INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L'HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

BELGIUM COUNTRY REPORTS

VRIJE UNIVERSITEIT BRUSSEL, BELGIUM

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN BELGIUM – ANTONELLA GALETTA & PROFESSOR PAUL DE HERT

LOCATING THE DATA CONTROLLER IN BELGIUM – ANTONELLA GALETTA & PROFESSOR PAUL DE HERT

SUBMITTING ACCESS REQUESTS IN BELGIUM – ANTONELLA GALETTA & PROFESSOR PAUL DE HERT

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN BELGIUM[1]

Application (primary and secondary legislation) and interpretation (case law) of data protection principles

The right to the protection of personal data is not explicitly mentioned in the Belgian Constitution which dates back to 1831. Like in the legal tradition of the European Convention of Human Rights, the constitutional legitimation of this right derives from the right to respect for private and family life. It is guaranteed by Art. 22 of the Constitution whose first paragraph provides that "everyone has the right to the respect of his private and family life, except in the cases and conditions determined by the law".[2]

The main legislative instrument at national level which protects and regulates the right to personal data is the Law on the protection of privacy in relation to the processing of personal data of 8 December 1992 (the Privacy Act).[3] It entered into force between 1 March 1993 and 1 September 1994 and was amended by the Law of 11 December 1998[4] and the Law of 26 February 2003.[5] These two latter amendments were introduced following the approval of the European Directive 95/46/EC to which the Privacy Act is anchored. The Privacy Act has been further implemented by the Royal Decree of 13 February 2001.[6] The authority that oversees and enforces the Privacy Act is the Belgian Commission for the Protection of Privacy (hereafter the Privacy Commission) (*Commissie voor de bescherming van de persoonlijke levenssfeer*/*Commission de la protection de la vie privée*). The Act applies in the case of processing of personal data which corresponds to "any operation or set of operations performed on personal data".[7] It concerns the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination,

[1] The author would like to thank Dirk De Bot (Vrije Universiteit Brussel, VUB) for his valuable comments on the report.

[2] The Belgian Constitution of 1831 and its modifications, http://www.senate.be/doc/const_fr.html (last accessed 28 May 2013). Furthermore, the Belgian Constitution safeguards the inviolability of the residence (Art. 15) and the confidentiality of the mail (Art. 29).

[3] Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*/*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*.

[4] Law of 11 December 1998 on the transposition of the European Data Protection Directive, Belgian Official Journal, 3 February 1999. This amending law entered into force on 1 September 2001.

[5] Law of 26 February 2003, Belgian Official Journal, 26 June 2003. This law modified the statute of the Belgian DPA (the Privacy Commission) and expanded its competencies.

[6] *Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel,* M .B., 13 May 2001. An unofficial English translation of the decree is available at http://www.privacycommission.be/sites/privacycommission/files/documents/Royal_Decree_2001.pdf (last accessed 11 July 2013).

[7] The Privacy Commission, *Protection of personal data in Belgium*, p. 5, http://www.privacycommission.be/sites/privacycommission/files/documents/protection-of-personal-data-in-belgium.pdf (last accessed 28 May 2013).

alignment, combination, blocking, erasure or destruction of personal data.[8] The Act does not apply to the processing of personal data carried out in the course of purely personal or household activities,[9] such as in the case of a private address file or a personal electronic diary. The application of the Act is considerably limited via numerous exemption categories in a number of circumstances, notably in the case of data processing for journalistic, artistic or literary purposes (Art. 3, Paragraph 3); for public security and intelligence purposes (Art. 3, Paragraph 4); for the purposes of implementing money laundering legislation (Art. 3, Paragraph 5); and for the fulfilment of duties of the judicial and administrative police (Art. 3, Paragraph 5).[10]

According to the Privacy Act, personal data have to be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed; accurate and, if necessary, kept up to date; and kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or further processed (Art. 4). Each of the requirements enshrined in Art. 4 originates a specific principle in the Belgian data protection system. Hence, they are the principles of legality, finality, proportionality, data quality and legitimation which are the cornerstones of the Privacy Act.[11]

Art. 5 of the Act highlights that personal data should be processed in specific circumstances only, namely:
"a) if the data subject has unambiguously given his consent;
b) if processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) if processing is necessary for compliance with an obligation to which the controller is subject by or by virtue of a law, decree or ordinance;
d) if processing is necessary in order to protect the vital interests of the data subject;
e) if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
f) if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed, provided that the interests or fundamental rights and freedoms of the data subject who has a claim to protection under this law, do not prevail".

There are three categories of data whose processing is subject to specific rules in the framework of the Privacy Act. These are data revealing racial or ethnic origin, political

[8] The Privacy Act, Article 1, Paragraph 2.
[9] The Privacy Act, Article 3, Paragraph 2.
[10] Additional limitations are established in the case of child protection (Paragraph 6) and for tax administration purposes (Paragraph 7).
[11] For a more detailed analysis of these principles see Boulanger M.-H., De Terwangne C. and Léonard, T., « La protection de la vie privée à l'égard des traitements de données à caractère personnel : la loi du 8 décembre 1992 », Journal des Tribunaux, 5675, 1993, pp. 369-388.

opinions, religious or philosophical beliefs, trade-union membership and sex life (the so-called sensitive data) (Art. 6), health-related personal data (Art. 7); and judicial data (data relating to litigation that has been submitted to courts, tribunals or administrative judicial bodies) (Art. 8). Articles 6, 7 and 8 of the Privacy Act can be invoked not only in the case those data are violated but also when there is the mere suspicion that such violation has occurred. The Act restricts the processing of these data to specific circumstances which are explicitly established by the Act itself.[12] (Written) consent and necessity represent the main legal basis that legitimises the processing for the first and second category of data. Indeed, noteworthy in Belgium the requirement of an explicit consent has been transposed as a written consent.

The Privacy Act defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his or his legal representative's agreement to the processing of personal data relating to the data subject" (Art. 1, Paragraph 8 of the Privacy Act).

Case law

A violation of the principle of proportionality was found by the Belgian *Cour d'arbitrage* (the former Belgian Constitutional Court)[13] in the affair *Monsieur J.V. v Communauté flamande*.[14] The claimant was a non-professional cyclist who had used anabolic steroids to improve his sport performances. The Belgian league of velocipedes then imposed upon him a lifetime suspension from all bicycle races. In addition, the notice of his suspension was published on the official website of the Flemish Community, in accordance with Art. 40, Paragraph 6.2 of the Flemish Decree of 27 March 1991. This article imposed the obligation to publish such notices and in particular to indicate the name, first name, date of birth, the suspension period and the sport played by the concerned sportsman.[15] Monsieur J. V. demanded the annulation of Art. 40, Par. 6.2 and claimed that it violated Art. 22 of the Constitution (right to the respect of private and family life). He argued that the publication of the suspension notice on a website accessible to anyone represented a disproportionate measure which was incompatible with the purpose to inform sports associations about the

[12] According to Art. 6 of the Act, the processing of sensitive data is allowed if the data subject has given his consent through a written statement; if the processing is necessary for the purposes of carrying out specific obligations and rights of the controller in the field of employment law of for in the framework of social security; if the processing is necessary to protect the vital interests of the data subject or another person; if the processing is carried out in the course of a legitimate activity of a foundation, association or non-profit organisation; if processing relates to data that have been made public by the data subject; if the processing is necessary for the establishment, exercise or defence of legal claims; if processing is necessary for scientific research or public statistics; and if processing is necessary for the purpose of preventive medicine or medical diagnosis. The bulk of these exceptions apply also for health-related personal data (Art. 7). Finally, judicial data can be processed under supervision of a public authority or ministerial officer; by natural or legal persons if the processing is necessary; and if the processing is necessary for scientific research.

[13] The Belgian *Cour d'Arbitrage* was given the name *Cour Constitutionnelle* on 7 May 2007.

[14] Cour d'Arbitrage, *Monsieur J.V. v Communauté flamande*, arrêt n° 16/2005, 19 January 2005.

[15] Indeed, Art. 40, Par. 6.2 stated that « les suspensions disciplinaires des sportifs majeurs sont publiées pour la durée de la suspension sur le site web que le Gouvernement crée à cet effet et par les canaux de communication officiels créés par les fédérations sportives. Cette publication contient les nom, prénom et date de naissance du sportif, le début et la fin de la période de suspension et la discipline sportive qui a donné lieu à l'infraction ».

fact a certain disciplinary measure has been taken and that they had to implement it. This argument was rejected by the Flemish government who pointed out that the publication of the notice was necessary to inform professional and non-professional sports associations and to keep them updated in the organisation of sport tournaments. In addition, Monsieur J.V. claimed a violation of the principles of equality and non-discrimination safeguarded respectively by Art. 10 and 11 of the Constitution. The Court found that the publication of disciplinary sanctions against sportsmen on a public website accessible to anyone constituted a violation of the right to respect for private life. Accordingly, the provision of the Flemish Decree infringed Art. 22 of the Belgian Constitution and the Privacy Act. As the Court underlined, the publication was not proportionate with the purpose pursued by the government to inform sports associations, considered that anyone could get these data and process them further even once the website had disappeared. The government's aim could have been reached making the notice accessible to specific organisations only (and not to the wide public), so respecting the claimant's private life. Thus, the Court repealed Art. 40, Par. 6.2 in some of its parts.[16]

The case *Federatie van verzekeringsmakelaars, Fédération des professionnels en assurance de Belgique v N.V. Kredietbank* of 7 July 1994 marked the application and enforcement of the Privacy Act for the first time at national level.[17] The case originated as a dispute between Uniprabel, the Belgian federation of insurance brokers and a local bank (Kredietbank). The bank processed personal data of its customers in order to obtain information about their interest in subscribing specific insurance products. These data were acquired analysing the bank transfers of customers. Uniprabel considered the processing unlawful and contrary to the good and honest market practices. Hence, it addressed to the Court of Trade of Antwerp alleging a violation of the Privacy Act and of the general principle of prudence that applies in trade practices. The judgment of the Antwerp Court is greatly based on the principles of legitimacy and finality which inspire the Privacy Act (Art. 4). As the Court pointed out, legitimacy requires data controllers to identify and make clear the purpose of the data processing. Moreover, data should not be processed in a way that is incompatible with the given purpose, according to the principle of finality. In the case at stake the Court found that the processing purpose declared by the bank (promotion of financial products, i.e.: loans, saving plans, payment methods, etc.) did not correspond to the purpose that the bank actually wanted to pursue, namely the marketing of insurance products specifically. As the Court argued, the practices of the bank constituted a "détournement de finalité". Nonetheless, an additional violation of the Privacy Act consisted in the bank's omission to inform data subjects about the actual purpose of the processing. Thus, the Court declared that the conduct of the bank violated the Privacy Act and that the bank processed its customer's data unlawfully. It is important to note that although the Court recognised that the violation of the Privacy Act was indirect, it formed the basis to state that the bank had committed dishonest practices.

[16] In particular, the Court withdrew the words «sur le site web que le gouvernement crée à cet effet et» from the text of the Flemish decree.

[17] Court of Trade of Antwerp, Rechtbank van koophandel te Antwerpen, *Federatie van verzekeringsmakelaars, Fédération des professionnels en assurance de Belgique v N.V. Kredietbank*, 7 July 1994. For an analysis of the case see also Léonard, T., "Grondrechten en vrijheden / Libertés et droits fondamentaux, Rechtbank van koophandel te Antwerpen, 7 juli 1994", *Consumentenrecht*, October 1994.

Application (primary and secondary legislation) and interpretation (case law) of the right of access to data

Chapter III of the Privacy Act illustrates the rights of the data subject and regulates the exercise of these rights. In doing so, it establishes specific obligations on the data controllers. According to Art. 9 of the Act, once the data controller obtains personal data from the data subject, he has to provide him with several pieces of information, namely:

"a. name and address of the controller and, if such is the case, of his representative;
b. the purposes of the processing;
c. the existence of a right to object on request and free of charges against the intended processing, if personal data are obtained for purposes of direct marketing;
d. other additional information, in particular:
• the recipients or categories of recipients of the data;
• whether or not replies to the questions are obligatory as well as possible consequences of a failure to reply;
• the existence of the right of access to and the right to rectify the personal data concerning him".

Where the data controller has not obtained data directly from the data subject, he must provide the above information, as well as information on the categories of personal data processed.

Article 10 of the Privacy Act regulates the individual's right to access to personal data relating to him/her. In order to have access to this information, the data subject has to submit a signed and dated request to the data controller. Having proved his identity, the data subject has the right to obtain from the controller the following:

a. confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the categories of recipients to whom the data are disclosed;
b. communication in an intelligible form of the data undergoing processing and of any available information as to their source;
c. knowledge of the logic involved in any automatic processing of data concerning him in the case of automated profiling;
d. knowledge of the possibility to lodge an appeal, and possibly, to consult the public register of all automatic processing operations of personal data.[18]

The information shall be communicated immediately and no later than forty-five days after receipt of the request. Any person has the right to obtain rectification of inaccurate personal data relating to him, free of charge (Art. 12). Similarly, if personal data have been obtained

[18] Article 18 of the Privacy Act states that this register is kept by the Privacy Commission.

for purposes of direct marketing, the data subject may object free of charge and without any grounds to the intended processing of personal data. Still, any person has the right to obtain free of charge the erasure of all personal data relating to him or the prohibition of using such data that are incomplete or irrelevant or that have been stored longer than the authorised period of time. In all these circumstances the data subject has to submit a signed and dated request to the data controller. In turn, the controller has to disclose all corrections and erasures of data within one month from the time of the submission of the request to the data subject himself, as well as to the persons to whom the inaccurate, incomplete or irrelevant data have been disclosed. The data subject has the right to appeal the decision taken by the data controller before the Privacy Commission (Art. 13) and to the tribunal of first instance (Art. 14).

Case law

The most relevant case concerning access rights in Belgium is *C.F.X.S (Financieel studiecentrum Xavier Serwy) v* the *Union royale professionnelle du crédit* (UPC).[19] C.F.X.S. acted as a credit intermediary for another company, H.S.A. In 1993 Mr M.X., business administrator of C.F.X.S., signed a leasing contract with H.S.A on behalf of C.F.X.S. according to which he was obliged to correspond monthly lease payments for the purchase of a car. Later on, H.S.A called C.F.X.S. to court because of its insolvency. Meanwhile, H.S.A. addressed to the *Union royale professionnelle du crédit* asking for the registration of C.F.X.S. in their data system, in order to evaluate and monitor its credit risk. M.X. and his wife were notified of the registration and asked the UPC to have access to their data. Once they got access, they realised that these were inaccurate and asked the UPC to rectify them accordingly. However, the UPC did not modify any data but took note that they were contested. Hence, M.X. and his wife took the UPC to the Brussels tribunal of first instance demanding the erasure of their data from the UPC databases within twenty-four hours.

The tribunal of first instance recognised the request of the claimant as legitimate and declared the UPC responsible for having registered the data erroneously. In particular, the Brussels Court underlined that the UPC's conduct was negligent in processing the claimant's data, despite of the fact that it knew they were not accurate. The Court noted that the UPC did not have to process the data it was given passively. Instead, it had to check first of all whether it could process them, in accordance with the provisions of the Privacy Act. In more general terms, the Court recognised that the right of information ensured by the Privacy Act is a fundamental right whose aim is to authorise citizens to check if any data included in the filing system is inaccurate, incomplete or non-relevant. This circumstance could originate a negative or erroneous image about the subject's personality. Thus, the data controller has to act prudently in processing data, paying special attention to the specific purpose for which data are treated. This judgment was confirmed on appeal.

[19] Tribunal de Première Instance de Bruxelles, Civ. Bruxelles (pres.), 22 March 1994. The judgment is available at: http://www.anthologieprivacy.be/sites/anthology/files/Tribunal_de_Premi%C3%A8re_Instance_de_Bruxelles%2C_22_mars_1994.pdf (last accessed 11 July 2013).

National exceptions to the EU Data Protection Directive and to the right of access to data

The Privacy Act sets national exceptions to the EU Data Protection Directive. As explained above, the application of the Act is limited in the case of processing of personal data for journalistic, artistic or literary purposes. In particular, according to Art. 3 Paragraph 3 of the Act, when these interests are at stake it is permissible to process health-related personal data, judicial and administrative data and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as data concerning sex life. This exception is in line with Art. 9 of Directive 95/46/EC which states that Member States derogate to the general data processing provisions in order to reconcile the right to privacy with the rules governing freedom of expression. As mentioned, the Privacy Act does not concern the processing of security and judicial data. This exception reflects Art. 3 Paragraph 2 of Directive 95/46/EC which establishes a different legal regime in case of data concerning public security, state security, defence and criminal matters. The Privacy Act limits the right to access and rectify data in the case of money laundering. This exception finds its counterpart in Art. 13 Paragraph 1 of the European Directive which allows Member States to restrict the scope of application of the right to the access to data and the right to notification in case it is necessary to safeguard the prevention, investigation, detection and prosecution of criminal offences or an important economic or financial interest of a Member State or of the EU (Art. 13, Paragraph 1, Subparagraphs d) and e)). Finally, the processing of personal data by a natural person in the course of a personal or household activity derogates to Art. 3 Paragraph 2 of the Privacy Act, in line with Directive 95/46/EC (Art. 3 Paragraph 2).

Compatibility of national legislation with Directive 95/46/EC

There is a strong link between the Privacy Act and Directive 95/46/EC. The interdependence between the Privacy Act and Directive 95/46/EC is apparent when comparing those provisions that define 'personal data',[20] 'data processing',[21] 'personal data filing system',[22] 'processor',[23] 'third party',[24] and 'recipient'.[25] The requirements and criteria for data processing fixed by the Privacy Act at Art. 4 (see above) are clearly stated by the European Directive. In fact, the Directive guarantees the principles of lawfulness and fairness (Art. 6 Paragraph 1 a)); finality (Art. 6 Paragraph 1 b)); proportionality (Art. 6 Paragraph 1 c)); and accuracy (Art. 6 Paragraph 1 d)). Similarly, there is a clear correspondence between Art. 5 of

[20] Art. 1 of the Act qualifies 'personal data' as any information relating to an identified or identifiable natural person. An 'identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity. This definition recalls Art. 2 a) of Directive 95/46/EC.
[21] Art. 1 Paragraph 2 of the Act mirrors Art. 2 b) of the European Directive.
[22] There is a clear correspondence here between Art. 1 Paragraph 3 of the Act and Art. 2 c) of the Directive.
[23] See Art. 1 Paragraph 5 of the Privacy Act and Art. 2 e) of the Directive.
[24] See Art. 1 Paragraph 6 of the Act and Art. 2 f) of the Directive.
[25] See Art. 1 Paragraph 7 of the Act and Art. 3 g) of the Directive.

the Privacy Act and Art. 7 of Directive 95/46/EC as regards the criteria for making data processing legitimate. Art. 9 of the Act is linked to Art. 10 of Directive 95/46/EC.[26]

Surveillance and access rights: codes of practice at national level (CCTV and credit ratings)

The use and installation of CCTV in Belgium is regulated by the *Loi Caméras* of 21 March 2007.[27] It defines the legal framework for CCTV surveillance in public and private places. The *Loi Caméras* does not apply in the case of CCTV cameras regulated by other specific laws (such as cameras installed in football stadiums)[28] and cameras installed in workplaces.[29]

According to Art. 5, the decision to install a CCTV camera in a public place is taken by the data controller, upon approval of the municipal council in which the concerned place is located. The data controller is obliged to notify this decision to the Privacy Commission and to the head of the local police. Art. 5.3 states that the notification can be done also (and at the latest) on the day before the operationalization of the camera. It can be made only by filling in an online declaration, which is available on the website of the Privacy Commission.[30] A payment of 25 euro is required whenever a new declaration is introduced, whereas 20 euro should be paid for modifying an existing declaration. The obligation to declare the installation of a CCTV camera does not apply in case the camera is located in a private place (not accessible to the public), and is used for personal or domestic purposes only. In 2012 the Privacy Commission received 115 notifications.[31] The data controller is obliged to post a pictogram (i.e.: a sign with an image of a camera) mentioning that a surveillance camera is in operation. The Royal Decree of 10 February 2008 established specific norms in this regard.[32] According to Art. 4 of the Decree, the CCTV pictogram should mention the following information in a visible and readable way:

[26] However, the Belgian Act expands somewhat the right of the data subject to be informed by imposing on the controller the obligation to make him know about the existence of the right to object to the intended processing for the purposes of direct marketing (Art. 9, Paragraph 1 c)). This clause is not explicitly stated in the European Directive but results from the transposition of Art. 14 of the Directive into the Belgian legal system.

[27] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007.

[28] Video surveillance in football stadiums is mainly regulated by the *Loi relative à la securité lors des matches de football*, 21 December 1998 (amended in 2003, 2004 and 2007). It can be find at http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1998122140&table_name=loi (last accessed 11 July 2013).

[29] In this case, it is necessary to apply the *Convention Collective de Travail* (CCT) (Collective Labour Agreement) n. 68 of 16 June 1998, concerning the protection of privacy with regard to video monitoring at the workplace. It can be found at http://www.privacycommission.be/sites/privacycommission/files/documents/01.02.02.10-cct68.pdf (last accessed 11 July 2013). For a detailed legal analysis on video surveillance in workplaces in Belgium see De Hert, Paul and Loncke Mieke, "Camera surveillance and workplace privacy in Belgium", in Nouwt, Sjaak, de Vries, Berend R. and Prins, Corien (eds.) *Reasonable expectations of privacy*?, Information Technology and Law Series, Asser Press, The Hague, 2005, pp. 167-209.

[30] The notification form can be found at https://eloket.privacycommission.be/elg/cameraMain.htm?siteLanguage=fr (last accessed 11 July 2013). In practice, this online notification system reaches both the Privacy Commission and the local police department.

[31] Commission de la protection de la vie privée, *Rapport Annuel 2012*, 2012, p. 56, available at http://www.privacycommission.be/sites/privacycommission/files/documents/Rapport-annuel-2012.pdf (last accessed 11 July 2013).

[32] *Arrêté royal définissant la manière de signaler l'existence d'une surveillance par caméra*, 10 February 2008.

(a) « *Surveillance par caméra - Loi du 21 mars 2007* » (legal basis);
(b) the name of the data controller (physical or legal person) and of his representative ;
(c) the mail address of the data controller and his email address, where necessary.

The *Loi Caméras* states that CCTV footages cannot be kept by the data controller for more than one month, unless they are used for law enforcement purposes (Art. 5.4).

The right to access CCTV footage is enshrined in Art. 12 of the *Loi Caméras*. It establishes that everyone has the right to access images that concern him/her. In order to do so, it is necessary to submit a written and motivated[33] request to the data controller. Art. 12 does not provide any additional detail as to how this right can be exercised but refers to Art. 10 of the Privacy Act. Most of all, Art. 12 does not give any further guidance which may help to define what a motivated request is or in what circumstances this criterion may be fulfilled. There is no case law at national level which provides explanations in this regard, potentially leading to a lack of clarity for data subjects in attempting to exercise their rights.

According to Art. 4 of the Belgian law on the Central Individual Credit Register,[34] physical or legal persons that subscribe a loan have the obligation to communicate to the Central Credit Register data concerning the contract as well as any insolvency notice. Moreover, every debtor can have free access to data that are kept in the Register on his or her name and to rectify them (Art. 7). Although best practices do not emerge in this respect, it is noteworthy that the Privacy Commission can play the role of mediator between the creditor and the debtor in order to assess whether the registration procedure has been carried out in accordance with law.

The promotion of access rights by DPAs and national authorities and their role in ensuring compliance to national norms

The Privacy Commission is the Belgian Data Protection Authority. It is an independent supervisory authority which acts under the auspices of the Belgian House of Representatives. Its mission is to ensure the protection of privacy and personal data, which are merged in the more general expression "vie privée". The Privacy Commission has five main tasks, namely assistance; complaint handling; enforcement; regulation and standardisation, and information. It is composed of sixteen members including one president, one vice-president, six "membres effectives" and eight substitute members.[35] They are appointed for a period of six years. The Privacy Commission is established at federal-national level.[36] Specific ah-hoc Committees are established within the Belgian DPA in order to ensure a high level of expertise, namely: *Registre national*;[37] *Autorité fédérale*;[38] *Sécurité sociale et santé*;[39] *Surveillance statistique*;[40]

[33] The Privacy Commission underlines that the request has to be "dûment motivée" (duly motivated).
[34] Belgian Parliament, *Loi relative à la Centrale des Crédits aux Particuliers*, 10 August 2001.
[35] The president and vice-president fulfil their task on a full-time basis.
[36] In addition, in 2009 it was created the *Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer*, a Commission which operates in the Flemish region only whose task is to control the electronic exchange of administrative data.
[37] This Committee is specialised in the protection of those data that are kept in the National Population Register and supervises the use of the identification numbers contained in the Register.

Banque-carrefour des entreprises;[41]and *Phenix*.[42] The main objective of these Committees is to authorise the exchange of data between administrations. In general, they are also meant to exercise a control in first line (where the Privacy Commission then assumes the second line of control). The Privacy Commission represents the third party in the relationship between data subjects and data controllers and interacts with them. Moreover, it plays an important role in interpreting national legislation concerning privacy and data protection and in proposing new laws or amendments. Hence, its activity bears a certain significance for governmental institutions, lawyers and judges.

On the one hand, the promotion activity of the Privacy Commission consists in informing citizens about national legislation on privacy and data protection and the rights enshrined therein. Detailed and exhaustive information can be found on the website of the DPA with regards to legislation on privacy and data protection in force at national, European and international level.[43] Its website contains several thematic sections on specific topics, such as surveillance cameras, biometrics, e-ID, direct marketing, the internet, cybersurveillance, etc.[44] On the other hand, the Privacy Commission engages in many initiatives to promote the protection of the "vie privée". Particularly noteworthy is the project "Anthologie de la vie privée", which was launched in 2013 to collect and classify in a systematic way all relevant sources of privacy and data protection law, including legislation, case law, doctrine and decisions of the Privacy Commission.[45] Moreover, the DPA has recently collaborated to the publication of a book for teenagers to increase their awareness of the use of internet and social media.[46]

Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights

[38] This Committee supervises the processing of data handled by federal administrative authorities.
[39] It "protects the privacy of beneficiaries of the Belgian social security network, and ensures particular supervision of the communication of health-related data". Commission de la protection de la vie privée, « Aperçu des Comités sectoriels institués au sein de la Commission vie privée », http://www.privacycommission.be/fr/node/4465 (last accessed 11 July 2013).
[40] This ad-hoc Committee supervises the communication of data transferred by the Belgian statistics office to third parties and their use of such data.
[41] It ensures the security of data processing operations within the Belgian bank of enterprises.
[42] It makes sure that data processed in the judicial fields are processed safely and confidentially.
[43] Commission de la protection de la vie privée, « Textes de référence relatifs à la protection des données », available at http://www.privacycommission.be/fr/legislation-et-normes (last accessed 11 July 2013).
[44] Commission de la protection de la vie privée, « Aperçu de nos dossiers thématiques », available at http://www.privacycommission.be/fr/dossiers-thematiques (last accessed 11 July 2013).
[45] The project "Anthologie de la vie privée" is an initiative of Willem Debeuckelaere (President of the Belgian DPA), Stefan Verschueren (Vice-president of the Belgian DPA), Paul De Hert and Serge Gutwirth (professors at the Vrije Universiteit Brussel, VUB). The anthology can be accessed on the website http://www.anthologieprivacy.be/ (last accessed 11 July 2013).
[46] The book has been published by Abimo with the title "Pro des médias!? Jeune et conscient de ses actes sur Internet".

The Belgian DPA plays an active role in ensuring that citizens are granted access to data that concern them. As the Privacy Commission states in its 2012 Annual Report, it operates with rapidity and dynamism.[47]

The website of the Privacy Commission contains a specific section which explains in practical terms how citizens can exercise their right to access data that concern them, on the basis of Art. 10 of the Privacy Act. As illustrated above, the concerned person has to submit a signed and dated access request to the data controller proving his/her identity. Hence, the Privacy Commission advises citizens to enclose with the request a copy of the data subject's identity card. In order to be valid, the request has to comply with formal requirements. Because of this, the Belgian DPA suggests using a specific letter template which can be found on its website.[48] The access request can be sent by post, fax, email (with an electronic signature) or delivered personally. The data controller has to follow up on the request within forty-five days, providing the following information:

1. whether or not data concerning the data subject are processed;
2. the purpose of the data processing;
3. the nature of the data;
4. the origin of the data;
5. information about the recipients of the data.

The data subject is entitled to exercise this right freely and no payment is due. In case the request is rejected or the data controller does not provide any reply or gives an unsatisfactory response, the data subject can submit the case to the Privacy Commission. Then, the DPA will operate actively as a mediator between the data subject and the data controller in order to ensure compliance with data protection norms. It is also possible to download from the website of the Privacy Commission a specific letter template to ask for mediation.[49] According to the figures contained in its latest Annual Report, the Privacy Commission handled almost three thousand dossiers in 2012, of which 303 dealt with mediation.[50] There has been an increase of 2.4% in the number of requests received in 2012 with respect to 2011.[51] 18.8% of them concerned credit; 13.9% principles related to privacy and data protection; 11.9% surveillance cameras; 7.9% Internet; and 5.3% direct marketing.[52]

[47] Commission de la protection de la vie privée, *Rapport Annuel 2012*, 2012, available at http://www.privacycommission.be/sites/privacycommission/files/documents/Rapport-annuel-2012.pdf (last accessed 11 July 2013).
[48] Commission de la protection de la vie privée, « Vos possibilités », available at http://www.privacycommission.be/en/node/7129 (last accessed 11 July 2013).
[49] Commission de la protection de la vie privée, « Vos possibilités », available at http://www.privacycommission.be/en/node/7129 (last accessed 11 July 2013).
[50] Commission de la protection de la vie privée, *Rapport Annuel 2012*, p. 57, available at http://www.privacycommission.be/sites/privacycommission/files/documents/Rapport-annuel-2012.pdf (last accessed 11 July 2013).
[51] Ibid.
[52] Ibid.

LOCATING THE DATA CONTROLLER IN BELGIUM

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details of 35 Belgium-based sites. In particular, the examples below are illustrative of the individual researcher's experiences conducted in Brussels and do not claim to reflect the practices of *all* data controllers in Belgium. This report illustrates some general trends noted alongside examples of good and bad practices encountered during the course of this research.

Methodological thoughts

We were able to locate details of data controllers in 33 sites, online (23 sites), asking for data in person (7 sites) and by phone (5 sites). We first attempted to find data controller details on the official websites of the concerned institutions, companies or organisations, made phone calls when they were not available online and visited sites in person when information was not available online or could not be obtained in either way. We found necessary to visit specific sites in person, in particular when we had to locate details of CCTV operators and to check CCTV signage in general. The use of emails proved to be useful especially in cases in which we could not find online neither details of the data controllers, nor any general phone detail.

In line with the methodology and purposes of this research, we were asked to pick the site located geographically closest to our place of work, to pick the site we would usually use (if the first circumstance did not apply) and lastly to conduct our investigation identifying the national market leader (if the first two options did not apply). In general, we were able to get data controller details conducting our research in the sites which were closest to our place of work. However, it was sometimes necessary to refer to the 'site we would usually use'. This was the case of the domain 'police record' for instance, when we had to locate the contact details of the police office which holds individual police records. In this case, we had to investigate the Brussels *Division Générale* (General Department), instead of local police departments. Moreover, we sometimes looked for data controller details in more than one site for a given domain, in order to double-check whether data controllers applied the same standards of transparency. This was the case of the domains 'locally-held primary school records' and 'locally-held secondary school records'. We decided to conduct this additional research to possibly confirm our findings and results.

Some of the research sites had to be analysed more than once as attempts to locate the data controllers did not succeed at first try. This was due to the fact that on the one hand some of the persons we spoke with were not aware about data subjects' rights or were not very informed about this. On the other hand, our first attempts failed because of a certain suspicion and resistance of some of our interlocutors. In these cases a 'second round' of visits was conducted.

We were asked to undertake this research introducing ourselves as lay persons, like any citizen would do. Although we did not reveal our identity and affiliation to anyone, we have to highlight that the idea of presenting ourselves as lay persons was not always very effective. In order to obtain data controller details we had sometimes to make reference to legislative texts and provisions, which proved a certain expertise from our side as regards access rights. Of course, we cannot know about citizens' awareness of access rights (which by the way is not the goal of this research). However, we believe that a citizen who asks about details of data controllers has at least a general understanding of what his or her rights are.

Overall impressions

Data controller contact details successfully identified in first round of visits	29 of 35 cases (82.8%)
Data controller contact details unable to identify in first round of visits	6 of 35 cases (17.1%)
Total number of data controller contact details successfully identified after second round of visits	33 of 35 cases (94.2%)
Total number of data controller contact details unable to identify after second round of visits	2 of 35 cases (5.7%)
Contact details identified via online privacy policy	19 of 33 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	7 of 33 (successful) cases
Contact details identified after speaking to member of staff in person	7 of 28 (successful) cases
Average rating given to visibility of privacy content online	2 – Adequate
Average rating given to the quality of information given by online content	1 – Poor
Average rating given to visibility and content of CCTV signage	2 – Adequate
Average rating given to quality of information given by staff on the telephone	1/2 – Poor/Adequate
Average rating given to quality of information given by staff in person	1 – Poor

In the first round of visits, data controllers were located in 29 of 35 cases. Although in many cases it was quite easy to identify data controller details online, information was often incomplete and unsatisfactory. Accordingly, additional research was required. At first, we were not able to find data controller details in 6 cases. In particular, this was the case of Facebook, Google and Microsoft and two banks. In addition, we were not able to find contact details of the CCTV operator of a small store. After the second round of visits, we succeeded in identifying all missing data controller details, with the exception of Facebook and Google. A few weeks ago we sent them an email through their online query system but we have not got any reply so far. We can consider this as a non-response. Thus, we have been successful in 33 of 35 sites searched.

<u>Online content</u>

Details about data controllers could be found on official websites of the institutions, organisations or companies picked up in 23 of the 33 successful sites. However, specific contact details were not always available online. Firstly, many of the website we visited had only general contact details of the concerned institution, organisation or company, without any reference to access rights. In such circumstance, we addressed to them directly by phone, email or in person. Secondly, not all research sites included privacy policies. Thirdly, almost none of the websites provided information as to how citizens can have access to data that concern them. The visibility of online privacy policies was rated as adequate, when available. Predictably, the web links to privacy policies could be found at the bottom of the web pages, in very small font. They were generally mentioned under the sections *"protection vie privéé"* (i.e.: website of the banks), *"politique de confidialité"* (website of the mobile operator) or under the more general category of *"mentions légales"* (website of the local authority and the police). Although the quality of the information provided ranged from poor to good, in general we found that specific information on access rights was definitely insufficient.

Several negative practices could be identified. In particular, the following ones got our attention:

- Local authority: the website does not give any information about neither access rights not personal data protection. The section *"mentions légales"* refers to copyright and hyperlinks only.
- Health insurance provider: the website did not include any privacy policy and did not refer to access rights at all.

We found that the websites we analysed did not provide satisfactory information on access rights. Our online research revealed that in most of the cases data controller details were not mentioned clearly and unequivocally. Moreover, there was little or no explanation about what access rights are and how data controllers can have access to data that concern themselves. As we will explain later on, in our view the lack of information represents a strategy of denial of the right of access to data and of the exercise of this right.

Public

Strategies of facilitation

We did not notice any remarkable strategy of facilitation or best practice when analysing public sites. However, we would like to mention here the case of the Police. Its website contains a web link called generally "*mentions légales*" which, among other things, provides information about data protection and access rights. It allows citizens to contact the police directly (by filling in an online form), in case they find that information on the website is incorrect or inaccessible. Citizens can consult data that are processed by the police and, if necessary, to have them rectified for free. In this case, a written, dated and signed request has to be sent to the specific address mentioned on the website of the police, together with a copy

of the ID of the data subject.[53] The website of the police provides all these explanations making also reference to the legal basis constituted by the Privacy Act of 1992.[54] Moreover, it is noteworthy that the website of the Police is available in four languages (Dutch, French, German and English).

Although the Belgian DPA (the Commission for the Protection of Privacy or Privacy Commission) did not constitute a 'site' for the purposes of this research, we contacted this institution to have clearer information about the citizens' access to police records. While showing great support, the Privacy Commission confirmed that citizens can have indirect access to these files in Belgium. Thus, data subjects can access their data indirectly in case of police records. By contrast, they can contact directly the Belgian Federal Police for having access to those personal data that are mentioned on the Police's website.

Strategies of denial

As mentioned earlier, the lack of information about data protection and access rights in particular should be considered as a strategy of denial. At present the website of the City of Brussels does not mention any information about data protection and access rights. Given our difficulties in identifying data controller details in this case, we rang the number of a certain department within the local authority. Our call was unsuccessful at least twice; hence we decided to contact them by email enquiring them about the exact contact details of the data controller. After a few days we were contacted back by an employee of the Municipality who wanted to have more clarifications about our request. While being very surprised about our query, she showed almost no awareness of citizens' right of access to data. Her surprise was also revealed from the expression "it is the first time I deal with this request" (translation from French to English). Lastly, she was not sure about who was the person responsible for handling such requests and suggested us to mention the general office's address on our access request.

Apart from the lack or inaccuracy of information about access rights, it is also important to stress that suspicion and/or resistance constitute strategies of denial. We found that police officers were particularly suspicious of us when we enquired about having access to police records. The person we spoke with told us that we should submit an access request to the Police General Department, attaching to it a copy of our ID. Then, in case our request concerns access to police records the case is handled by the Privacy Commission (as confirmed by the Privacy Commission itself). Despite the clarifications provided by the Police and the Privacy Commission, it remains not very clear what data are treated by the Police and for what purpose (which is of course out of the scope of this research). Moreover,

[53] Police Fédérale Belge, *Mentions légales, Protection des données,* http://www.polfed-fedpol.be/disclaimer_en.php (last accessed 30 July 2013).

[54] Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 [*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel]*.

we found also a certain difficulty in locating the data controller in this field. These elements contribute to frame the picture of the strategies of denial.

Private

Strategies of facilitation

Although we cannot refer to best practices in the researched private sectors, we noticed that private companies use different standards as regards the quality and quantity of information about access rights and data protection in general. We found that the mobile phone company for instance provides on its website information as to how citizens can access their own data, under the section "*Politique de confidentialité*", "*Accès aux données, correction et questions*". Although the company does not explain in detail how citizens can exercise this right, it makes clear that they can address queries to the company either in writing, by email or telephone.[55]

We were able to locate details of data controllers in 'locally-held primary school records' and 'locally-held secondary school records' with a certain ease. On the official website of the school we selected there was the web link "*images/vie privée*" which directed us to the regulation of the school as regards privacy protection. Although this document did not refer explicitly to access rights, it contained the name and contact details of the data controller.[56] Moreover, the regulation mentioned some of the provisions of the Privacy Act and made reference to a specific recommendation on image rights issued by the Privacy Commission.[57] The appointment of the data controller, the establishment of a specific regulation on privacy and data protection and references to the existing legal framework at national level are considered as best practices which should be implemented by schools, as well as by any other institutions. However, these practices are not implemented by all primary and secondary schools in Brussels.

In our view, strategies or policies of facilitation depend also on the way in which explanations and information about access rights are given. We notice that there is a certain difference in this respect among the companies we looked at. One of the banks for instance states clearly on its website that its customers have the right to access personal data that concern themselves and to get them corrected and updated. Most of all, the bank points out that "in order to exercise these rights, it is sufficient to send a written request to (the bank), duly dated and signed, to the following address …"[58] On the contrary, the statement

[55] BASE, *Politique de confidentialité, Accès aux données, correction et questions* http://www.base.be/en/node/3766 (last accessed 30 July 2013).
[56] The school regulation can be found at the following web link : http://www.lindthout.eu/fondamental/pdf/charte%20droit%20image%20WEB.pdf (last accessed 30 July 2013).
[57] The Privacy Commission, *Recommandation d'initiative concernant la diffusion d'images,* (A/2007/033), 2007.
[58] This is a translation from the French version of the bank's website, BNP Paribas Fortis, *Vie privée, Avis informatif concernant les traitements de vos données*, https://www.bnpparibasfortis.be/portal/start.asp (last accessed 30 July 2013).

concerning access rights that can be found on the website of the other bank we investigated is more articulated but actually turns out to be less clear to a lay person. It states that:

"Those responsible for processing data of a personal nature relating to the individuals in question which is communicated via the (the bank's) website are (address based in Belgium is provided), (e-mail address is provided) and, where appropriate, another (bank) company established in a member state of the European Union."[59]

Strategies of denial

We got details of data controllers in private sites while conducting our research on their official websites, in person, using the phone and via emails. Despite the fact that we were able to locate data controllers in almost all the given sites, we encountered several difficulties in obtaining these data and in conducting our research. The significant amount of data that we gathered was not due neither to the availability of these details, nor to the openness of companies in sharing them. We succeeded in getting data mainly because we visited and analysed the sites several times, sometimes more than twice. Nonetheless, in the end we failed to locate details of data controllers in two cases.

As explained earlier, we attempted to locate details of data controllers in person in all cases where we had to identify CCTV operators. While it was quite easy to find the data controller details of the CCTV operator in the Brussels transport setting, our research became more problematic for the other CCTV sites. In a first round of visits, we went to the closest metro station and looked for CCTV signage. The operator's full postal contact details are provided on the signage as per Picture 1 below. We interpret this as a good practice as we were able to locate data controller details instantly. In contrast, when we tried to locate the data controller details of the CCTV operator in bank, we found a certain resistance and scepticism. At first we spoke with one of the bank employees at the bank who had no expertise on the matter and asked one of her colleagues to help us. They were both very surprised about our request which they did not expect. We were told that the bank does not provide any detail about data controllers to anyone as this is a security issue. Then, we insisted saying that the right to access CCTV images is safeguarded under Belgian law by the *Loi Caméras*[60]and personal data are protected by the Privacy Act. At this point the employee got also a bit irritated and told us that if we wanted to have access to their CCTV footages we had to ask the police. Indeed, she told us the following "we do not give away this kind of images! Ask the police!" Given the result of this first visit, we contacted another bank, sending an email to an address we found on the signage at the entrance of the bank (see Picture 2 below). We got a reply a few days later which mentioned the details of the CCTV controller. Although with some difficulties, we were able to find the contact details of the CCTV controller in a large supermarket/department store in the first round of visits. At the beginning we decided to talk to the security guard who was in the store, assuming that he could provide us with the required information. While being surprised about our request, he tried to somehow change

[59] Quoted from the company's privacy policy.
[60] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007.

the subject of our conversation saying that all CCTV cameras that are installed in the outside area surrounding the store are operated by the police. On the one hand, he showed understanding for our privacy concern and was at ease with our questions. However, on the other we noticed that he had almost no knowledge about access rights and the Belgian legislation on this matter. We were a bit stunned by this lack of knowledge, as we assumed that security guards were aware about the legislative framework which regulates the use of CCTV in Belgium. In the end, the security guard suggested us to ask the question to the customer service of the store that provided us the contact details of the CCTV operator. We encountered even more difficulties when we had to locate the data controller of CCTV in a small/local store. Our question was left unanswered at least twice as employees of the selected shops had no clue about the name of the data controller and about access rights in general. We succeeded in identifying data controller details in the third round of visits. Lastly, in order to get information about access to CCTV footage in a public space/city centre, we had to address the local Police department. A police officer told us that a formal access request has to be addressed to this department. However, access to these images is allowed upon approval.

The most remarkable strategies of denial in accessing data controller details were found when encountering Microsoft (email data), Facebook and Google (search engine). We decided to contact Microsoft in order to get access to our own data concerning an Hotmail account. At first, we made an extensive research on the company's website to find more information in this respect. Microsoft has elaborated an "Online Privacy Statement" illustrating briefly its policies as regards the collection, use, sharing and access of personal information, the communication of promotional emails and advertising, the collection and use of children's personal information, the use of cookies and web beacons, spams, etc.[61] We found that the information on access rights under the section 'accessing your personal information' was very vague and incomplete. In addition, it explained mainly how to 'add', 'update', 'review', 'edit' and 'delete' a profile or other data contained therein but did not give the user details about how to exercise the right of access to data in practice. Hence, we tried to contact the company directly. There was no telephone number on the privacy statement page of Microsoft, so we had no choice than to send them an email via the online web form used for general queries. On the form we explained that we wanted to submit an access request and asked them to kindly provide us with the name and contact details of the data controller. Within 24 hours we received from Microsoft a reply, saying among other things that:

> "in order to release member information regarding an MSN or Windows Live Hotmail account, Microsoft must first receive a valid subpoena, court order, or search warrant from law enforcement or a civil attorney. Please address the appropriate legal document to the Microsoft Corporation and include all pertinent information for Microsoft to identify the particular MSN or Windows Live account(s) you seek to locate. The legal document may be faxed to (425) 727-3490 for MSN and Windows

[61] Microsoft, Microsoft Online Privacy Statement, http://privacy.microsoft.com/en-us/fullnotice.mspx#accessing (last accessed 30 July 2013).

> Live Properties or (650) 693-7061 for Hotmail and Passport. Law Enforcement Officials should refer to the Microsoft Online Services Legal Request Hotline. In the United States: (425) 722-1299; outside the US: (1) (425) 722-1299."

We replied to this email making clear that we did not have any privacy issue related to our Hotmail account and that we did not want to start any legal action against Microsoft. Still, we explained that we wanted simply to introduce an access request and that we needed the data controller details in order to do so. Further to this second email, we have not heard back from Microsoft and we can now conclude that this is a non-response. The only information we have been able to obtain is the fax number which we will use to send them the access request in the next phase of the research.

We had a similar experience when attempting to locate the data controller details of Google. We initially made a search on the company's official website and found that, like Microsoft, Google implements certain privacy rules.[62] Among other things, they illustrate what data are collected by Google and how they are used and shared. These rules contain also a section on access and modification of personal data. Like Microsoft's privacy principles, Google's rules place great emphasis on the user's right to edit, update, add and review personal information rather than on his right to have access to personal data that concern himself. In fact, these rules do not deal with data access as a right but as a possibility which is given to customers whenever they find that their own data are inaccurate or outdated. In Google's view, access and rectification are free *services* (italics added).[63] We were not able to find data controller details on this web page. Hence, we decided to contact the company directly. In order to do so, we had to follow the FAQ link, where a contact form was available. We believe that the choice to insert this form under the section 'FAQ' is definitely a strategy of denial which detaches the data subject from the data controller and makes the exercise of access rights difficult or almost impossible. Thus, we filled in the form and sent it to Google. We never got a reply back from them and we consider this as a non-response.

Similarly, our attempt to locate data controller details of Facebook was unfruitful. We looked for these details on the website of the company but unsurprisingly we were not able to find them. Like Microsoft and Google, Facebook has developed its own policy on the use of personal data.[64] Written in small fonts, this long set of rules does not provide satisfactory information about how the user can access personal data. These rules include also a section called 'access requests'. It explains that data subjects can access personal data by accessing their own account and that Facebook users can also request a copy of their own data to the company. Although we found this function very useful, there was not sufficient information

[62] Google, Règles et Principes, Règles de confidentialité, http://www.google.com/policies/privacy/ (last accessed 30 July 2013).
[63] Ibid.
[64] Facebook, Data Use Policy, https://www.facebook.com/full_data_use_policy (last accessed 30 July 2013).

on access rights on the website.[65] Hence, we contacted Facebook by email via their online contact form.[66] We never got a reply back from them and we consider this as a non-response.

CCTV and signage

The deployment and use of CCTV in Belgium is regulated by the *Loi caméras* of 21 March 2007 (hereafter the Law).[67] This legislative tool applies to any fixed or mobile system of observation whose purpose is to prevent, record or detect crimes against persons or property (Art. 2). It is not applicable in the case of cameras whose use is regulated by specific legislation and of camera surveillance in the workplace (Art. 3).[68] The Law sets detailed provisions as regards the installation and use of fixed and mobile cameras (Chapter III and III/1 of the law respectively) and some common rules that apply to both kinds of cameras. Although the main purpose of the Law is to combat crime in a preventive logic, it recognises the right of access to surveillance cameras images. In fact, Art. 12 states that any person who has been filmed by a surveillance camera can exercise this right by introducing an access request to the data controller, in accordance with Art. 10 of the Belgian Privacy Act.[69] Accordingly, the data subject has to submit a written and motivated access request to the data controller, attaching to it copy of his/her identity card. However, the right of access to images that have been taken in closed places accessible to the public or not accessible to the public is granted to the data controller only or to the person acting on his behalf (Art. 9).

The Law of 2007 is complemented by the Royal Decree of 10 February 2008 which sets specific rules as regards the CCTV signage.[70] Apart from certain features in terms of size, the CCTV pictogram should mention the following information (Art. 4 of the Decree):

1. the quote "*Surveillance par caméra - Loi du 21 mars 2007*";
2. the name of the data controller and of his representative, in case;
3. the mail address and, in case, the electronic mail of the data controller.

[65] In order to meet privacy and subject access requests, Facebook has also activated a self-download tool which allows users to download specific files which contain the data subject's data. However, as previous research has found, this tool does not actually provide all personal data (i.e. *Europe v. Facebook*).
[66] Facebook, Help, Contact, https://www.facebook.com/help/contact/?id=173545232710000 (last accessed 30 July 2013).
[67] Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, ibid.
[68] The deployment and use of surveillance cameras in the workplace in Belgium is regulated by the Collective Labour Agreement No. 68 of 16 June 1998 which was adopted by the National Labour Council and concerns the protection of privacy in the workplace [*de collectieve arbeidsovereenkomst No. 68 van 16 juni 1998 gesloten in de Nationale Arbeidsraad, betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats*], made obligatory by the Royal Decree of 20 September 1998, Belgian Official Journal, 2 February 1998. See De Hert, Paul and Mieke Loncke, "Camera surveillance and workplace privacy in Belgium", in Nouwt Sjaak, de Vries Berend R. and Corien Prins, *Reasonable expectations of privacy?*, ITeR, The Hague, 2005, pp. 167-209.
[69] Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, ibid.
[70] The Belgian Head of State, *Arrêté royal définissant la manière de signaler l'existence d'une surveillance par camera*, 10 February 2008.

The CCTV signage of the sites we analysed complied with the rules of the Royal Decree. In particular, the signage of the company STIB-MIVB and of the Bank Paribas Fortis was in accordance with law (pictures 1 and 2 respectively). However, in sites other than those investigated for the purpose of this research, it was also easy to find unlawful pictograms, such as the signs shown below in pictures 3 and 4.

Picture 1: Signage in a transport setting

Picture 2: Signage in a bank

Picture 3: Signage at the entrance of a corporate office

Picture 4: Signage at the entrance of a private building

Concluding thoughts

This research shows that data subjects experience several difficulties in accessing their own data and so in exercising the right of access. Although we were able to locate data controller details in almost all sites we visited, our research experienced a certain rate of failure in the first round of visits. As discussed earlier, we could not conduct this research as truly lay persons. Accordingly, it would make sense to argue that the rate of data controller details that we would have identified in 'normal' conditions would have been probably lower. Strategies of denial and facilitation influence the identification of data controller details and thus the exercise of the right of access to personal data. The spectrum of strategies of denial and facilitation is quite broad and it is not possible to make an exhaustive list out of them. However, taking into account the finding of our research they can be summarised and clustered as follows,

- Strategies of denial:
- any difficulties in locating data controller details;
- lack of information;
- lack of clarity;
- lack of support and assistance;
- lack of knowledge about legislation;
- lack of expertise about the handling of an access request;
- suspicion, skepticism and resistance;
- irritation;
- indifference.

- Strategies of facilitation:
  - appointment of the data controller;
  - establishment of specific regulations on privacy and data protection;
  - mention of legal norms and reference to laws and legal provisions;
  - access to information;
  - clarity and accuracy of information;
  - availability of information in foreign languages (or languages other than national languages);
  - support and assistance of the national DPA;
  - likeliness of the data controller to make himself available and possibility of the data subject to reach him.

Difficulties of data subjects in getting data controller details prevent and dissuade them from submitting access requests and thus from accessing data. This increases the data subject's perception of having lost full control over his own personal data. Moreover, the detachment of the data subject from the data controller generates a gap between them and an imbalance in their mutual relationship. In this circumstance the balance of power between the data controller and the data subject is somehow affected and the right of access to data seems to be

degraded to a mere presumption left to the discretion of the data controller. Of course, the question as to what extent access rights are nullified by strategies of denial is an open one which deserves a separate analysis.

SUBMITTING ACCESS REQUESTS IN BELGIUM

Introduction

This report illustrates the main results and findings emerging from the phase of the study which consisted of submitting subject access requests. After having located data controllers earlier in the study, we narrowed the sample and proceeded to exercise the right of access to personal data in practice. This empirical phase of the research was tackled by introducing access requests to data controllers. This 'access rights exercise' revealed the many difficulties and obstacles in 'operationalising' the right of access to personal data in Belgium, which are described in this comprehensive report. Similarly, this study highlights specific practices of facilitations implemented by data controllers, where applicable. Restrictive and facilitative practices are reported providing ethnographic data, transcribing verbatim and quoting from correspondence with data controllers where appropriate.

This report consists of a number of main sections. The first section will refer to the methodology used to develop the selected cases and sites. The next section will provide a general overview and illustrate emerging trends, whereas the following part will present quantitative and qualitative data. Specific case summaries will be presented in the next section with some of these focussing on CCTV. The final section will present concluding thoughts, as well as general reflections on access rights.

Methodological issues

The VUB analysed 19 sites, which are outlined in the table below:

	Public/Private	**Site**
1	Public	CCTV in an open street
2	Public	CCTV in a transport setting
3	Public	CCTV in a government building
4	Private	CCTV in a large department store
5	Private	CCTV in a bank
6	Public	Local authority

	Public/Private	**Site**
7	Public	Vehicle licensing records
8	Public	Police criminal records
9	Public	ANPR
10	Private	Banking records
11	Private	Credit card records
12	Private	Loyalty card (supermarket)
13	Private	Loyalty card (department store)
14	Private	Loyalty card (air miles)
15	Private	Mobile phone carrier
16	Private	Advanced passenger information
17	Private	Facebook
18	Private	Microsoft
19	Private	Google

This report presents in detail those cases were particularly interesting and from which striking practices in data access emerged. The remaining cases are presented more briefly but these generally reflected experiences that are identical or similar to the ones we encountered in the development of the cases described in detail below.

The bulk of our access requests were sent in October 2013. Access rights requests were sent by post to the concerned data controllers. All requests were written and filed in French and/or Dutch, in order to test the likelihood of companies and multinationals to fulfil the expectations of any Belgian citizen who would have introduced the same access request.

Recalling the provisions of the Belgian Privacy Act (in particular Article 10)[71] and of Directive 95/46/EC (in particular Article 12),[72] we asked data controllers to provide us with the following:

- Information as to whether or not personal data had been processed;
- Information as to the purposes of the processing;
- Information as to the origin of those data (where and how data controllers got them);
- Information as to the categories of data concerned;
- The recipients or categories of recipients to whom the data had been disclosed;
- Information as to the data disclosed to third parties;
- Knowledge of the logic involved in any automatic processing of data in the case of automated decisions and how it was applied to the concerned data processing.

While referring to Article 12 of the Belgian Camera Act,[73] in the case of access request to CCTV footage, we asked data controllers to provide us with the following:

- Access to CCTV footage;
- Information as to the images shared with third parties, where applicable;
- Information as to the categories of recipients of those images;
- Knowledge of the logic involved in any automatic processing of data in the case of automated decisions and how it was applied to the concerned data processing.

According to Article 10 of the Belgian Privacy Act, data controllers were supposed to follow up on our request without delay and at the very latest forty-five days after receipt of the request. Reminder letters were sent to all those data controllers who did not react to our requests within the terms prescribed under Belgian law. In this second communication we asked data controllers to provide us with the required information as soon as possible and within 7 days of the receipt of our second letter. The letter also stated that should we fail to obtain a response within that time, we would seek to file a complaint before the Privacy Commission (Belgian DPA).

Complaints were submitted to the Privacy Commission in the following cases:

- Data controllers did not follow up on our access right request and reminder letter by the due time;
- We did not deem the answer provided by data controllers as satisfactory;
- Data controllers refused to provide us with the required information.

General overview and emerging trends

[71] Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)*.

[72] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in OJ L 281/31-39, 23.11.95.

[73] Loi du 21 mars 2007 *réglant l'installation et l'utilisation de caméras de surveillance* (Loi Caméras).

As we will explain in the following sections, our experience in submitting access requests in Belgium revealed that data controllers do not facilitate citizens' access to their personal data. Rather, they have put in place numerous strategies of denial and practices which restrict the exercise of access rights. Generally speaking, we encountered a number of difficulties in carrying out our access rights exercise. Firstly, it was not easy to locate data controllers especially in the case of multinational corporations such as Google, Facebook and Microsoft (this aspect is stressed in the case summaries below). Neither private companies nor public bodies explained on their websites the procedure data subjects had to follow in order to introduce access rights requests. Guidance was almost absent and information was sometimes unclear and confusing.[74] Data controllers did not react to our access requests promptly. Some of them did not respond until the very near end of the time limit. Others did not act at all and simply ignored our request. Accordingly, data controllers showed unreceptive, unresponsive and uncooperative attitudes. As regards access to CCTV images, data controllers were suspicious about our request and gave the impression that our requests were illegitimate. As a consequence, they prevented and discouraged us from exercising the right of access and thus restricted our ability to exercise our informational rights. Given this unsatisfactory feedback, we had to resubmit our requests. Not all data controllers gave us response after this second submission. As a consequence, we filed several complaints with the Privacy Commission.

In total, complaints with the Privacy Commission were filed in the six cases mentioned as follows:

- loyalty card – large supermarket
- loyalty card
- loyalty card – air miles
- mobile phone carrier
- advanced passenger information (via airlines)
- Facebook

Quantitative and qualitative data

Only 11 data controllers out of 19 replied to our access requests within the legal time limits when we contacted them in the first instance (about 57% of the total). Many of the replies we received in this first stage were unsatisfactory and/or unclear, so we contacted the concerned data controllers again asking for clarifications. In particular, in four cases a new letter to data controllers was sent in which we requested clarifications. In eight cases data controllers did not respond at all to our access requests. Reminders were sent to those data controllers who did not react to our requests. After that, we received five (late) replies by data controllers that at first had ignored our requests. As such, in three cases we never received any response

[74] Difficulties related to the lack of information and clarity were overcome thanks to the support provided by the Privacy Commission. Detailed and exhaustive information on access rights are available on its website. In addition, here we found also templates of access rights requests and of requests of mediation by the Privacy Commission.

despite several attempts to submit our access requests. These cases were reported to the Privacy Commission.

After one or more attempts to get in contact with data controllers, in the end we were able to get access to personal data in the following cases: local/city/municipality authority; vehicle licensing; banking records; credit card records; loyalty cards (air miles); Microsoft. Moreover, further to the mediation of the Privacy Commission, we were also able to get access to personal data processed by a mobile phone carrier. Remarkably, as we will underline in the section of this report analysing CCTV sites specifically, we did not succeed in getting access to any of the CCTV footage of us from either public or private systems. As a consequence, data controllers refused to grant access to personal data in the following cases:

- CCTV (public) – open street city centre system
- CCTV (public) – public transport
- CCTV (public) – government building
- CCTV (private) – large department store
- CCTV (private) – bank
- police (criminal intelligence)
- ANPR (police/border/highway)

As mentioned above, we introduced six formal access rights requests to the Privacy Commission, out of the 19 access rights sites the VUB was asked to analyse. It follows that more than 30% of our access requests resulted in a complaint to the Belgian DPA. In addition to that, we contacted the Privacy Commission at least three times by phone asking them clarifications and additional information as to how our requests had to be handled by data controllers. The support of the Privacy Commission was crucial in this. Of the six requests sent to the Belgian DPA, four have been already processed in a prompt and satisfactory way, with regards to the following sites: loyalty card – large supermarket; loyalty card – air miles; mobile phone carrier; advanced passenger information – via airlines. Thus, at present two complaints are still pending before the Belgian DPA.

Case by case analysis

<u>Public – Facilitative Practices</u>

Local/city/municipality authority

I contacted administrative authorities of the local authority in order to get access to personal data about me processed by them. Contact details of the demographic department of the Municipality were not very easy to find on the general website of the local authority. I was able to find them after having clicked five times on the right icons. The website of the local authority did not provide any information about how citizens could have access to personal data processed by the administration or to data stored in the population register. Hence, we contacted the Municipality and sent a formal access request asking for access to those very data. A first request was sent in early October 2013. We did not receive any reply within the

legal term of forty-five days. A second reminder letter was sent on 2 December. A few days after that, I was contacted by a department from the local authority. The letter of the data controller consisted of two main pages. The first provided details about the categories of persons who are entitled to have access to the population register. The second page listed all data about me which are processed by the local authority. Data were grouped into two categories, namely legally compulsory information and complementary information. The first category of data concerned my name, address, date of birth, place of birth, marital status, profession, citizenship and other essential personal data about me. This first set of data indicated also the date when I registered as a resident at the local authority. The second category of data related to my family and reported the names of my parents and my place of birth. Moreover, the number of my residence card was mentioned, as well as data about when it was released.

As mentioned here above, the local authority did not reply to my access request in due time. However, their letter was sent just after the prescribed deadline. Despite this delay, their reply was clear and detailed in all its elements. This shows us a certain experience and competence of the local authority to handle access rights requests. Although in the first instance my request was ignored, the organisation has a standardised, formal request procedure to deal with access requests. Nonetheless, this case shows that the onus of getting access to personal data is basically on the data subject who has to chase a response from the data controller pro-actively despite the clear existence of a formalised procedure to respond to access requests.

Vehicle licensing

In order to get access to our personal data for this site we contacted the public office for mobility and transport. The office replied to our request disclosing the required data. They made clear that personal data concerning vehicle registration are transferred to competent authorities only, namely the Police, the judicial authority, federal public services and the vehicle registration holder. Their reply did not contain any information about automated decision making. Hence, we contacted them by phone. They confirmed that no automated decision had been taken when using our data.

Public – Restrictive Practices

Police criminal records

According to Article 13 of the Belgian Privacy Act, data subjects can have access to police records in an indirect way only, by contacting the Privacy Commission and not the Belgian police directly. The procedure that should be followed in this specific circumstance is described by the royal decree of 13 February 2001.[75] In October 2013, we introduced a formal access request to the Belgian DPA (the Privacy Commission) asking for access to police records and any files processed by the police about me. The Privacy Commission replied to this request promptly, within a few days after my enquiry. My access request was

[75] In particular at Articles 36 and ss. of the *Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'egard des traitements de données à caractère personnel*, 13 February 2001.

considered inadmissible and was rejected. Referring to the provisions of the above-mentioned royal decree, the Privacy Commission pointed out that my access request did not contain all information requested by law in order to be considered as valid and legitimate. In particular, it did not mention details about the police authority or the specific police service which processed my data. Moreover, the Privacy Commission highlighted that my request did not contain any reference to the data to which I sought access such as their nature, origin and the circumstances in which the police obtained them. According to Article 37 of the royal decree all these elements have to be mentioned on the access request letter addressed to the Belgian DPA, otherwise it can be rejected. So the Privacy Commission did so.

Being compliant with national legislation, in this case we could only take note of the decision of the Privacy Commission. This experience shows that the access to personal data processed by the police is allowed in specific circumstances only, when the data subject has a real and concrete concern linked to his previous criminal record. Accordingly, the Belgian legislation does not allow Belgian citizens to know if the police might be processing personal data about them. In other words, data subjects cannot submit 'general' or 'exploratory' request but rather specific requests concerning a particular issue. In this case, national legislation creates a sort of fictitious presumption that the data subject has a criminal record, substantiated by concrete evidence. If so, the concerned person has to prove that the police processes or processed data about him/her. Thus, in this case the mere research purposes linked to my access request were not compatible with national requirements and provisions.

Hence, the Belgian legislation sets significant limitations to the right to have access to personal data if data are stored in police files or police records. In this case, the provisions established under the Belgian law make the scope of access rights very vague and unclear. Access rights are basically meant to allow data subjects to take control of their data by finding out what is held about them, should any data indeed be held about them. If legislation requires data subjects to know what is held about them and by whom *before* they can even enquire about this, then the right of access loses somehow its *raison d'être* and becomes a tautology.

ANPR

We encountered difficulties in having access to images taken by ANPR cameras which are somehow similar to those described below when investigating CCTV sites. Several ANPR devices are installed in Brussels and in particular in the city centre.[76] We drove through the main roads of the centre. Then, we sent an access request to the police requesting access to ANPR footage taken by cameras installed in the Louise tunnel which displayed our number plate. The police replied to our request saying that those ANPR cameras were installed merely for the detection of suspected vehicles. As such, access is usually granted in the framework of a judicial proceeding only. As a consequence, our access request was refused on the basis of that only law enforcement may have access to this type of data. This reasoning recalls the reason for denial of other CCTV footage (see further below).

[76] A detailed description of the deployment of ANPR cameras in Brussels and in Belgium can be found in the IRISS report concerning the impact of surveillance on democratic and open societies, issued from WP3.

Private – Facilitative Practices

Advanced passenger information

In order to get advanced passenger information, I sent a letter addressed to the national main airline operator. I did not encounter major difficulties in locating the data controller. I found the name and address of the data controller on the main website of the company, by clicking on the link "security and privacy policy". As a second step, I submitted a formal access request by sending a letter in early October 2013. A few days after my enquiry, I was contacted by phone by a person working within the Legal Department of the company. He asked me about why I introduced such access request and whether this was linked to any specific concern about data protection from my side. I replied by saying that it was a 'simple' access request, not linked to any specific issue or concern. One month later, I received a formal reply to my request by post. Brussels Airlines confirmed the company processed data about me, in particular, details about my name, surname, gender, email address, phone, country of residence and language. Their letter made clear that these data had been communicated by me once I made reservations online of products or services provided by Brussels Airlines. As the company pointed out, these data were processed by the company itself for the sole purpose of providing services which I had requested. The company did not process any of my data for marketing purposes as I did not request to receive advertising material from them and did not subscribe to their loyalty card programme. Moreover, the letter stated that no automated decision had been taken by using my personal data[77]. Lastly, Brussels Airlines remarked that my personal data had been communicated only to companies acting on behalf of the company and under its exclusive authority in order to provide the required service.

Although we were quite satisfied with the reply given by the airline operator, we noticed that it did not mention explicitly the name of those third companies to which personal data had been transferred. Hence, I contacted the company again asking for clarifications in this regard. The company answered this second enquiry saying that, in their view, their first letter contained all required information and so that they had performed all duties prescribed by Belgian law on access rights. This was true, considering that the Belgian Privacy Act prescribes that data controllers have the right to obtain from the data controller information regarding the "categories of recipients the data is disclosed to" (Article 10, § 1 a)). However, the European Directive 95/46/EC tends to broaden a bit more the scope of the right of access saying that information to the data subject concerns "the recipients *or categories of recipients* to whom the data are disclosed" (Article 12, a)). In order to dispel any doubts over this issue, we contacted the Belgian DPA asking whether the reply of the data controller to our access request was compatible with Article 12 a) of Directive 95/46/EC. The Privacy Commission answered that data controllers have the legal obligation to inform data subjects about the

[77] Whether this assertion is true is unclear given the existence of 'no fly' lists and other similar procedures. However, one may assume that such processes involve some form of human intervention, rendering them not wholly automated.

categories of recipients to whom data have been communicated and not necessarily about the recipients. Thus, it recognised that the reply provided by the conpany was compliant with Article 10 of the Belgian Privacy Act.

Although it is lawful for data controllers to provide information about the "recipients *or* categories of recipients" indistinctively, this expression gives data controllers significant discretion when handling personal data. This discretionary power creates an unbalance in the relationship between data subjects and data controllers which, in such a way, might dissimulate their data protection policies and practices. The distinction between categories of recipients and recipients matters for data subjects. In cases where information about the categories of recipients only is provided, data subjects are not given the exact names of companies who process or may process their personal data. Hence, in this case data subjects can only rely on the assumption that data controllers are acting in good faith but without having any evidence to prove this. More generally, from the perspective of data subjects the expression "recipients or categories of recipients" denotes a certain lack of transparency in legislation and practices on access rights. Thus, as it stands now, this vagueness in the European legislation on access rights on the one hand makes practices of non-disclosure legitimate and on the other considerably weakens data subjects' position and data access claims.

Loyalty card (air miles)

We contacted another airline operator in order to get access to personal data processed by the company within the scope of the membership to their loyalty card scheme. A few days after the notification of the request, I was contacted back by the company. The company provided me with a transcript of all personal data about me which were associated with the programme. Their reply stressed that "data was only transmitted according to the (loyalty card scheme) Terms and Conditions to co-publisher and partner companies". Given the ambiguity of this expression, we contacted the Privacy Commission by phone asking whether it was compliant with Article 10, § 1 a) of the Belgian Privacy Act and Article 12, a) of the European Data Protection Directive. Like in the case of advanced passenger information illustrated above, the Belgian DPA confirmed that the concerned company acted lawfully. The vagueness of expressions such as "co-publisher and partner companies" gives a clearer idea about the extent to which the lack of distinction between recipients and categories of recipients weakens the position of data subjects.

Loyalty card (supermarket)

We introduced an access requests to a large supermarket chain in early October 2013 claiming access to our personal data. We did so by reason of our affiliation to the services linked to the company's "Bonus card". We did not receive any reply within the time limit prescribed by law. Hence, we contacted the company again in early December 2013 asking them to reply to our request within seven days. Being ignored for the second time, we addressed our request to the Privacy Commission. After that, the company contacted us by phone. They looked for my data in their databases but the search did not match any result.

Thus, the company concluded that no personal data had been processed about me. Although this might indeed be the case, it is important to note that cards like the above-mentioned "Bonus card", although anonymised, could keep record of data concerning product consumption and data could be used for marketing purposes.

Microsoft

We encountered several obstacles when attempting to get access to personal data held by Microsoft. As stressed in our attempts to locate data controller contact details, one of the main difficulties arose from the location of the data controller. Provided that no information in this regard was available on the website of Microsoft, we had to contact the company directly via their online web form for general queries. Although we did not succeed in obtaining accurate details of the data controller, Microsoft provided us with a fax number. This number is, according to Microsoft, usually used for introducing legal claims on the basis of a "valid subpoena, court order, or search warrant from law enforcement or a civil attorney".[78] Even though we did not introduce any legal claim of such kind, we used this fax number to submit our access request as it was the only reference we were provided with.

The access request was faxed in October 2013. We did not receive any reply from Microsoft within forty-five days from the notification of the request. Hence, a second fax was sent almost two months later reminding and chasing the data controller to provide us with feedback within 7 days. In early December 2013, I was contacted by phone by an Advocacy Manager of Microsoft. She asked me additional details about my request and in particular about the Microsoft account which originated my complaint. Moreover, she enquired about the reasons why I sought access to my personal data. I replied saying that this is a right data subjects have according to national legislation. Soon after our phone conversation, the Microsoft Advocacy Manager contacted me by email explaining that her colleagues from the Privacy Department in the United States were processing my request and had started all necessary searches. I had many email exchanges with the above-mentioned Microsoft Advocacy Manager in December 2013 and January 2014 (I counted more than fifteen emails), but did not get any substantial feedback on my access request. On 23 January the Privacy Department Team of Microsoft in the United States asked for additional information, as the search they had conducted until that moment did not enable them to locate any records in their data bases. Their reply of 23 January reads as follows.

> "We have completed our search of databases within Microsoft for the unique personal information you provided with your request, and did not locate any records. Please be advised that our search was limited to the information you provided. If you have Microsoft accounts associated with email addresses not included in your request, we cannot provide data related to any such account(s) until you have notified us of their existence and proved your ownership of the account(s). We hope this information is satisfactory to you. Thank you for taking the time to reach out to Microsoft".

[78] This is a quote from the official reply we received from Microsoft.

Hence, I gave them additional data, namely my email address associated with a Microsoft account. The US Privacy Team started a new search and then finally responded to my access request on 7 March. Some excerpts of their reply are reported here as follows.

> "To confirm our original response, we advised that we conducted a search of databases within Microsoft for the unique personal information you've provided with your request, and found the following information:
> - Your full name, email address, and information associated with your account, such as account name, account ID, account type, account status was located in a customer service support database.
> - Your full name (first and last name), date of birth, gender, region, country, postal code, time zone, preferred language, and email address was located in the Microsoft Account database. If you wish to view/edit that information please go to http://account.live.com/ and log in with the e-mail address in question.
> - Information concerning the categories of recipients with whom personal information may be shared is provided in the Microsoft Privacy Statement.
> - Lastly, with respect to your request for information concerning whether Microsoft used your data to make automated decisions, please be advised that we conducted a search for the information you provided in your request could not locate any such data".

We consider the reply given by Microsoft as satisfactory, although only partially so. It is worth noting that their response made clear not only the categories of data held by the company but also the specific database in which they were stored. However, no transcript of the concerned data was attached to their reply. As for the sharing of data with third parties, Microsoft did not state clearly whether and with whom my data had been shared. They asserted simply that they implement their privacy policy.[79] According to the Microsoft Privacy Statement, personal data are not shared with third parties without the data subject's consent. The cases in which personal data may be shared with third parties are described in detail on the company's website. Microsoft may share or disclose personal information in the following cases:

- "With other Microsoft controlled subsidiaries and affiliates.
- As part of a corporate transaction such as a merger or sale of assets.
- With vendors or agents".[80]

Moreover, Microsoft may also share or disclose personal information, including the content of data subjects' communications:

[79] Microsoft, Microsoft Privacy Statement can be found at the following link: http://www.microsoft.com/privacystatement/en-us/core/default.aspx (last accessed 10 March 2014).

[80] Microsoft, Other Important Privacy Information, http://www.microsoft.com/privacystatement/en-us/core/default.aspx?Componentid=pspOtherInformationModule&View=Description (last accessed 10 March 2014).

- "To comply with the law or respond to legal process or lawful requests, including from law enforcement and government agencies.
- To protect the rights or property of Microsoft or our customers, including enforcing the terms governing your use of the services.
- To act on a good faith belief that access or disclosure is necessary to protect the personal safety of Microsoft employees, customers or the public".[81]

Private – Restrictive Practices

Facebook & Google

Apart from Microsoft, we contacted two multinational companies which process personal data, namely Google and Facebook. We encountered similar but even greater difficulties in carrying our access requests exercise in these two cases. The first difficulty concerned the location of the data controller. Facebook and Google have offices in Brussels and at thus we initially sent our access requests to these satellite offices of the companies. In response, both Facebook and Google came back to us saying that access requests should be addressed to their headquarter offices in Dublin and Mountain View, respectively and we did so. Facebook Ireland sent us a quite unsatisfactory reply to our access request as it did not mention the personal data whose access we claimed. Their reply simply stated that data could be accessed, edited and deleted by entering our Facebook profile and the possibility of submitting a request to the organisation directly was not countenanced. Hence, we contacted the Privacy Commission asking for mediation. At present, the case is still pending before the Belgian DPA. To date, we have not received any reply from Google USA with regards to our access request.

Loyalty card (department store)

We submitted a request to a department store as members of their loyalty card scheme. The company disregarded our request twice and hence we filed a complaint to the Belgian DPA. At present the case is still pending and so far the company has not provided any reply to our access request.

Mobile phone carrier

An access request was sent to a mobile phone carrier, one of the main mobile phone operators in Belgium. We contacted them twice, in October and December 2013 but our request was ignored. Hence, we asked the Privacy Commission to get access to the concerned personal data. The Belgian DPA got in contact and mediated with them. Finally, the company replied to our request and provided us with the required personal data. We did not deem their reply satisfactory as it did not mention whether an automated data processing had occurred. As a consequence, we got back to the data controller who advised that such processing does not

[81] Ibid.

take place. Although access to personal data was granted, the company showed a certain lack of experience in processing access requests.

Banking & credit card records

We sent a data access request to our bank in early October 2013 and then in early December 2013 as at first our request was ignored. Following our second letter, we received a reply from the bank. They sent a detailed transcript of all data they held about me which concerned not only my personal data and bank account numbers but also the name of my employer and date of appointment. Information about third-party data sharing and automated processing of data was not provided in their reply explicitly. Hence, I contacted the bank by phone and asked these questions directly. They denied such practices related to the use of my personal data. As such, while we received our personal data, we only did so after a second attempt. Our query regarding third party data sharing practices and automated decision making were ignored, necessitating us to pursue the data controller for an answer. In summary therefore, we consider the data controller to have employed strategies of denial in this case and demonstrated poor practice in general.

CCTV

Article 12 of the Belgian Camera Act states that any person who has been filmed has the right to get access to CCTV images. In order to do so, the data subject has to submit a written and motivated[82] request to the data controller. Referring to this provision, we submitted several requests claiming access to images of CCTV cameras located in public spaces. In response to our requests, none of the concerned data controllers granted access to CCTV footage. The reason for denying such access was based on a number of arguments including the fact that the footage had been erased, that our request lacked a suitably motivated reason (such as the occurrence of a crime) and that footage is only shared with law enforcement officers.

Given the negative feedback we received from data controllers, we contacted the Privacy Commission asking whether the responses we received from CCTV data controllers/operators were compliant with the Belgian law and in particular with Articles 12 and 9 of the Camera Act. The Privacy Commission stressed that all access requests to CCTV footages made by data subjects have to be motivated, as prescribed by the Belgian law. Accordingly, data requests that lack a "proper" motivation have to be rejected. This is also confirmed by the legal note issued by the Privacy Commission in 2010.[83] Here the DPA made clear that the duty to motivate access requests is meant to give the data controller the possibility to balance the interest of the data subject against security. Thus, the Privacy Commission concluded that the refusal of our access requests was legitimate in accordance with Art. 12 of the Belgian Camera Act.

CCTV (private) – large department store

[82] The Privacy Commission underlines that the request has to be "dûment motivée" (duly motivated).
[83] Privacy Commission, *Note relative à la loi réglant l'installation et l'utilisation de caméras de surveillance*, Note principes loi caméras 2007.2, 20 Junuary 2010, pp. 1-20, p.14.

Among the CCTV sites we investigated was the case of CCTV in a private and large department store. In this case research was conducted with respect to the main department store which can be found in Brussels. As in the previous cases, the first task was to locate the data controller, namely by getting details of the company in charge of processing CCTV images. Although signage appeared in the halls and at the main entrances of the department store, we asked the managers of the store to provide us with the exact details of the data controller. At first they were very reluctant to give me this information. They enquired about the reasons and purposes of my wishing to introduce an access rights request. I replied by saying that I wanted to submit an access request because this is a right granted by national legislation. Although in the end I did not manage to dispel their suspicion completely, they provided me with the details I needed.

I exposed myself to the gaze of the CCTV cameras of the department store and submitted an access request to the data controller soon afterwards. My access rights request was sent in early October 2013. Among other things, it mentioned specific details which would have allowed the data controller to identify me unequivocally. In particular, I specified the date, time and place in which footage about me was captured and additional personal details, such as the way I was dressed in that particular circumstance. I received a phone call from the data controller around one month after my enquiry. The person on the phone presented himself as an assistant security manager. He asked me several questions about my access request, namely why I introduced an access request, if it was linked to a crime, how I got the details of the data controller and if I knew him beforehand. After several preliminary explanations from my side, he said he found himself surprised about my request as they usually deal with requests made by police officers. He explained to me that his company has implemented a specific protocol to deal with access rights requests made by the police. He reported that the CCTV cameras they operate are linked to a hard disk which records images for a limited period of time, until the disk saturation. After that, CCTV footage is destroyed and becomes inaccessible. I asked for more information about the CCTV protocol they implement and whether I could have access to it. He said this was only an internal document, for internal purposes. While making reference to the provisions of this document, he said he had to reject my access request because police officers are the only persons entitled to have direct access to CCTV images. This usually happens on the basis of an order given by a judicial authority. If the police or judicial authorities get access to CCTV images, then these are usually shared with the data subject who thus gets indirect access. He said that in the concerned case sharing CCTV footage directly with me would have implied a breach of the Belgian law and in particular of the Camera Act. In spite of this resistance, he reassured me about the way CCTV images were processed by the company he represented. He underlined that the company had asked and notified the Privacy Commission about the use of CCTV cameras. Accordingly, the name of this company appeared on the register linked to the Camera Act. In addition, he said that access to CCTV images was granted only to the police and a very limited number of people within the company. Hence, in his opinion, I should not have to be concerned about the way the company processed CCTV images. Generally speaking, he referred to the fact that their internal procedures and practices were compliant with the law and thus the company acted lawfully.

Further to this reply, we contacted the Privacy Commission asking whether the answer provided by the company was compliant with Belgian law and in particular with the provisions of the Camera Act. As mentioned earlier, the Privacy Commission found that our request was not motivated according to the legal definition of this term and hence access was denied on a legitimate legal basis.

Open street CCTV in a city centre

In this case, our request was denied by the Belgian Police based on the fact that the footage had already been erased before it could be disclosed to us. The Belgian police said that images taken by CCTV cameras installed on streets are stored for 10 days only. Although access was refused, the police pointed out that they processed our access request carefully as it originated an administrative enquiry. Although data subjects cannot be granted any material access in this circumstance, it is important to note that this argument can be used by data controllers speciously and might dissimulate a denial of the right to access. Indeed, legislation leaves data controllers a certain margin of manoeuvre as regards to when requests should be handled. Once data controllers receive an access request, they might take several days to answer it. Moreover, complying with the formal requirements prescribed under Belgian law, access requests have to be sent by post, which already takes a few days before data controllers receive them.

CCTV in a metro station

We were confronted with the same argument when we contacted the data controller of CCTV systems in the Brussels transport setting. We located the data controller without major problems and the company replied to our access request relatively promptly. Access was denied because images had been destroyed a few days after their recording as no evidence of crime or damage was found or images did not allow identification of criminals. The reply of the company stressed that I could have challenged this decision addressing to the judicial authority.

CCTV in a government building

Some of the data controllers we contacted rejected our access rights request because it was not motivated and no notice of crime emerged from the concerned footage. As explained above, this argument was put forward by the metro station company alongside the fact that the footage had already been deleted. The same reasoning was used by the data controller of CCTV cameras installed in a government building. We carried out research for this site claiming access to images taken by CCTV cameras installed at the entrance of the Belgian Ministry of the Interior. In this case access was denied because the data controller argued that our request was not properly motivated, as required by Art. 10 of the Belgian Camera Act. It is apparent from this example that the lack of a “proper” motivation prevents data subjects from having access to CCTV images and represents one of the main obstacles to the exercise of access rights.

CCTV in a bank

Another argument put forward by data controllers to deny access to CCTV images referred to the identity of the claimant. They refused access to CCTV footage saying that the police and judicial representatives are the only authorities entitled to access this data. Data controllers held this argument on the basis of Article 9 of the Camera Act. This Article establishes that data controllers can transfer CCTV images to the police or judicial authorities in case they observe that criminal activity emerges from a certain CCTV image. Data controllers have the legal obligation to do so when asked by the police in the framework of a police or administrative procedure. It is important to note here that from a legal point of view Article 9 of the Camera Act constitutes the strongest argument for data controllers to deny access to CCTV images. Access was denied on these grounds by the bank when we sought access to CCTV cameras installed at the entrance of one of their bank branches. It appears therefore that data controllers have wrongly inferred that because they have a legal right to disclose CCTV footage to the police, that this is an exclusive right and that it trumps citizens' access rights.

Considerations about CCTV and access rights in Belgium

Disappointing results emerged from the exercise of access rights in Belgium. Among other things, the systematic refusal to grant access to CCTV images shows some of the main inconsistencies of the Belgian Camera Act. We encountered three major obstacles in getting access to CCTV footage, namely: the unavailability of images (due to limited storage period); the lack of a proper motivation to substantiate access requests; and the need to make security prevail over private life interests. As for the first of these obstacles, this research illustrated how storage period limits that are very tight may restrict access and turn it into a vanishing right. The second and third obstacles showed how the right to access can become a void provision, left to the discretion of data controllers. In more general terms, these three obstacles represented also specious arguments on the basis of which access was denied by data controllers.

Although the right to have access to CCTV images is explicitly safeguarded in Art. 12 of the Belgian Camera Act, it is still very unclear if and to what extent data subjects can exercise it. The need to motivate access request was contemplated also in the former versions of the Act and can be traced back to the parliamentary works of 2006. According to the early drafts of Art. 12 (ex Article 13 of the Act), access to CCTV images was granted to data subjects who had a manifest interest in getting such access.[84] However, the data subject did not have direct access to CCTV images but had to submit his request to the Privacy Commission which then asked data controller for the footage. The orientation of the Parliament in this first stage was

[84] Art. 13 of the Act stated that "les personnes filmées ont un droit d'accès aux images à condition de pouvoir témoigner d'un intérêt manifeste". Sénat de Belgique, *Proposition de loi réglant l'installation et l'utilisation de caméras de surveillance,* déposée par MM. Stefaan Noreilde, Philippe Moureaux, Ludwig Vandenhove et Berni Collas, Legislative document N° 3-1734/1, Session de 2005-2006, 31 May 2006.

in line with the Belgian approach on the exercise of access rights.[85] The Privacy Commission proposed amendments to this early version of Art. 12 of the Camera Act claiming that access to CCTV images had to be exercised by the data subject directly, without the mediation of the DPA.[86] Most of all, it suggested the Parliament to delete the provision of the manifest interest as a condition to get access to CCTV images. As the Privacy Commission pointed out, the need to motivate access requests was not contemplated neither by the Belgian Privacy Act, nor by Directive 95/46/EC. Moreover, it could have caused legal uncertainties.[87] Lastly, the Belgian Parliament decided to replace "*intérêt manifeste*" for "*demande motivée*" (Art. 12 of the Camera Act).

Retrospectively, one can reasonably say that the legal uncertainties raised by the Privacy Commission with regards to the former drafts of the Camera Act have not been solved. They emerged clearly in the course of this research. According to the Privacy Commission, motivation has to be provided in order for the data controller to balance data subjects' interests against security interests. Although the balance between these interests may be legitimate, it is hard to comprehend why data controllers should perform this task, instead of a third and impartial authority. This sort of conflict of interests is apparent especially when CCTV images are processed by the police. Thus, as it reads now, Art. 12 of the Belgian Camera Act does not allow for the exercise of access rights and does not take in due account private life interests.

Concluding thoughts

The empirical access rights exercise conducted at this stage of the research allows us to draw several conclusions. From a practical point of view, the right to have access to personal data is almost disregarded by data subjects. This was confirmed by the very surprised reactions of data controllers when we approached them. In turn, this shows a certain negligence or ignorance amongst data subjects in handling and managing their own personal data, the reasons for which cannot be analysed in this report. Regardless of this lack of interest amongst data subjects, data controllers seem to be too unprepared to deal with access requests. They do not provide enough guidance and support to data subject which could allow them to get access to personal data successfully. In particular, this is the case of small and medium companies which sometimes do not implement any specific privacy policies or practices. However, data subjects also have substantial difficulties in getting access to personal data held by big corporations like Google, Microsoft and Facebook. In this case, it is

[85] As mentioned earlier, in Belgium access to personal data can be direct or indirect. See also Kindt, Els J., *Privacy and data protection issues of biometric applications. A comparative legal analysis*, Springer, 2013.

[86] Sénat de Belgique, *Proposition de loi réglant l'installation et l'utilisation de caméras de surveillance, Avis de la Commission de la protection de la Vie Privée*, Legislative document N° 3-1734/3, Session de 2005-2006, 9 August 2006, http://www.senate.be/www/?MIval=/index_senate&MENUID=22140&LANG=fr (last accessed 15 May 2014).

[87] "En ce qui concerne l'exigence d'« *un intérêt manifeste »:* il n'apparaît pas clairement pour quelle raison une personne concernée devrait témoigner « d'un intérêt manifeste ». Cette disposition peut également engendrer une très grande insécurité juridique: que veut dire disposer d'un intérêt manifeste ? Les Développements ne fournissent pas de réponse à ce sujet. Enfin, l'article 10 de la LVP, article sur lequel s'est basé l'article 13 de la proposition de loi, n'exige pas un tel intérêt et celui-ci n'est pas non plus requis par la Directive 95/46/CE. Cette exigence doit dès lors être supprimée". Ibid.

not always easy for data subjects to locate data controllers and to understand what the legal regime is that they should comply with. Moreover, administrative procedures of such kind are not always smooth and clear to the data subject.

Nonetheless, our attempt to have access to CCTV footage in Belgium shows that law enforcement and security claims still represent one of a number of obstacles to the exercise of access rights. However, the argument according to which "access is not granted unless security concerns arise" seems somehow to contradict the very nature and scope of access rights.[88] Apart from questioning the rationale of holding informational rights, the need to provide justifications for the exercise of access rights does not ensure adequate protection to the data subjects' privacy and data protection interests.

[88] A detailed analysis in this regard can be found in the comparative report of the legal and administrative frameworks across Member States.

SIGNIFICANCE OF FINDINGS - BELGIUM

Hereafter we summarise the main findings which emerged while conducting research on access rights in Belgium. This report digests and recalls the main results of this study. It goes without saying that remarks concerning experiences encountered in Belgium can also be appreciated in a broader perspective and may reflect experiences in other European countries.

Although the right of access to personal data is part of the legal framework which applies to data protection in Belgium, getting access to personal data is for the data subject an exercise which is harder than what legal theory would suggest. Similarly, though we succeeded in locating data controllers in almost all sites we investigated, access was not always granted. On the one hand, our experience in exercising access rights revealed a certain discrepancy between theory and practice. On the other, it showed difficulties and best practices in operationalising access rights.

As it is designed under the current legal framework, the right of access to personal data provides data subjects a very limited possibility to get access to personal data. As our research showed, this possibility is quite unrealistic when it comes to access to CCTV and ANPR footage. Access rights are denied on several grounds in Belgium. In this research we have identified a number of reasons for denial of access to personal data. Under the category 'strategies of denial', we have indicated the following problems: difficulty in locating data controllers details; lack of information about access rights; lack of knowledge about legislation; lack of clarity about the content of normative provisions; lack of support and assistance by data controllers; lack of expertise about the handling of access requests; suspicion, scepticism, resistance, irritation and indifference towards access rights requests. Acting as data subjects, we were often denied access to personal data. However, it is important here to note that, while denial was often invoked on legitimate grounds, most of the times it was neither substantiated by any legal provision, nor explicitly foreseen by the law. This was the case in the context of access to CCTV and ANPR images for instance. None of the data controllers we contacted provided us access to such footage. In these cases, access was denied mainly because, according to data controllers, our access requests were not duly motivated, as prescribed by national law. The lack of a sufficient or proper motivation represented for us the major obstacle in getting access to CCTV and ANPR images.

Whatever the reason for denying access rights is, refusal means for the data subject the impossibility of getting control over his personal data. Most of all, in case of denial the data subject finds himself powerless in the face of the data controller as the former is precluded any opportunity for getting access to his data. The submission of a complaint to the DPA still remains an option in this circumstance, as well as the filing of a judicial complaint. In principle, the recourse to the national DPA might represent a feasible solution for the data subject to obtain access to his data. However, this does give him any guarantee to reach this goal as there is no certainty about whether, how and when the DPA will process the concerned access request. Of course, the lack of certainty on these points does not impinge on the role of DPAs, like the Belgian Privacy Commission which are greatly involved in promoting data protection and access rights. Nevertheless, because of legal uncertainties and weaknesses in the role and powers of DPAs, most of the time the exercise of access rights is left to the discretion of data controllers. As highlighted by the Snowden revelations, imbalances in the relationship between the data controller and the data subject constitute a serious matter of concern for democracy.

To sum up, the right to have access to personal data provides a weak legal protection to data subjects mainly for the following reasons:

- Access rights hold a minor role in the framework of data protection, if compared to other rights such as cancellation, rectification; opposition, etc. Moreover, private corporations are more likely to consider access as a service, rather than a right and our research experiences reflected this;
- Member States have a wide margin of discretion in setting exceptions and restrictions to access rights. Although Art. 13 of the European Directive 95/46/EC enlists cases in which access rights can be legitimately denied, these exceptions are often interpreted broadly by Member States. This is partly due to the fact that concepts such as national security or public security are very ambiguous and hence open to several interpretations;
- Data controllers have themselves quite a significant discretion in handling access requests. Among other things, this is confirmed by the considerable timeframe they have for handling access requests in Belgium (which is of 45 days from the notification of the request);
- No sanction is foreseen for data controllers who disregard access requests or do not comply with the law;
- Weaknesses in the role, composition, resource endowment and independence of national DPAs jeopardise access rights (however, in the Belgian case this was not felt to be particularly present);
- In more practical terms, the exercise of access rights is made even more difficult when data are processed by companies like Google, Facebook or Microsoft. In this case it is difficult to locate data controllers and to understand what the legal regime they should comply with is.
- The lack of case law at national (and European) level represents certainly another major problem. Because of this, the protection of access rights is greatly left to legislation and in particular to national legal traditions and sensitivities in protecting personal data.

The empirical study on the exercise of access rights in Belgium resulted in important (and somehow unexpected) findings. It allowed us not only to exercise access rights so putting ourselves in the data subjects' shoes but also to test the Belgian Privacy Act and the Camera Act. To our knowledge this is the first comprehensive analysis on the exercise of access rights in Belgium. Although the results of this study are quite relative and indicative, it makes Belgian data subjects more familiar with access rights and suggests how the right of access to personal data could be improved.

References

Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993 [*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens*/*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel]*.

Belgian Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data, Belgian Official Journal 18 March 1993.

Belgian Parliament, *Loi réglant l'installation et l'utilisation de caméras de surveillance*, 21 March 2007.

Belgian Parliament, *Loi relative à la Centrale des Crédits aux Particuliers,* 10 August 2001.

Boulanger M.-H., De Terwangne C. and Léonard, T., « La protection de la vie privée à l'égard des traitements de données à caractère personnel : la loi du 8 décembre 1992 », Journal des Tribunaux, 5675, 1993.

Commission de la protection de la vie privée, *Rapport Annuel 2012*, 2012, available at http://www.privacycommission.be/sites/privacycommission/files/documents/Rapport-annuel-2012.pdf (last accessed 11 July 2013).

Convention Collective de Travail (CCT) (Collective Labour Agreement) n. 68 of 16 June 1998, concerning the protection of privacy with regard to video monitoring at the workplace. Cour d'Arbitrage, *Monsieur J.V. v Communauté flamande*, arrêt n° 16/2005, 19 January 2005.

Court of Trade of Antwerp, Rechtbank van koophandel te Antwerpen, *Federatie van verzekeringsmakelaars, Fédération des professionnels en assurance de Belgique v N.V. Kredietbank*, 7 July 1994.

European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in OJ L 281/31-39, 23.11.95.

Kindt, Els J., *Privacy and data protection issues of biometric applications. A comparative legal analysis*, Springer, 2013.

Law of 11 December 1998 on the transposition of the European Data Protection Directive, Belgian Official Journal, 3 February 1999.

Léonard, T., "Grondrechten en vrijheden / Libertés et droits fondamentaux, Rechtbank van koophandel te Antwerpen, 7 juli 1994", *Consumentenrecht*, October 1994.

Loi relative à la securité lors des matches de football, 21 December 1998.

Microsoft, Microsoft Privacy Statement can be found at the following link: http://www.microsoft.com/privacystatement/en-us/core/default.aspx (last accessed 10 March 2014).

Microsoft, Other Important Privacy Information, http://www.microsoft.com/privacystatement/en-us/core/default.aspx?Componentid=pspOtherInformationModule&View=Description (last accessed 10 March 2014).

Nouwt Sjaak, de Vries Berend R. and Corien Prins, *Reasonable expectations of privacy?*, ITeR, The Hague, 2005.

Nouwt, Sjaak, de Vries, Berend R. and Prins, Corien (eds.) *Reasonable expectations of privacy*?, Information Technology and Law Series, Asser Press, The Hague, 2005.

Privacy Commission, *Note relative à la loi réglant l'installation et l'utilisation de caméras de surveillance*, Note principes loi caméras 2007.2, 20 Junuary 2010, pp. 1-20.

Sénat de Belgique, *Proposition de loi réglant l'installation et l'utilisation de caméras de surveillance, Avis de la Commission de la protection de la Vie Privée*, Legislative document N° 3-1734/3 Session de 2005-2006, 9 August 2006, http://www.senate.be/www/?MIval=/index_senate&MENUID=22140&LANG=fr (last accessed 15 May 2014).

The Belgian Constitution of 1831 and its modifications, http://www.senate.be/doc/const_fr.html

The Belgian Head of State, *Arrêté royal définissant la manière de signaler l'existence d'une surveillance par camera*, 10 February 2008.

The Privacy Commission, *Recommandation d'initiative concernant la diffusion d'images,* (A/2007/033), 2007.

Tribunal de Première Instance de Bruxelles, Civ. Bruxelles (pres.), 22 March 1994.

List of Abbreviations

ANPR - Automatic Number Plate Recognition

Art. - Article

CCTV - Closed-circuit television

C.F.X.S. - *Financieel studiecentrum Xavier Serwy*

DPA - Data Protection Authority

E-ID - electronic identity card

EU - European Union

ID - identity/identity card

MSN - Microsoft Network

USA - United States of America

VUB - Vrije Universiteit Brussel