Stibbe

ICT Law Newsletter

Number 49 – June 2014

Judica Krikke

Partner
T • +31 20 546 02 12
judica.krikke@stibbe.com

Gérald Origer

Partner
T • +352 26 61 81 11
gerald.origer@stibbe.com

Erik Valgaeren

Partner
T • +32 2 533 53 43
erik.valgaeren@stibbe.com

FOCUS: EUROPE

European Court of Justice clarifies the scope of technological prevention measures designed to prevent unauthorized use

On 23 January 2014, the European Court of Justice ("ECJ") issued a judgment in response to a request from the Tribunale di Milano ("Milan Court of First Instance") for a preliminary ruling on two questions regarding the scope of technological protection measures as articulated in Article 6 of Directive 2001/29/EC of the European Parliament (the "Copyright Directive"). The ECJ maintained that Article 6 of the Copyright Directive legally protects rightholders from establishing technological mechanisms to prevent unauthorized use, but ruled that courts should consider whether alternative technology could have protected against unauthorized use while also allowing the use of legitimate multimedia produced by other manufacturers.

The case opposed Nintendo to PC Box. Nintendo manufactures and sells portable DS-game consoles and fixed Nintendo Wii-consoles. Nintendo also installs "recognition systems" and "key codes" to prevent the use of unauthorized copies of Nintendo videogames. These "technical protection measures" interact to identify copies and restrict unauthorized use, i.e., videogames and multimedia content without a key code cannot be used on either the portable or the fixed Nintendo Wii-consoles.

PC Box sells Nintendo game consoles and additional software called "homebrews" specifically designed to avoid Nintendo's key codes and recognition systems. This software is made by independent producers and can deactivate the technical protection measures (key codes and recognition systems) that Nintendo installed to prevent illegal use of videogames. Nintendo sued PC Box and 9Net before an Italian court, arguing that the principle purpose of the PC Box equipment was to circumvent Nintendo's protection measures. However, PC Box opined that the Nintendo protection measures prevent the full use of the consoles by restricting the device to read only Nintendo videogames.

The Copyright Directive emphasizes the need for Member States to legally protect technological measures implemented to effectively prevent unauthorized use, but it does not clearly establish how broad the technological measures may extend. Nintendo's technological protection measures prevent the use of not only unauthorized copies of Nintendo videogames but also prevent legal videogames by other manufacturers. Thus, Nintendo's key codes and recognition systems obstruct the use of illegal copies of games, and make it impossible to use videogames of other producers on the Nintendo devices.

The ECJ ruled that protective measures that require interaction between the videogame and the console fall under the concept of "effective technological measures" if their objective is to prevent or limit unauthorized use of protected material. However, a producer of videogame consoles should only invoke the digital protection of its videogames if the protection system is aimed to make the use of illegal copies of videogames impossible or harder. Protection should not prevent the use of non-infringing software (games) from other legitimate producers if an alternative technology accomplishes the same protection but does not restrict the use of non-infringing software at a comparable cost.

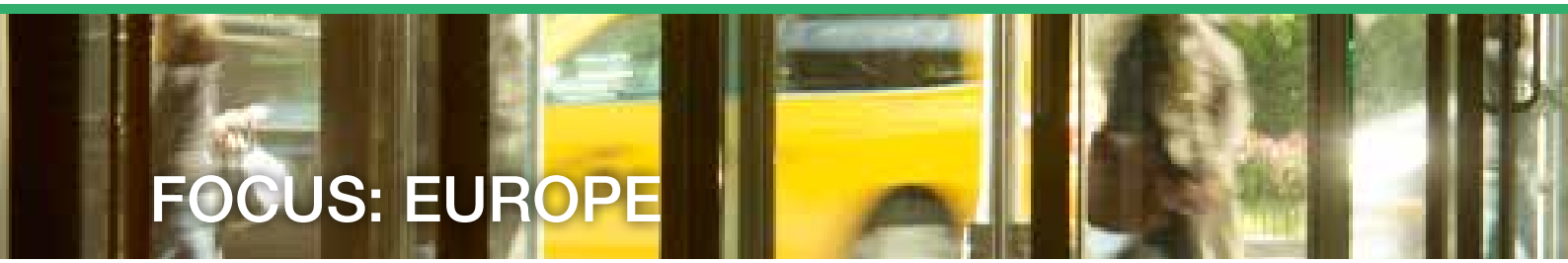
Here, the court should look at whether alternative technological measures could have protected Nintendo's rights without restricting the use of legal third-party activity. The court should look at evidence of actual use and how often PC Box's devices are used to allow unauthorized copies of Nintendo games, compared to how often PC Box's devices are used for legal purposes that do not infringe Nintendo copyrights.

The decision maintains the required legal protection for Nintendo's technological measures to prevent unauthorized use, but it does not condemn PC Box, on the condition that PC Box can prove that the use of its devices was lawful. National courts must still decide whether other measures causing less interference while still providing adequate protection are available, including a consideration of the different costs of these measures, as well as the purpose of the device used by PC Box whether the PC Box device is used primarily to play legal non-Nintendo games or, more often, to play illegal unauthorized copies of Nintendo games.

The case (C-355/12) can be found on http://www.curia.europa.eu

Michiel Van Roey

Junior associate
T • +32 2 533 52 07
michiel.vanroey@stibbe.com



FOCUS: EUROPE

Municipalities are allowed to levy fees at cost when an individual exercises its right of access

On 12 December 2013, the European Court of Justice ("ECJ") delivered an interesting judgment on the amount of charges municipalities are allowed to levy when a data subject exercises its right to access its personal data that are processed in the municipal personal records database. This case concerns a dispute heard by the Court of Appeal of The Hague which submitted preliminary questions to the ECJ.

In 2009, X committed a traffic offence and was fined. She did not pay the fine and had to appear in court. She argued that she had not received any order of the fine or any subsequent demands for payment that had been issued by the public prosecutor. At the time the fine was issued, she moved from one house to another several times, and she assumed that the fine and the subsequent payment demands might have been sent to the wrong address. To prove this, she requested the administrative office of the municipality where she currently lives to indicate specifically which data are held in the municipal personal records database. In accordance with Section 79(3) of the Municipal Database (Personal Records) Act (currently Section 2.55(3) of the Municipal Database (Personal Records) Act), the municipality supplied her with a certified document containing her requested data and charged her EUR 12.80 for it. But X refused to pay this.

Section 79 Municipal Database (Personal Records) Act specifically elaborates on Section 12 EU Directive 95/46/EC (the "Privacy Directive"), which specifies that a data subject should be given access to its personal data "without constraint at reasonable intervals and without excessive delay or expense". Based on Section 79(2) Municipal Database (Personal Records) Act, allowing a data subject's inspection of his/her personal data free-of-charge could be achieved by showing him/her the information on the computer screen of the civil servant working at the administrative office. If the data subject wants to obtain a copy thereof, he/she must pay for any administrative charges.

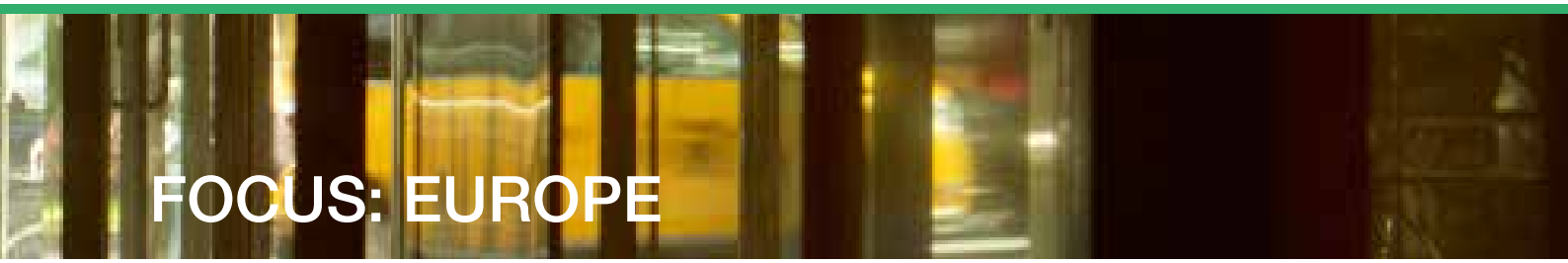
The Court of Appeal of The Hague submitted several preliminary questions to the ECJ. One of them, which is the more interesting one, is summarized as follows: Are municipalities allowed to levy fees for an extract from the municipal personal records database or does the Privacy Directive preclude this? The ECJ answered this question by saying that when a data subject exercises its right of access, levying fees is allowed, as long as they are not excessive. The fees should not have the effect of causing the data subject to waive its right of access. Therefore, the fees should not exceed the cost of data supply. Authorities can also choose to charge less than the actual costs in order to safeguard one's right of access.

For X, the essential question is whether or not the levied fees exceeded the actual cost of data supply. If the fees did exceed it, then it remains to be seen whether, in this case, charging the data subject for the actual cost that is currently known will not be considered an obstacle for the data subject to inspect the data after all.

The case (C-486/12) can be found on http://www.curia.europa.eu

Friederike van der Jagt

Senior associate
T • +31 20 546 01 44
friederike.vanderjagt@stibbe.com



FOCUS: EUROPE

Svensson-case: European Court of Justice rules hyperlinking to protected works can be done without consent

In 2012, the Court of Appeal of Svea (Sweden) submitted to the European Court of Justice ("ECJ") preliminary questions on whether providing hyperlinks constitutes an act of communication to the public under Directive 2001/29/EC (the "Copyright Directive"). This Directive stipulates that authors have the exclusive right to authorize or prohibit any communication of their works to the public.

The background facts of this specific case are the following: news articles from the daily newspaper *Göteborgs-Posten* are published on its own website which is freely accessible. A Swedish company, called Retriever Sverige, provides its clients with hyperlinks to news articles that are published on other websites, including that of *Göteborgs-Posten*. The journalists who were authors of those articles saw this hyperlinking as a breach of their copyright.

On 13 February 2014 the ECJ ruled that a clickable hyperlink to an authorized publicly available work does not infringe the "communication to the public" right because there is no communication to another, new public. In other words: while a link is an act of making available and where a work is already freely accessible on the Internet, then that act of making available does not require the consent of copyright holders because that act does not communicate the work to a "new public". The ECJ indicates that a new public is a public that has not been taken into account by the copyright holders at the time the initial communication was authorized. And there is no such "new public" from the website operated by Retriever Sverige.

The ECJ's conclusion is that website owners are allowed to redirect Internet users, via hyperlinks, to protected works that are available in a freely accessible basis on another site, without the authorization of the copyright holders. It must be kept in mind that different considerations apply regarding the situation where a hyperlink takes you to a website that is not freely available. Furthermore, the ECJ concluded that the Member States do not have the right to give wider protection to copyright holders by broadening the concept of "communication to the public".

The case (C-466/12) can be found on http://www.curia.europa.eu

Dianne Schaafsma

Transaction support lawyer
T • +31 20 546 01 79
dianne.schaafsma@stibbe.com

FOCUS: EUROPE

European Court of Justice specifies conditions under Article 8(3) of the Copyright Directive governing an injunction against ISPs

In a decision of 27 March 2014, the European Court of Justice ("ECJ") held that Article 8(3) of Directive 2001/29/EC (the "Copyright Directive") also allows injunctions to be applied for against Internet Service Providers ("ISPs") if an ISP has granted access not to the copyright infringer itself but only to the users of the protected movies. The ECJ described the conditions under which an injunction, prohibiting an ISP from allowing its customer's access to a website that places protected movies online, is compatible with EU fundamental rights.

This case concerns a dispute between Constantin Film and Wega (two film production companies) and UPC Telekabel (a major Austrian ISP). UPC Telekabel provided its customers with access to the website under the domain name kino.to that enabled users to download or stream films protected by the copyright held by the two film production companies. The two film production companies applied for an injunction to have UPC Telekabel ordered to block its customers' access to kino.to. UPC Telekabel contested the order mainly for two reasons: first, the ISP has no relationship with the operators of the website, and second, the various measures that can be introduced to block access to the website can all be technically circumvented.

In the first part of its decision, the ECJ confirmed its earlier case-law in *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten* and *Scarlet* to the extent that it recognizes that ISPs may in principle be regarded as "intermediaries whose services are used by a third party to infringe a copyright" within the meaning of Article 8(3) of the Copyright Directive. Moreover, the ECJ further clarified the case-law on the protection of copyright on the Internet by holding that Article 8(3) of the Copyright Directive covers an injunction against ISPs that have granted access to the users of the protected works. This conclusion was reached even from recognizing that no contractual relationship exists between the ISP and the copyright infringer (i.e., the operator of the website kino.to) and without having to prove that the ISP's customers actually accessed the protected works via the website.

In the second part of its decision, the ECJ describes the conditions under which an injunction (which prohibits an ISP from allowing its customers access to a website which places protected works online without the consent of the rightholders) would be compatible with EU law. The ECJ reviews the compatibility of the injunction by considering different conflicting EU fundamental rights such as the protection of intellectual property rights under Article 17(2) of the Charter of Fundamental Rights (the "Charter"), the freedom to conduct a business under Article 16 of the Charter, and the freedom of information of Internet users under Article 11 of the Charter.

As regards the freedom to conduct a business of an ISP, the ECJ held that the very substance of this right is not affected because, on the one hand, the ISP is free to determine the specific measures it will take to achieve the blocking of the website so that it can choose the measures that are best adapted to its resources and abilities, and on the other hand, the injunction allows the ISP to escape liability if the ISP can prove it has taken all reasonable measures that could be expected of it in order to prevent its customers' access to the website. Consequently, the ISP is not expected to make unbearable sacrifices since it is not the copyright infringer. In this regard it must also be possible for the ISP to maintain the confirmation before the court that the measures taken were indeed those that could be expected of it in order to prevent the condemned result.

Finally, the ECJ stresses that the measures taken by the ISP must comply with the Internet users' fundamental right to freedom of information and also comply with the protection of intellectual property rights. It states that:

- the measures may not unnecessarily deprive Internet users of the possibility of lawfully accessing the information available and;
- the measures must prevent unauthorized access to protected works or at least make the unauthorized access difficult to achieve (i.e., measures that must be appropriate to attain the objective of protecting intellectual property rights under Article 17(2) of the Charter of Fundamental Rights).

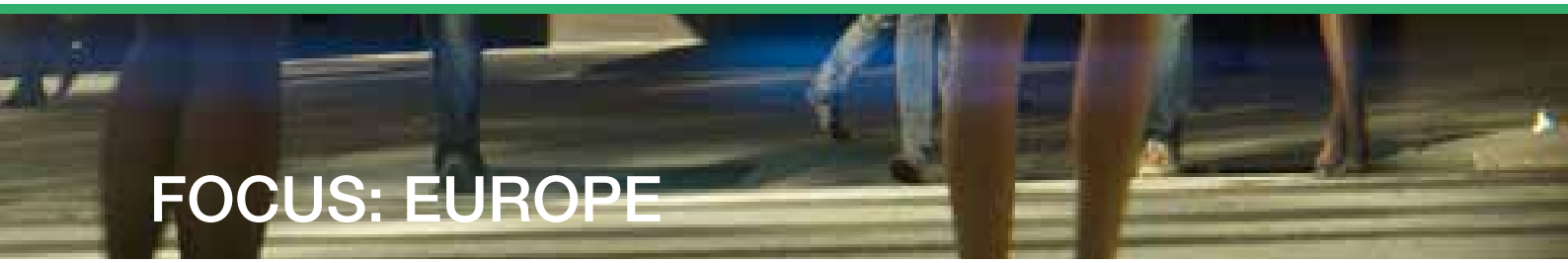
In summary, the ECJ held that under the conditions described above, EU fundamental rights must be interpreted as not precluding an injunction, such as the injunction in the case here which prohibits an ISP from allowing its customers access to a website that placed protected works online without the consent of the right holders.

The case (C-314/12) can be found on http://curia.europa.eu/.

Student trainee Steffie De Cock also contributed to this article.

Cédric Lindenmann

Junior associate
T • +32 2 533 54 56
cedric.lindenmann@stibbe.com



FOCUS: EUROPE

Search engine activities are subject to data protection rules when processing online personal data

On 13 May 2014 the European Court of Justice ("ECJ") rendered a decision in a case in which the Court had to answer important questions relating to the material and territorial scope of application of the Data Protection Directive 95/46 on search engine activities and to a data subject's "right to be forgotten".

The situation at issue related to the Google search results' display of links to web pages of a daily newspaper that contained announcements mentioning the plaintiff's name and relating to a real-estate auction connected with attachment proceedings for the recovery of social security debts.

According to the ECJ, a search engine's activity consisting in finding information that is published or placed on the Internet by third parties, indexing it automatically, storing it temporarily, and, finally, making it available to Internet users must be classified as "processing of personal data" if that information contain personal data. In this regard, the ECJ already stated in the past that loading personal data on an Internet page must be considered to be such "processing" (see Case C-101/1 Lindqvist). But, here, there is more to come: Unlike the opinion of the Advocate General who expressly argued for a reasonable interpretation of that concept, the ECJ ruled that, since the search engine operator determines the purposes and means of that activity, and thus of the processing of personal data that it carries out by itself, the search engine operator must be regarded as the "controller" in respect of that processing, notwithstanding the fact that those data were first published on third parties' web pages.

Normally, the territorial scope of application of the Directive is triggered by either the location of the establishment of the controller in the European Union or the location of the means or equipment being used if the controller is established outside the EU. Nationality or place of habitual residence of data subjects is not decisive, nor is the physical location of the personal data. In the case here, the search engine operator argued that the processing of personal data at issue was carried out exclusively by the American mother company, without any intervention from the local European subsidiaries whose activity is limited to providing support to the group's advertising activity, which is separate from its search engine service. Nevertheless, the ECJ found that the processing of personal data in question is not required to be carried out "by" the controller itself, but only to be carried out "in the context of the activities" of the establishment of the controller. Therefore, the processing of personal data for the purposes of the service of a search engine is carried out "in the context of the activities" of the local establishment if the latter is intended to promote and sell—in that Member State—advertising space to make the services offered by that engine profitable.

The ECJ also stated that the "right of access" to personal data processed by the controller and the "right to object" to such processing in certain situations have to be interpreted as enabling the data subject to require the search engine operator to remove from the displayed list of results, following a search made on the basis of his name, links to web pages published lawfully by third parties. Those data subject' rights override—as a rule—in not only the economic interest of the search engine operator but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for "particular reasons" such as the role played by the data subject in public life, that the interference with the data subject's fundamental rights is justified by the preponderant interest of the general public in having access to the information in question through the list of search results.

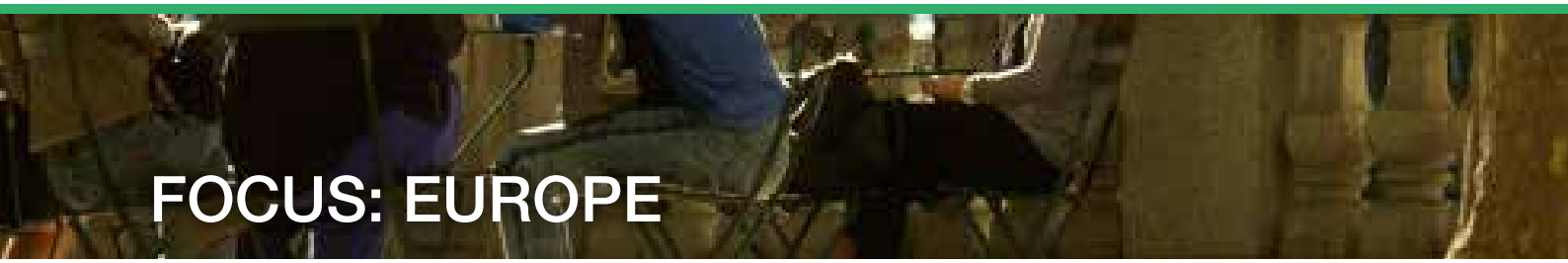
Also, the ECJ did not recognize the search engine's processing of personal data to be carried out "solely for journalistic purposes", so the operator may not benefit from derogations from the requirements laid down by the Directive.

This decision might be considered a landmark case, but it does not solve everything. On the contrary, it raises new questions, such as the search engine operators' compliance process with other data protection obligations, and far-reaching practical issues, such as the implementation of appropriate take-down mechanisms. Also, it is noteworthy that the ECJ did not refer to Article 10 of the European Convention on Human Rights which protects the freedom of expression and information, covering the freedom to receive and impart information.

The decision (C-131/12) can be found on http://curia.europa.eu.

Nicolas Roland

Senior associate
T • +32 2 533 51 51
nicolas.roland@stibbe.com



FOCUS: EUROPE

European Court of Justice declares the Data Retention Directive invalid

In its decision of 8 April 2014, the European Court of Justice ("ECJ") declared the Data Retention Directive 2006/24/EC (the "Directive") invalid. The ECJ ruled that the Directive entailed "a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary".

The judgment was rendered in response to questions posed to the ECJ by the Irish High Court and the Austrian Constitutional Court. The ECJ had to examine the validity of the Directive in the light of two fundamental rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data. More in particular, the ECJ was asked to examine whether the interference of the Directive with these fundamental rights was justified.

The Court first stated that the retention of data required by the Directive does not as such adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data. The Directive does not permit the acquisition of knowledge of the content of the electronic communications and provides that service or network providers must respect certain principles of data protection and data security.

In addition, the retention of data for the purpose of their possible transmission to the competent national authorities genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security.

However, the ECJ observed that the data retained made it possible (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place, and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

The ECJ acknowledged that those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships, and the social environments frequented.

Thereafter, the ECJ identified several particular concerns regarding the proportionality of the Directive:

1. The generality of the Directive: It covers all individuals, all electronic communications and all traffic data without differentiations, limitations, or exceptions;

2. The Directive fails to lay down objective criteria for and procedures regulating access to and use of the data;

3. The Directive fails to lay down objective criteria to determine the data retention period between 6 and 24 months and does not take into account the type of data, its usefulness, or its proportional necessity;

5. The Directive does not provide sufficient safeguards against possible abuse, unlawful access, or use of data;

6. The Directive does not require retaining the data in the EU so that compliance with the EU data protection laws cannot be ensured.

Therefore, the ECJ concluded that even though the retention of data required by the Directive may be considered to be appropriate for attaining the objective pursued by it, the Directive exceeds the limits imposed by compliance with the principle of proportionality.

The decision (C-293/12 and C-594/12) can be on http://curia.europa.eu.

Valerie Vanryckeghem

Junior associate
T • +32 2 533 51 72
valerie.vanryckeghem@stibbe.com

FOCUS: EUROPE

Article 29 Data Protection Working Party issues Opinion on Personal Data Breach Notifications

On 25 March 2014, the Article 29 Working Party ("WP 29") issued Opinion 03/2014 (the "Opinion"). The Opinion provides guidance to data controllers to help them decide whether to notify data subjects about a personal data breach.

In the first part of the Opinion, the WP 29 considers the notification obligations of telecommunications service providers that are imposed by the Directive 2002/58/EC. This Directive requires personal data breaches to be notified to the competent national authority. In addition, when the data breach is likely to adversely affect the personal data or privacy of a data subject, the data controller must also notify the data subject about the breach without undue delay.

However, the Directive 2002/58/EC as well as the Proposed EU General Data Protection Regulation (the "Proposed Regulation") contain an exemption to this notification obligation. That is, if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures to render the data unintelligible to any person who is not authorized to access it and if those measures were applied to the data concerned by the security breach, then notification of a personal data breach to a data subject is not required.

The WP 29 advises controllers to take appropriate technological and organizational measures to ensure a level of security that is appropriate to the risk represented by the processing so that they can rely on the exemption and avoid the need to notify the data subject. In this respect, the WP 29 notes that data controllers should proceed with notification when they have doubts about the likelihood of the adverse effects on the personal data or privacy of the data subjects.

In the second part of the Opinion, the WP29 lists both examples of data breaches where the affected data subjects should be notified as well as examples of cases where notification to the affected data subjects would not be required. The WP 29 also gives examples of technical measures which, if they had been in place prior to the breach, might have allowed for the avoidance of the need to notify the data subject, such as a confidentiality data breach that only concerns either encrypted data with a state of the art algorithm or salted/keyed, hashed data with a state of the art hash function (assuming all the relevant keys and salts are not compromised).

Finally, the Opinion talks about the various considerations companies face when assessing whether or not to notify the affected data subjects. The WP 29 emphasizes the need to factor in likely secondary adverse effects on the data subjects and indicates that companies should notify even if only one data subject is affected.

The Opinion can be found on http://ec.europa.eu/justice/data-protection/article-29/.

Student trainee Steffie De Cock also contributed to this article.

Valerie Vanryckeghem

Junior associate
T • +32 2 533 51 72
valerie.vanryckeghem@stibbe.com

FOCUS: BELGIUM

Belgian Privacy Commission's position on use of dashcams

The Belgian Privacy Commission ("BPC") recently addressed the privacy implications concerning the use of dashboard cameras ("dashcams") in cars. The use of a dashcam to film traffic constitutes the processing of images (in the light of advice no 34/1999 of 13 December 1999), where personal data (e.g., a license plate) can be registered. This would imply that the dashcam user, as data controller, is bound by the obligations of the Belgian Data Protection Act of 8 December 1992 ("BDPA"). However, not every use of a dashcam falls within the scope of the BDPA. The BPC makes the distinction between (i) dashcams for recreational use, (ii) dashcams for use as evidence in the event of a collision of cars, and (iii) dashcams used in the interior of a taxi.

First, Article 3, §2 BDPA exempts an individual's recreational use of a dashcam if the video images are solely used for "personal and domestic purposes." Thus, a dashcam's recreational use is acceptable if the video footage is only viewed by a certain well-defined group of family members, acquaintances, and friends of the individual user. Publishing the video footage on a publicly accessible website (or even on Facebook) falls outside the definition of "personal and domestic purposes", so that the requirements of the BDPA will apply.

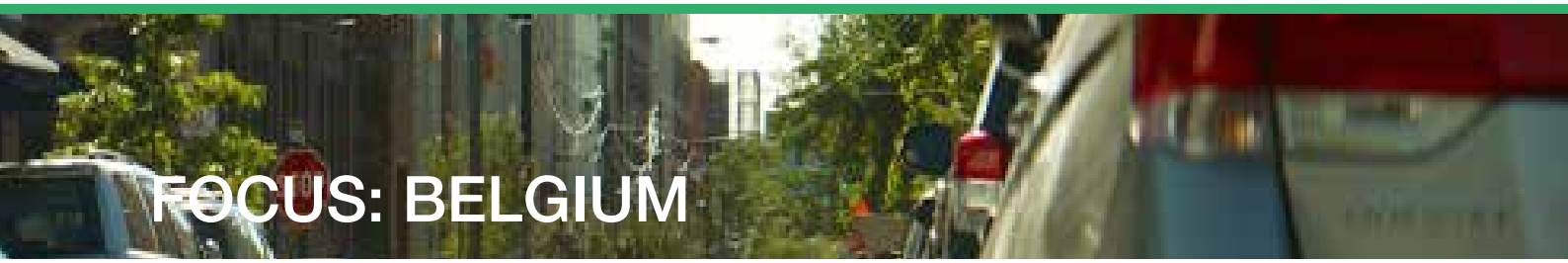
Second, the BPC elaborates on the use of dashcams for evidential purposes in the event of a collision. The recording of video footage during a car collision does not constitute the processing of personal data, but rather the processing of legal personal data. Legal personal data processing is expressly excluded from the BDPA. However, the BPC allows for an exception, and that is, it permits the processing of information concerning suspicions, prosecutions, and convictions by any person for the purposes of handling his/her own dispute. The BPC states that the data controller must inform the subject of the footage immediately after the accident, should the people involved in the collision communicate with each other after the accident. In addition, the dashcam user will be required to file a privacy notification to the BPC.

Finally, the BPC describes the use of dashcams in taxis. These dashcams are intended to protect the driver or to record a possible theft or act of vandalism. In these circumstances, a dashcam is seen as a surveillance camera in a private place which is accessible to the public. Thus, this use does not fall under the BDPA, but rather within the scope of the Act of 21 March 2007 regulating the installation and use of surveillance cameras ("Belgian Camera Act"). The Belgian Camera Act stipulates that taxis equipped with a dashcam must exhibit a uniform icon so that customers are aware that they are being filmed. The data controller, either the employer or the taxi driver himself, will have to inform or notify the BPC and the chief of police of its decision to use a dashcam the day before it commissions the use of the camera.

The explicative notice can be found on http://www.privacycommission.be

Michiel Van Roey

Junior associate
T • +32 2 533 52 07
michiel.vanroey@stibbe.com



FOCUS: BELGIUM

Court of Appeal of Antwerp confirms Yahoo!'s obligation to cooperate with law enforcement agencies

On 20 November 2013, the Court of Appeal of Antwerp partially confirmed the Criminal Court of Dendermonde's judgment dated 2 March 2009. The Criminal Court convicted Yahoo! and obliged it to disclose the identity of the persons who committed fraud via their Yahoo! e-mail accounts.

The public prosecutor of Dendermonde had requested US-based Yahoo! to disclose the identity of certain people who used their Yahoo! e-mail accounts to commit Internet fraud. The public prosecutor's charge against Yahoo! was based on Article 46bis of the Criminal Procedure Code, which obliges electronic communication services providers to disclose identification data to law enforcement agencies when these agencies request them. Although Yahoo! is established in the US and has no branch or office in Belgium, the public prosecutor was of the opinion that Yahoo! is considered an electronic communications service provider and is consequently obliged to comply with law enforcement agencies' request for such information.

Yahoo!, however, refused to disclose the identification data, arguing that it is not subject to Article 46bis of the Criminal Procedure Code because it was not an electronic communications service provider. According to Yahoo!, the term "electronic communications service provider" in Article 46bis of the Criminal Procedure Code had the same meaning as the term "electronic communications service provider" in Article 2 of the Electronic Communications Act of 13 June 2005. Since this Article 2 states that a provider of information society services, such as providers of free e-mail addresses, are not considered a provider of electronic communications services, Yahoo! asserted that it was not obliged to disclose identification data to the public prosecutor.

The Criminal Court of Dendermonde did not follow Yahoo!'s argument, but Yahoo! challenged the decision successfully before the Court of Appeal of Ghent. However, the public prosecutor appealed this decision before the Court of Cassation, and this Belgian supreme court on 18 January 2011 held that the term "electronic communications service provider" in Article 46bis of the Criminal Procedure Code has an autonomous meaning. Therefore, it does not have the same meaning as that in Article 2 of the Electronic Communications Act. In the Court of Cassation's opinion, a provider of a service which allows its users to gather, disclose, or distribute information by using an electronic communications network is considered an electronic communications service provider within the meaning of Article 46bis of the Criminal Procedure Code.

The case was afterwards referred to the Court of Appeal of Brussels. This Court, on 12 October 2011, took the position that the Court of Cassation's order had not been validly communicated to Yahoo!. In the Court of Appeal's opinion, the mere fact that it is technically possible for the public prosecutor to contact Yahoo! from the Belgian territory by means of electronic or other means of communication is not sufficient. The public prosecutor lodged a second appeal before the Court of Cassation, and this Court found, on 4 September 2012, that the public prosecutor's sending of his written request within the meaning of Article 46bis of the Criminal Procedure Code (whereby the cooperation is required from an operator established outside Belgium) from Belgium to a foreign address does not render the request invalid. The case was then referred to the Court of Appeal of Antwerp. This Court confirmed the applicability of Article 46bis of the Criminal Procedure Code and fined Yahoo! € 44 000 and € 22 000 of this sum is conditional over a three-year period.

This Court concurred with the Criminal Court of Dendermonde that Yahoo! was "virtually" located in Belgium by offering electronic communications services in Belgium and that the offence of refusing to provide the public prosecutor with the required identification data took place in Belgium. The Court added that if Yahoo! is not willing to comply with the requirements of Article 46bis of the Criminal Procedure Code, it may decide to exclude Yahoo!'s IP-range from Belgium. The Court, however, did not order the disclosure of identification data since the public prosecutor did not insist on it anymore.

The case can be found on http://www.ie-forum.be

Nicolas Roland

Senior associate
T • +32 2 533 51 51
nicolas.roland@stibbe.com

FOCUS: THE NETHERLANDS

Dutch government violated Article 8 ECHR by requesting and saving personal data in central register

Recently, the Court of Appeal of The Hague held that the storage of Dutch citizens' personal data in a central register is an unjustified violation of the right to privacy.

In light of, amongst other things, the implementation of the European regulation on standards for security features and biometrics in passports and travel documents, and to comply with this regulation, the Dutch Passport Act was amended in 2009. This new Passport Act states that future passports would have to contain a chip with a digital facial image and two fingerprints of each applicant. The Dutch government therefore planned to create a central register to hold the facial image files and four fingerprints of each applicant (two of which are included in the passport for identity verification). This new register would also serve other purposes: it would help passport fraud control, and it would allow applicants to renew their passport in any municipality in the Netherlands. The national government acknowledged that the request and saving of these personal data would form a violation of the right to privacy of Dutch citizens, but the government stated that the data storage was proportionate and justified, considering the intended purposes.

The interest group Privacy First disagreed with the government. This group, which seeks to publicly promote the enhancement and preservation of the right to privacy, believed that the creation of this central register violates this fundamental right enshrined in several international laws and regulations. The group launched legal proceedings against the Dutch government. The district court of The Hague ruled that Privacy First did not have a cause of action. Privacy First then appealed against this verdict.

Remarkably, the government meanwhile reviewed their amendments to the new Passport Act. The government concluded that the storage of these personal data in a central register did not achieve its purpose, namely passport fraud control via one's identity verification. Therefore, the Act's provisions that related to the storage of personal data in a central register would be suspended. Furthermore, the number of fingerprints to be taken for the filing would be reduced from four to two in accordance with European regulation.

On appeal, the Court of Appeal ruled that since Privacy First and the government now share the same views about the central register, Privacy First would have lost its standing in their cause of actions, so it dismissed the interest group's claims. However, the Court of Appeal found that the district court had erred when it held that Privacy First did not have a cause of action at the time. Since Privacy First is an interest group advocating the protection of the general interest of Dutch nationals' right to privacy, it should have been able to bring proceedings before the civil court according to Article 3:305 of the Dutch Civil Code *(Burgerlijk Wetboek)*. This would only have been different if the interest group had represented the combined interest of individuals. The Court of Appeal further ruled that Privacy First incurred a financial risk.

The Court of Appeal also ruled that in view of all the circumstances of the case at first instance, the district court should have ruled in favour of Privacy First concerning their arguments against the setting up of a central register. This central register's storage of Dutch citizens' personal data is an unjustified violation of one's right to privacy enshrined in Article 8 ECHR because it did not fulfill its purpose. The Court of Appeal understands that this was a violation from the start, but this had only become evident after the first ruling.

[Source: Court of Appeal The Hague, 18 February 2014, ECLI:NLGHDHA:2014:412]

Dianne Schaafsma

Transaction support lawyer
T • +31 20 546 01 79
dianne.schaafsma@stibbe.com

FOCUS: THE NETHERLANDS

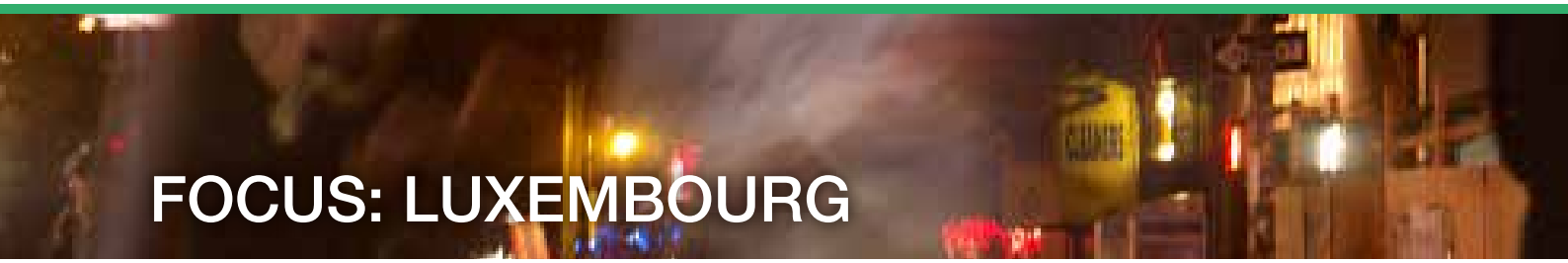
Rabobank fulfilled its duty of care by issuing a warning for phone "phishing"

The Dutch bank Rabobank hosts Internet banking for its customers. On 8 June 2010 Montage B.V. and others ("Montage") fell victim to fraud. Someone presented himself via the telephone as an employee of Rabobank and asked for Montage's login data to access Montage's Internet banking account (an act, which can also be done via email and other communications, known as "phishing"'). Montage, being under the impression that they were dealing with an employee of Rabobank, communicated its internet banking login data to the impersonator, enabling him to execute several transactions and wire money to his own account. Montage sought damages from Rabobank for the stolen money on grounds that Rabobank would not have fulfilled its duty of care by not explicitly warning Montage about persons who would masquerade themselves via the telephone as Rabobank employees and ask Rabobank customers for their internet banking login data. After the first instance and the first interlocutory judgment, the final question in the second interlocutory hearing was whether the bank failed to warn its customers about this specific type of fraud. Montage and others claim that they only saw Rabobank's warnings on phishing after 8 June 2010. Even though Montage and others did declare they all saw the warning after 8 June 2010, they all stated that they saw different warnings. In response, Rabobank stated that the bank did issue the warning via their "message center" on the Rabobank website. On the basis of the statements from Montage and the Rabobank, the Court accepted Rabobank's defense and ruled that the warning via Rabobank's "message center" about phone phishing was specific and clear enough (and was issued before 8 June 2010), so Rabobank did warn its customers and, with that, fulfilled its duty of care. The bank had therefore no obligation to pay damages to the claimants.

[Source: Court of Appeal 's-Hertogenbosch, 18 February 2014, ECLI:NL:GHSE:2014:39.]

Joost van Eymeren

Junior associate
T • +31 20 546 03 32
joost.vaneymeren@stibbe.com



FOCUS: LUXEMBOURG

Luxembourg launches data protection association

The Luxembourg data protection association called *l'Association pour la protection des données* (the APDL) was officially launched on 11 March 2014. The APDL's purpose is to, inter alia, (i) enable its members to exchange and communicate with administrations and local regulators, as well as to be represented towards these bodies, (ii) share information and knowledge about data protection through the organization of events, conferences, and partnerships at both local and international levels, and (iii) create ties with foreign data protection associations.

The APDL welcomes members from all kinds of backgrounds because the diversity of its members allows Luxembourg to have an active data protection community from all sectors.

The APDL has planned a seminar entitled "Towards a new EU Data Protection Regulation: Legal & Practical implications" from 18 to 20 September 2014 in Luxembourg, in cooperation with the International Association of Lawyers.

Further information (only in French) is available on this link: http://www.apdl.lu/Joomla/

Nicolas Van Heule

Senior associate
T • +352 26 61 81 15
nicolas.vanheule@stibbe.com

Johanne Mersch

Associate
T • +352 26 61 81 20
johanne.mersch@stibbe.com

Stibbe

For more information

If you require further copies of this newsletter, or advice on any of the matters raised in it, please contact:
Erik Valgaeren, T +32 2 533 53 51, F +32 2 533 51 15, erik.valgaeren@stibbe.com

Brussels

Central Plaza
Loksumstraat
Rue de Loxum 25
1000 Brussels
Belgium
T • +32 2 533 52 11
F • +32 2 533 52 12

Amsterdam

Stibbetoren
Strawinskylaan 2001
PO Box 75640
1070 AP Amsterdam
The Netherlands
T • +31 20 546 06 06
F • +31 20 546 01 23

Luxembourg

Rue Jean Monnet 6
2180 Luxembourg
Luxembourg
T • +352 26 61 81
F • +352 26 61 82

The ICT Law Newsletter is also available on our website

www.stibbe.com

Dubai

Dubai International Financial Centre
Gate Village 7, Level 4
PO Box 506631
Dubai UAE
United Arab Emirates
T • +971 4 428 63 13
F • +971 4 365 31 71

Hong Kong

Suite 1008-1009
10/F, Hutchison House
10 Harcourt Road
Central, Hong Kong
T • +852 2537 0931
F • +852 2537 0939

London

Exchange House
Primrose Street
London EC2A 2ST
United Kingdom
T • +44 20 7466 6300
F • +44 20 7466 6311

New York

489 Fifth Avenue, 32nd floor
New York, NY 10017
USA
T • +1 212 972 4000
F • +1 212 972 4929