19, 2013, the following data must be retained:

a) Providers of public **fixed telephony services** (and providers of the underlying public electronic communication networks) retain the following data:

- Data necessary to identify the user, his communication equipment and the communication service used:
  - the number allocated to the user;
  - the user's personal data;
  - the subscription's starting date or the registration date;
  - the type of fixed telephony service used and the types of other services to which the user is registered;
  - in case of number transfer, the identity of the transferring provider and of the receiving provider;
  - the data relating to the payment method, the instrument of payment and the time of payment of the subscription fee or for the use of the service.

- Traffic and location data:
  - the calling number and the number called;

- the location of the network connection point of the calling party and of the called party;
- the identification of all lines in case of group calls, call forwarding or call transfer;
- date and time of the start and end of the call;
- description of the telephony service used;

b) Providers of public **mobile telephony services**(and providers of the underlying public electronic communication networks) retain the following data:

- Data necessary to identify the user, his communication equipment and the electronic communication service used:
  - the number allocated to the user and his International Mobile Subscriber Identity (IMSI);
  - the user's personal data;
  - the date and location of the user's registration or subscription;
  - the date and time of the first activation of the service and the cell ID from which the service is activated;
  - the additional services to which the user has subscribed;
  - in case of number transfer, the identity of the transferring provider;
  - the data relating to the payment method, the instrument of payment and the time of payment of the subscription fee or for the use of the service.
  - The ID number of the user's mobile equipment (IMEI);

- Traffic and location data:
  - the telephone number of the calling party and of the called party;
  - the identification of all lines in case of group calls, call forwarding or call transfer;
  - the IMSI of the calling and called participants;
  - the IMEI of the mobile equipment of the calling and called participants;
  - the date and time of the start and end of the call;
  - the location of the network connection point at the start and the end of each connection;
  - the identification data of the geographic location of cells at the time of connection;
  - the technical characteristics of the telephony service used.

c) Providers of public **Internet access services**(and providers of the underlying public electronic communication networks) retain the following data:

- Data necessary to identify the user, his communication equipment and the electronic communication service used:
  - the user ID allocated;
  - the user's personal data;
  - the date and time of the user's registration or subscription;
  - the IP-address, source port and network connection point of the connection used for subscribing or registering the user;
  - the additional services to which the user has subscribed with the provider concerned;
  - the data relating to the payment method, the instrument of payment and the time of payment of the subscription fee or for the use of the service

- Traffic and location data:
  - the user's ID;
  - the IP-address;
  - in case of shared use of an IP-address, the ports allocated to the IP-address and the date and time of allocation;
  - the identification and location of the network connection point used when logging-in and logging-off;
  - date and time of an Internet access service session's log-in and log-off;
  - the data volume up- and downloaded during a session;
  - data necessary to identify the geographic location of cells at the time of the connection;

d) Providers of public **Internet email services** and providers of **Internet telephony services**(and providers of the underlying public electronic communication networks) retain the following data:

- Data necessary to identify the user, his communication equipment and the electronic communication service used:
  - the user ID;
  - the user's personal data;
  - the date and time of creation of the email or Internet telephony account;
  - the IP-address and source port used for the creation of the email or Internet telephony account;
  - the data relating to the payment method, the instrument of payment and the time of payment of the subscription fee or for the use of the service.

- Traffic and location data:
  - the user's ID relating to the email or Internet telephony account, including the number or ID code of the intended recipient of the communication;
  - the telephone number allocated to each communication entering the telephony network in the framework of an Internet telephony service;
  - the IP-address and the source port used by the user;
  - the IP-address and the source port used by the addressee;
  - the date and time of the log-in and log-off of a session of the email service or Internet telephony service;
  - the date and time of a connection made by means of the Internet telephony account;
  - the technical characteristics of the service used;

4) The data necessary to identify the user, his communication equipment and the electronic communication service used must be retained as from the date of subscription to the service, for as long as incoming or outgoing communication is possible by means of the service and for a period of **12 months** from the date of the last incoming or outgoing communication.

Traffic data and location data must be retained for a period of **12 months** from the date of the communication.

5) Furthermore, it is important to note that no data revealing the content of the communication may be retained pursuant to this legislation.

Criticism

6) The Royal Decree of September 19, 2013 imposes more far-reaching obligations upon telecom operators compared to the EU Data Retention Directive, since (much) more data need to be retained.

The Ministers responsible for drafting the decree justify its scope by referring to the period elapsed since the adoption of the Data Retention Directive in 2006 and the fast evolving technological developments, increasing the need for data by the judicial authorities.

7) However, both privacy and human rights organizations oppose to the new legislation. The Belgian Privacy Commission announced it will assess the legality of the Royal Decree in view of the Data Retention Directive and, if necessary, take further steps.

Moreover, the legality of the Data Retention Directive itself is under discussion, as several references for preliminary ruling are currently pending before the EU Court of Justice (cf. cases C-293/12, C-594/52 and C-46/13).

For more information, contact: Karel Janssens

PRIVACY & DATA PROTECTION

Will We Have a New EU Data Protection Regulation in 2014?

In January 2012, the European Commission published its proposal for a general Regulation on data protection, which would apply directly in all EU Member States (see our newsletters from February 28, 2012, July 12, 2012, and January 22, 2013). The new Regulation should replace the current Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the various national laws implementing this Directive.

The Commission's proposal meanwhile has been extensively discussed within the European Parliament and the Council, thousands of suggested amendments to the original text have been made and lobbyists and interest groups are working overtime.

The vote within the LIBE committee, the European Parliament's lead committee for the proposed Regulation, has already been postponed twice and is now expected to take place on October 21, 2013. This vote is a condition for negotiations to start between the European Parliament and the Council. As there are still many key issues that are under discussion, these negotiations promise to be difficult and lengthy.

Hence, whereas under the current timetable it is still the intention to adopt the new Regulation prior to the EU Parliament elections to be held in May 2014, there is an increasing concern about the delays to implementation.

Political pressure in order to get the Regulation voted before these elections in May 2014 is now increasing. On September 18, 2013, for instance, Viviane Reding, vice-president of the European Commission and EU commissioner for justice, tweeted: "*It's time political leaders showed determination + adopted the Data Protection Regulation - Europe's citizens deserve nothing less*." The weeks and months to come will therefore be very important.

However, whereas everyone agrees that the current legal framework, mainly based on a 1995 Directive, is no longer adapted to the needs of the digital economy, one should not forget that this existing legislation is still in place and that in certain areas more recent legislation exists (e.g. e-commerce Directive). Moreover, if the new Regulation will be voted before the 2014 EU Parliament elections, it will only sort its effects in 2016. If it is not voted by then, the decision making process will start again after the elections and the newly elected bodies will not be bound by the results of the current negotiations, which means that there will be additional delays of several months, if not years.

The current legal framework and the various national data protection laws may therefore be in place for many more years to come. Hence, whereas companies should definitively start thinking about how they will deal with the new Regulation, they should meanwhile not forget about their obligations under the current legislation.

This is in particular true because national data protection authorities (DPA's) - in those countries where they have the power to do so - do not hesitate to enforce the rules. Even when under the current legal framework, these enforcement measures do not – contrary to what will be the case under the Regulation – result in heavy fines, the adverse publicity caused by media attention, should make companies act carefully. Recent events such as the NSA's Prism program have made privacy and data protection an increasingly important topic in the media.

Some recent decisions illustrate this perfectly.

Belgium

NMBS Europe (international branch of the Belgian national railways)

Issue: Data breach - When cleaning out the data in the customer lists of the online sales department and the lists of the call center of NMBS Europe, personal data of at least 700.000 customers of NMBS Europe was temporarily transferred from a secure environment to an unsecure environment. This made the personal data available on the website of NMBS Europe via Google.

The personal data concerned names, addresses, date of birth, sex, mother tongue, e-mail addresses and (mobile) phone numbers of individuals who had requested information or who had purchased train tickets. The list apparently also included ministers, officials of the EU commission and personnel of several embassies.

The issue became public in December 2012, but the breach occurred in May 2012 already, so that the data had been available over the internet for more than eight months. Only when a blogger made the news public in December 2012, did the NMBS react.

More than 1.700 individuals filed a complaint with the Belgian DPA.

This data breach, one of the biggest of its kind in Belgium, received a lot of media attention, not only with respect to the breach itself but also with respect to the poor way in which the NMBS responded to these events.

Actions of the DPA: The Belgian DPA investigated the matter and decided that the NMBS had infringed the Belgian data protection act (insufficient level of security and violation of the obligation of a fair and lawful processing).

The Belgian DPA, which itself cannot impose sanctions, transferred the file to the office of the public prosecutor in accordance with article 32 of the Belgian Privacy Act. The public prosecutor will decide whether or not there will be a criminal prosecution.

Following this and some other recent data breaches, the Belgian DPA has published a recommendation on Information Security on January 21, 2013 (available in Dutch and French here).

The Netherlands

Data analysis by mobile operators

Issue: The four largest mobile network operators in the Netherlands - KPN, Tele2, T-Mobile and Vodafone - analyzed data traffic (packet inspection) on the mobile network.

Actions of the DPA: The DPA investigated the matter and in its reports of May/June 2013, the DPA confirmed the existence of violations of the Dutch Data Protection Act and of the Telecommunications Act by all four operators. The mobile operators were found to have stored detailed data about websites visited and apps used, in breach of the law. The DPA also concluded that, customers were not, or incorrectly, informed about the processing of such detailed information and the purpose thereof, in breach of the Data Protection Act.

Some of the established infringements have meanwhile stopped. The Dutch DPA will verify to what extent some established violations are still on-going and decide whether it will take enforcement measures.

Healthcare institutions and access to patient data

Issue: In 2011 and 2012, the DPA received signals about an alleged broad access to digital patient files by workers of healthcare institutions.

Actions of the DPA: The DPA initiated an investigation with nine healthcare institutions on the way workers could access the digital patient files. In its June 2013 report, the DPA announced that at none of the healthcare institutions concerned the access to digital patient files was organized in such a way that it would be limited to persons treating the patient or for whom access was necessary for the treatment. None of the institutions concerned were therefore in compliance with article 13 of the Data Protection Act.

The healthcare institutions have provided an action plan to the DPA in order to become compliant and the DPA is in contact with them on the timing for compliance. The DPA will take sanctions if the road to compliance takes too long.

France

Access request - Equipement Nord Picardie

Issue: An employee invoked his right to access the personal data (in particular geo-localization data) processed about him by his employer, the Société Equipement Nord Picardie. The latter, however, refused to provide a copy of the personal data that it processes (offering the employee to come and see the data at the premises). Moreover, the employer did not to cooperate with the DPA when it sent a notice of default, in which it asked to communicate the data concerned and also to communicate to the DPA the procedures put in place by the employer in order to respond to access requests.

Actions of the DPA: The DPA decided in June 2012 that there was a violation of the French Data Protection Act by not adequately replying to the notice of default of the DPA and ordered the employer to pay a fine of 10.000 EUR.

Video surveillance - SAS Professional Service Consulting

Issue: In December 2010, an employee of SAS Professional Service Consulting filed a complaint about the use by his employer of video surveillance .

Actions of the DPA: The DPA initiated an investigation and *i.a.* established that (i) the cameras filmed the working place of certain employees without interruption, (ii) the information provided to the data subjects was insufficient, and (iii) the security measures to access the data were insufficient. Notwithstanding notices, subsequent controls and promises of the company, the DPA had to establish in December 2012 that the system was still in place and that the violations had not stopped. The company was ordered to pay a fine of 10.000 EUR in May 2013.

Germany

Google Street View – April 2013

Issue: From 2008 to 2010, Google collected wireless-network data by its cars taking photos for the Street View service. Google's cars captured the data, including contents of e-mails, passwords, photos and chat protocols.

Actions of the DPA: In April 2013, Google was ordered to pay a fine of 145.000 EUR and was ordered to destroy all the data concerned. In a similar matter, the French regulator CNIL levied a 100.000 Euro fine in 2011.

United Kingdom

Nationwide Energy Services Ltd / We Claim you Gain.

Issue: Direct Marketing The UK Office of Communications (OFCOM) is responsible for keeping a register of phone numbers allocated to subscribers who have notified that they do not wish to receive unsolicited calls for direct marketing purposes on those lines. Telephone Preference Service Limited (TPS) is a company set up by OFCOM to carry out this role. Businesses who wish to carry out direct marketing by telephone can subscribe to TPS for a fee and will then on a monthly basis receive the list of numbers in that register. Nation Wide Energy Services Ltd and We Claim you Gain Ltd, both part of the same group of

companies, made unsolicited calls for the purpose of direct marketing to consumers on the TPS list. 2.700 complaints were made to TPS which notified the DPA thereof, and the DPA also received complaints directly.

Actions of the DPA: TheDPA held that it is a necessary step for businesses undertaking telesales to make arrangements to ensure that they do not make direct marketing calls to consumers that have subscribed to TPS, unless they have obtained the informed consent of the consumers concerned. Nation Wide Energy Services Ltd was ordered to pay a monetary penalty of 125.000 £ and We Claim you Gain Ltd was ordered to pay a monetary penalty of 100.000 £ in June 2013.

Bank of Scotland

Issue: Customers' account details were repeatedly faxed to the wrong recipients by the Bank of Scotland. The information included pay slips, bank statements, account details and mortgage applications, along with customers' names, addresses and contact details.

Actions of the DPA: The DPA ruled that several provisions of the UK Data Protection Act had been infringed, including the obligation to take appropriate technical and organizational measures against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. A monetary penalty notice in the amount of 75.000£ has been served on the Bank of Scotland in July 2013.

For more information, contact: Frederik Van Remoortel

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Thomas De Meese
Partner – Brussels
Phone: +32.2.282.1842
Email: tdemeese@crowell.com

Frederik Van Remoortel
Partner – Brussels
Phone: +32.2.282.1844
Email: fvanremoortel@crowell.com