Case study: Legal Requirements for the Use of Social Login Features for Online Reputation Updates

Yung Shin VAN DER SYPE
ICRI – KU Leuven
Sint-Michielsstraat 6, bus 3443
3000 Leuven, BELGIUM
+32 495 21 33 31
yungshin.vandersype@law.kuleuven.be

Jean-Marc SEIGNEUR
Université de Genève
7 route de Drize
1227 Carouge, SWITZERLAND
+41 22 379 0238
Jean-Marc.Seigneur@reputaction.com

ABSTRACT
Online users use more and more social login on third-party sites or applications. To use an existing account to login is faster than to fill in personal information forms over and over again. However, many online users, even those who frequently use social login systems, are not aware of the policies and conditions they agree with. They are often unaware of the consequences of their authentications to access websites and applications, and thus of the information that can be retrieved from their social networks.

In this paper, we provide a case-study of the legal requirements that must be observed when social login features are used for authentication in a mobile application in the workplace. The legal requirements considered in this case-study follow from the Belgian implementation of the EU legal framework on privacy and data protection. Particularly interesting for this study is the storage of the data following from external social network profiles; the retention of the retrieved information processed to compute an extra layer of reputation; and the policies accompanying the social login features.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues – *Privacy, Regulation.* K.4.3 [**Computers and Society**]: Social Issues – *Employment.* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Authentication.*

General Terms
Security, Human Factors, Legal Aspects.

Keywords
Social Login, Online Reputation, Workplace Privacy, Legal Aspects.

SAC'14, March 24-28, 2014, Gyeongju, Korea.

http://dx.doi.org/10.1145/2554850.2554857

1. INTRODUCTION
More and more sites and applications allow their users to create an account and authenticate for further logins via a third-party social network such as LinkedIn, Google, Facebook or Twitter. Users tend to prefer such social login because they do not have to fill in again their personal information every time they request access. Once they are logged in to a social network, they can easily use this login to access the other site or application. Thus this way of registration is faster for the user, and also more convenient because they do not need to remember other passwords than the one they use for their social network.

However, users often do not take the time to carefully read the policy explanations before they authorize websites and applications to use their social networks for login. As a result they may not be aware of which information the websites and applications can retrieve from their social networks.

In this paper, we provide a case-study of the legal requirements that must be observed when social login features are used for user authentication to access a mobile application, which retrieves information from social networks to compute an extra layer of reputation on top of that retrieved information, and which is owned or controlled by the user's employer or contracting party. The considered legal requirements are based on the EU legal framework on privacy and data protection, as implemented in Belgian law. In Section 2 we discuss related work in the fields of social login and reputation computation. In Section 3 we present the studied mobile application. Section 4 lists our findings regarding the legal requirements for social login and further reputation computation according to Belgian law. And finally, in Section 5 we conclude and discuss future work.

2. RELATED WORK
In this section, we start by related work regarding the technical aspects of social login and reputation computation and then delve into related work regarding legal requirements.

2.1 Social Login
For the past 10 years, many technical initiatives have been launched in order to achieve single-sign-on (SSO) and federated identity management between different services, applications and Web sites owned by different legal entities. A few of these technical initiatives were strongly backed up by major information technology companies such as Windows Cardspace, Liberty Alliance or IBM Higgins [1]. Surprisingly, it is not them that achieved large scale user adoption but a combination of the

creation of open authentication and authorization protocols and their use by large scale online social networks such as Facebook. Users had already massively joined these online social networks and filled their information including with whom they are friends or connected. To avoid having to spend time re-authenticating, filling their information, and to remember new passwords, they then adopted massively the Facebook Connect social login option that many services, Web sites and application started to easily implement thanks to an Application Programming Interface (API) provided by Facebook. Given the success of Facebook Connect, other major online social networks started to provide their social login option and API such as Twitter or LinkedIn. Although most of them have built their social login according to the OAuth [2] open standard for authentication and authorization, the original open standard for authentication, which OAuth took a number of ideas from, is OpenID [3]. Unfortunately, although most of them have used a common standard basis and provide an API, their APIs are constantly evolving, often without backward compatibility with the previous version of their API, and are very different between the social networks. Thus, it has become difficult for a third-party service to cover all the potential social networks that a new potential user may want to use to create their account. This is why a new type of providers has emerged on top of these "social login" providers. Those providers do the hard work to maintain a tool that allows a user to create an account with all the "social login" providers as well as store and manage users information on behalf of the service or Web site that uses this tool. Thus, user management has started to be used for such services to clearly underline they go beyond previous identity management solutions that focused on the authentication and identity certification issues. The owners of Web sites and services install the user management tool on their Web site or service in order not to have to worry about maintaining code when one of the "social login" providers change their API. The price of allowing a user to create an account with any of the main online social networks providers without having to maintain each "social login" module has to be weighed against the subscription price to one of these user management providers such as Janrain [4] or Gigya [5]. As the number of intermediaries managing users information increase, some privacy concerns arise, especially when the users do not take the time or are not enough technology aware to check the information they allow to be shared between the intermediaries. It is the reason we tackle the legal aspects further in this paper.

2.2 Reputation Computation

The mobile application of our case-study, detailed in Section 3, uses the information extracted from the social login of the users in order to compute their reputation regarding different skills such as computer security technology awareness. A computational model of trust based on social research was first proposed by Marsh [6]. The EU-funded SECURE project [7] created a computational trust engine that uses evidence to compute trust values in entities and corresponds to evidence-based trust management systems. Evidence encompasses outcome observations, recommendations and reputation. A trust metric consists of the different computations and communications which are carried out by the trustor (and his/her network) to compute a trust value in the trustee. When recommendations are used, a social network can be reconstructed. Golbeck and Hendler [8] studied the problem of propagating trust value in social networks, by proposing an extension of the Friend-Of-A-Friend (FOAF) vocabulary and algorithms to propagate trust values estimated by users rather than computed based on a clear count of pieces of evidence. Reputation has been defined as follows : *"Reputation is the subjective aggregated value, as perceived by the requester, of the assessments by other people, who are not exactly identified, of some quality, character, characteristic or ability of a specific entity without taking into account direct previous interactions with the entity"* (adapted from [9]). However, to be able to perceive the reputation of an entity is only one aspect of reputation management. The other aspects of reputation management for an entity consist of:

- Monitoring the entity reputation as broadly as possible in a proactive way;
- Analysing the sources spreading the entity reputation;
- Influencing the number and content of these sources to spread an improved reputation.

Founded in 1995, eBay is the first large-scale online reputation service that allows the users to check the reputation of other buyers/sellers users or selling companies based on the number of positive and negative ratings that are aggregated in their Feedback Score as well as potential written text comments. Founded in 2004, Opinity [9] was one of the first commercial effort to build decentralized online reputation for users in all contexts beyond eBay's limited e-commerce context. Unfortunately, Opinity closed as several other services that tried to become the leader in online reputation calculation because very few users are willing to pay for such service. However, a few new services try to compute the influence of users in such or such topic, which is related to the reputation of these users regarding a topic. For example, Klout [10] was created in 2008. Once the Klout account is linked to a user's social network via social login, it can detect automatically when the user sends a new post and check how much buzz it has generated. Thus instead of computing the reputation of a person mainly based on recommendations from other users, Klout analyses the social networks of the user, e.g., Twitter based on the following 3 main criterions:

- True Reach: the number of followers of the user's Twitter account and following the user's tweets
- Amplification: the number of people who share a post (who distribute it to other users)
- Network: the influence of the users composing the True Reach themselves

Klout may integrate other evidence such as posts on other social networks (such as Facebook) or other users who recommend the user by adding a +K to the user on specific topics, meaning that they click on a link provided by Klout saying that the user has influenced them regarding that topic. Unfortunately most of those influence/reputation metrics are not open, i.e., it is not really clear how the results have been computed and based on which evidence.

2.3 Legal Requirements

Social login features allow sites and applications to process large amounts of personal data. The use of those features thus has a legal impact on the privacy and data protection rights of the users.

In the mobile application in our studied case, as is described in Section 3.1, the user might be a contractor or an employee to the company. For both types of users, the information retrieved from social networks is discussed according to the legal requirements resulting from the European Union Data Protection Directive. With regard to the general application of European data protection law and its implementation in the Belgian national law, De Bot [11], Kuner [12] and many others defined, analyzed and categorized the rights and principles of data protection extensively. More specifically with regard to the retrieval of personal data from social network profiles Valcke *et al.* [13] recently published an interesting book. In this book Graux [14] observes some challenges about the use of applications to retrieve user information. Though, his observations are more focused on user-protection in marketing and advertising matters. Our studied mobile application differs from this situation since it envisages to enhance company security, rather than profit making. Regarding workplace privacy, Hendrickx examined the use of social media in a Belgian employment context [15]. However, to the best of our knowledge, there is no academic legal research undertaken on the specific subject of this paper.

3. DESCRIPTION OF THE STUDIED MOBILE APPLICATION

In this section we first describe the mobile application that we used for our case-study. Then we detail the social login and reputation computation aspects of this application.

3.1 MUSES Mobile Application

Corporate users increasingly use computing environments in many other places than the corporate offices, accessing corporate information from homes, airports, conferences, etc. They often also use their own devices as part of the Bring Your Own Device (BYOD) trend. In addition, there are more and more projects where different companies and contractors have to collaboratively work together. Thus, the trustworthiness in both employees and external collaborators, who have no direct employment contract with the company of the Chief Security Officer (CSO), has to be taken into account in a more dynamic way. The computing environments are not fully controlled by the CSOs and new metrics to dynamically assess the trustworthiness of computing environments are needed.

The mobile application used for our case-study is the mobile client of an EU-funded FP7 project called MUSES [16]. The overall purpose of MUSES is to foster corporate security by reducing the risks introduced by user behavior, especially when they want to access corporate data when they are outside of the company and/or with their personal device in a BYOD way. Once the MUSES mobile application is installed on the user device, a computational trust engine that is running in the mobile application, monitors what the user is doing, as well as its security state. Based on the analysis of this context information, MUSES enforces appropriate security policies.

One of MUSES' strengths is its user and device neutrality. This means that the system will be useable by everybody who is dealing with company data assets, regardless whether he is an independent contractor or employed by the company, and regardless the ownership of the device being used to request company information. In MUSES, the following cases occur:

1. An employee uses a company-owned mobile device;
2. A contractor uses a company-owned mobile device;
3. An employee uses a personal mobile device;
4. A contractor uses a personal mobile device.

3.2 Social Login

The first time the user installs the MUSES mobile application on a new mobile device, as depicted in Figure 1, the user must agree with the installation policy, which must take into account the legal requirements of the country where it is installed, for example, in Belgium the ones we present in Section 4.

Figure 1. MUSES installation and social login user interfaces

After installing our MUSES mobile application, as depicted in Figure 1, the user has the choice to create an account and log in either with a MUSES login/password or social login through a number of social networks.

3.3 Reputation Computation

When a user requests to access sensitive company data assets, the MUSES application will check the trustworthiness of the user. One way by which the application foresees to update the user's online reputation is through the use of social login features.

If the user chooses to login via a social network, the MUSES mobile application, depending on the social network, may also be able to retrieve other information about the user and use it to compute the reputation of the user in MUSES context. For example, as depicted in Figure 2, if the user chooses to log in via LinkedIn, the user's skills endorsed in LinkedIn and education degrees and diploma are used to compute a reputation score from 1 to 10 regarding security technology awareness. A user with a Master in Computer Science will get a higher score than a user without education related to computer science. The details of the reputation computation are beyond the scope of the paper that focuses in the following section on what kind of further computation can be done from a legal point of views, after which user consents, how long, and depending on the user type, employee or contractor.

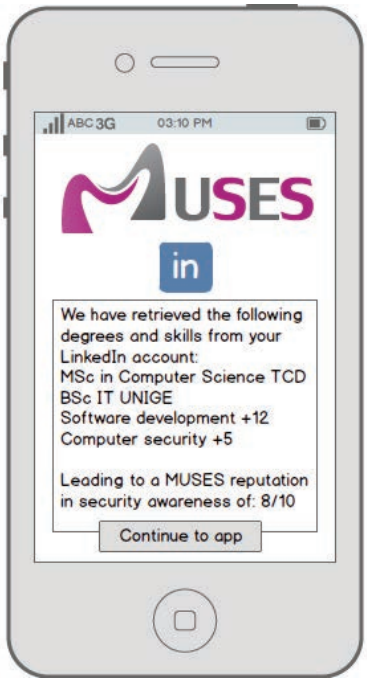

Figure 2. MUSES reputation computation user interface

4. THE USE OF SOCIAL LOGIN FEATURES IN THE WORKPLACE ACCORDING TO BELGIAN LAW

By using social login features, applications gain access to user information stored on the user's social networks. What happens here is that the application will scan a user's profile in order to compute his current level of trustworthiness, and accordingly grant or deny him access to the requested company information. The use of such social login features thus provokes a discussion on privacy and data protection rights. Since the studied application is a company-controlled application, this discussion should be held accordingly taking into account the particularities of workplace environments.

In what follows, the legal requirements for the use of social login features are examined when using personal data of workers. The first subsection provides an overview of the applicable law. The second subsection summarizes the general European principles of privacy and data protection in the workplace in the context of our MUSES application. Where relevant, these general principles are further specified according to Belgian law. The choice for a Belgian approach follows from the interesting specifications with regard to employee data protection foreseen by the Belgian legislators.

4.1 Applicable Law

The processing of personal data is regulated in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [17]. The Data Protection Directive protects data subjects whose personal data are processed. According to Article 2, a) of the Directive, **personal data** is "*any information relating to an identified or identifiable natural person ('data subject')*". The information retrieved from the user's social network by the here studied application is thus considered as personal data. The concept of **processing** is defined as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*" (Art. 2, b Data Protection Directive). This is a widely formulated definition including basically all operations one could possibly perform upon personal data. To gain access to someone's social network in order to analyze the there-found information, is thus considered as processing of personal data. Since the Data Protection Directive has a very general character, also employees are protected by this Directive.

As it is necessary for directives to get enforced, the Data Protection Directive was implemented in the national Belgian law[1]. With regard to the general aspects of data protection, the Belgian law by the Law of 8 December 1992 on the privacy protection in relation to the processing of personal data was modified [18]. In particular with regard to the protection of employees in their employment context, the general (European) data protection principles are specified in the Belgian Collective Bargaining Agreement No. 81 (CBA No. 81) of 26 April 2002 on the privacy protection of employees regarding the surveillance of their electronic online communication [19]. The applicability of this *lex specialis* is limited to the processing of personal data which concerns employees. The processing of personal data of contractors, not employed by the company, falls outside the scope of CBA No. 81. Such processing operations must be reviewed in the light of the general data protection rules (Belgian Privacy Law).

4.2 Workplace Data Protection Principles and Case-Study Law-derived Requirements

The Data Protection Directive provides data subjects with legal guarantees in case their personal data are processed[2]. As a general rule, the Directive only allows data processing when the data are "*processed fairly and lawfully*" (Art. 6, 1, a) DP Directive). In the next paragraphs more requirements are discussed.

4.2.1 Controller and Processor of Personal Data

Before any processing activity is carried out, it should be clear who is charged with the **role of the controller**. The controller is the natural or legal person who is responsible for the processing of the personal data (Art. 2, d) DP Directive; Art. 1, §4 Law). He defines the means and purposes of the data processing activity and he shall notify the national data protection authority before the data are processed (Art. 18, 1) DP Directive; Art. 17, §1 Law). In the mobile application in our studied case, it is most likely the

[1] The Belgian Law was already adopted in 1992, but when the Directive was adopted, it was implemented in the existing Law. They chose not to adopt a new Law, but alter the existing one to be compatible with the Directive.

[2] On 25 January 2012 the European Commission proposed a comprehensive reform of the data protection legislation in the European Union. Due to the limited extent of this paper and the many uncertainties on the substance of the proposed changes, especially with regard to the employment context, the proposed changes are left out of the discussion in this paper.

company to whose networks the user aims to gain access to, who acts as controller since he provides the MUSES mobile application configured for its company information system and network. However, it is possible that the company delegates the actual act of the processing of the personal data to another entity (**the processor**), who will in that case process the data on behalf of the controller (Art. 2, e) DP Directive; Art. 1, §5 Law).

4.2.2 Legal Grounds for the Processing of Personal Data

The controller must ensure that at least one of the criteria for making the processing legitimate is met (Art. 7 DP Directive; Art. 5 Law). These criteria are called **legal grounds** and include situations where the data subject has given his unambiguous consent; the processing is necessary for compliance with an obligation to which the controller is subject; the processing is necessary in order to protect the vital interests of the data subject; the processing is necessary for the performance of a task carried out in the public interest; or when the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed. It might thus happen that personal data are processed without the data subject's consent, though the interpretation of the provision is very restrictive. It is required that a national law specifically foresees in an obligation to process the personal data, e.g. for social security or tax purposes. With regard to the processing of special categories of data, such as sensitive data, the legal grounds are even more restrictive (Art. 8 DP Directive; Art. 6-7 Law). As **sensitive data** should be considered: "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life*" (Art. 8, 1) DP Directive). Although not the only legal ground for processing, the consent of the data subject remains the most likely ground for processing [20].

Currently consent is the most common legal ground. To make this consent legitimate, privacy policies, accessible at the time of installation of the mobile application, are of cardinal importance. When the user agrees with the privacy policy, he gives his consent for the processing of the personal data. In the studied case this action is materialized by a ticking-box. Although this is a very easy accessible way of asking consent, the value of online consent through ticking-boxes has been challenged [21]. Crucial is that the individual must fully understand that by the action of ticking the box, he is giving his consent. Therefore, it is recommended to not pre-tick the consent box. The Data Protection Directive requires that the consent of the data subject has to be given freely, informed and for a specific purpose (Art. 2, h) DP Directive). 'Freely' means that the consent must be given without external influence and with the possibility to withdraw. 'Informed' means that the data subject must be aware of the means and purposes of the processing before he grants his consent. 'Specific' means that the consent can only be given for a specific operation, any new processing operation requires a new consent [11]. The purpose (to check trustworthiness and reputation of the user), and the extent of the data processed (which data), must be included in the policy. Besides the users should also be informed that their personal data will be used to compute further reputation and about all their rights and the procedures guaranteeing this rights. Specifically, the users must be informed about which personal data will be processed, how long they will be stored and who will have access to it. At least it must be clear from the policy who the controller is of the personal data, and if any, who the processor is, the procedures for the rights of the data subject. The importance of the notion of consent becomes is also visual in Article 7 of the proposed Data Protection Regulation, that is entirely dedicated to the notion of consent.

Another interesting difficulty with regard to the data subject's consent as a legal ground for the processing of personal data follows from the fact that users can only agree with the processing of their own personal data, and cannot agree with the use of their friends' personal data [14]. In our mobile application case where recommendations are made by friends or contacts, it means that the personally identifiable information about the friends or contacts of the retrieved recommendations cannot be processed if the friends or contacts have not given their consent. The recommendations can be used for reputation computation but without storing personally identifiable information of friends or contacts if they have not given their consent.

With regard to the use of the personal data of employees, some additional considerations should be made. The MUSES mobile application, which allows users to access company sensitive data, would be frequently used by employees. These employees may use their personally owned or corporate mobile devices to access the corporate networks. However, the subordinate relationship which characterizes the relationship with their employers, draw a particular attention to their situation. In the legal analysis of the social login feature, and on the assumption that the application and the system is legitimate, the ownership of the device is not determinant. In case the employee uses a device owned by the company, the application is most likely standard on the device. Still, there should be a legal ground for the processing. As discussed here above, the most likely legal ground is consent. In both cases, personally and company owned, the user should give his free consent. The Article 29 Working Party "*takes the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent*" [22]. Reliance on consent should therefore be "*confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment*" [22]. This is the case when workers are offered reasonable alternatives and when they are not subjected to any direct or indirect pressure to use the social login for the MUSES application. In the studied case the social login is not the only way to gain access to the MUSES application. As an alternative the user could complete a traditional form to gain access to the application. It should be pointed out that consent is not the only legal ground, and that the processing can be found on other legal grounds. In Belgium a legal ground for the processing of personal data retrieved from social network profiles of employees can be found in Article 5, §1, 3° CBA No. 81, allowing the processing of personal data of employees for purposes of security and the functioning of the IT-networks of the company. In this case all formal procedures set out in the CBA are to be respected. However, the CBA is formulated in a very general and very abstract way.

The Proposed Regulation significantly restricts the use of consent for legitimizing data processing. For MUSES particularly

interesting is the introduction of Article 7 (4) of the Proposed Regulation. Under this provision, the use of consent is not allowed as a legal basis for the processing, "*where there is a significant imbalance between the position of the data subject and the controller*". Recital 34 clarifies that such an imbalance includes especially the case where the data subject is in a situation of dependence from the controller. As situation of dependence should be considered, amongst others, the situation where personal data are processed by the employer of employees' personal data in the employment context.

The use of consent as a legal basis for the processing of employee data will thus be even more difficult. Though, the Data Protection Regulation Proposal also brings solutions. Also under the current Directive it is difficult to find a clear legal basis for the processing of employee data for network and IT security purposes. To tackle this difficulty, Recital 39, explicitly clarifies that "*the processing of data to the extent strictly necessary for the purposes of ensuring network and information security [...] constitutes a legitimate interest of the concerned data controller*".

4.2.3 Data Protection Principles

Moreover the controller must ensure that the processing operations comply with all **data protection principles** (Art. 6 DP Directive; Art. 4 Law). The first principle is concerned with **purpose limitation**. Article 6, 1, b of the Data Protection Directive states that personal data may only be collected for "*specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*". It is required to precisely define the reason why the personal data is processed.

In line with the first principle the principle of **data minimization and data accuracy** states that personal data might only be processed when this is necessary to achieve the described purposes. To this end Article 6, 1, c-d requires that the data are "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*" (data minimization), and that the data are "*accurate and, where necessary, kept up to date*" (data accuracy). This means that the controller can only process personal data when this is necessary to achieve the goals of the processing. Thus, once the goals of the processing are clear, the controller must precise which information (such as the name of the user) is necessary to achieve thesegoals. With regard to the discussed case, it should be considered whether all social network profiles are relevant for the application (data relevance). Moreover it should be considered whether some profiles should be excluded from the list of profiles potentially used for the reputation update. Questions that should be asked are: is the information necessary and is there no less-intrusive way? It is possible that Facebook profiles are presumed to be part of the private life more than of the professional life. A potential social network profile to check online reputation for professional purposes is LinkedIn, since a professional character is deemed to be inherent to the social network.

The third data protection principle concerns the **data retention.** This principle limits the controllers in the storage of the processed personal data. It states that personal data can only be kept in a "*form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*" (Art. 6, 1, e DP Directive). Again it has to be clear for which purposes the data will be used and how long they will be stored according to that purpose. Storing data for a longer period than necessary is only possible in anonymized form. For the reasons of prevention, investigation, detection and prosecution of criminal offences, the recent Belgian implementation of Directive 2006/24/EC[3], introduced a new obligation for network operators. From now on, location and traffic data of users should be kept for a period of twelve months, though this period will be further specified by a Royal Decree. The CBA does not provide for specific retention periods and only discusses the principles. In our mobile application case study applied in Belgium, there is no requirement to store location and traffic data for the reasons of prevention, investigation, detection and prosecution of criminal offences.

Although no sensitive data (Art. 8 DP Directive; Art. 6-7 Law) is required by our studied mobile application, the processing thereof is likely to depend on the API agreements with the social networks mentioned. These API agreements must be analyzed and transparently described to the users. Retrieved data must be encrypted when possible. The data must be stored in the EU and not transferred to third countries. With regard to non-anonymized data, a distinction is made between the unprocessed retrieved personal data from the social networks, on the one hand, and the personal data relating to the results of the computed online reputation, on the other hand. In the studied case of social login one could argue that the retrieved personal data might only be kept until access to the application (and consequently the company network) is granted, since the purpose of the processing of the social network data is limited to the social reputation update, and *maximum maximorum* to the access of the company network, which is the ultimate goal of the social login. However, this does not necessarily exclude the possibility to keep the data for a longer period of time, even in a non-anonymized form. The controller may keep the data when the storage of these data is based on another legal ground serving another purpose, which might follow from the purpose of the processing of personal data by the application or even the MUSES system in general (not likely for this type of data). With regard to the 'by-the-MUSES-system-processed' retrieved data, it can be argued that they could be stored for a longer time period. If the purpose of the processing is the update of the online reputation and this information stays relevant for the application until the next update, say the next login, storage could be necessary for this time period. Even when this, between two logins, is a very long time, it could be argued that such a storage of data is necessary for the purposes of the processing. Nevertheless, if the user does not want the system to keep the data for a longer period, and the data are no longer adequate or accurate, he could ask for the erasure of the personal

[3] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communications networks and amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF; implemented by the Belgian Law of 30 July 2013 concerning the modification of Articles 2, 126 and 145 of the Law of 13 June 2005 on the Electronic Communication, and Article 90*decies* of the Criminal Procedure Code, *Belgisch Staatsblad* 23 August 2013, http://www.t-regs.com/wp-content/uploads/2013/08/Moniteur-belge-23-aug-2013.pdf.

data (Art. 12, b) DP Directive). According to the new Belgian Electronic Communications Law, as modified by the Law of 30 July 2013, it is required that traffic and location data are kept for 12 months for purposes of criminal investigations (Art. 126, §3, 2 Electronic Communications Law). Other data should still be kept for no longer period than necessary according to the Privacy Law and the CBA.

Finally, all processing operations on personal data must be done "***fairly and lawfully***". Even when the legal ground for processing is defined, and all other data protection principles are respected, Article 6, 1, a of the Data Protection Directive foresees in a kind of ultimate catch-all protection mechanism that requires that personal data "*must be processed in a way that does not bring about a breach of either data protection law or other legal requirements*" [22], and moreover that the data are processed fairly, with respect to all interests at stake. Interesting here is the discussion on the reasonable expectations of workers and the proportionality principle.

4.2.4 Rights of the Data Subject

In addition, the controller should also be aware of (and respect) the **rights of the data subject**.

A first right that is foreseen by the Directive and the Law is the **right of information** (Art. 10-11 DP Directive; Art. 9 Law). This right shows that privacy policies are not exclusively relevant to acquire an informed consent, but also in order to comply with the principle of transparency and information. There must be clarity and transparency about the data that will be retrieved, and about the consequences of the data received by third parties. In most cases this is (pre-)determined by the API agreements with the concerned social networks. Yet, it is the role of the MUSES service provider to communicate the specifics of the context to its users.

The second right data subject right is the **right of access**, which also covers the right to rectification, erasure and/or blocking of data which processing does not comply with the Directive (Art. 12 DP Directive; Art. 10 Law). The third right of the data subject is the **right to object** to the processing of data relating to him/her (Art. 14 DP Directive; Art. 12 Law). Though this third right specifically aims to protect the data subjects against the re-use of their personal data for direct marketing purposes, which is not the case here discussed.

Moreover, data subjects have the **right to judicial remedy** in case of breach (Art. 22 DP Directive; Art. 14-15 Law).

And finally, Article 15 of the Directive grants the data subjects with a **right of protection against automated individual decisions** (Art. 12*bis* Law). An automated individual decision is a decision that significantly affects a person and which is based solely on automated processing of personal data in order to evaluate him as a person. Since such an evaluation may relate to different personal aspects, such as performance at work, creditworthiness, reliability, conduct, etc., the decisions made by the MUSES system should be considered as automated individual decisions. Automated individual decisions are in principle prohibited, although, this prohibition does not apply when the decision is taken in the context of an agreement, which also lays down measures to safeguard the data subject's legitimate interests (such as objection to wrongful decisions). Yet again, the information and transparency towards the data subject are an essential condition for legitimate processing of personal data.

4.2.5 Security Obligations

Another data protection safeguard laid down in the Directive relates to the security of the processing and the personal data processed (**security principle**). The controller must implement "*appropriate technical and organizational measures to protect personal data against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access*" (Article 17, 1 DP Directive; Art. 16 Law). In practice this means that 'state of the art' measures are implemented depending on the character of the processed personal data. For example, encryption of personal data might help to prevent data breaches in case unauthorized parties gain access to databases and the there stored data.

4.2.6 Transfer of Personal Data

Personal data may only be transferred to third countries under certain conditions. Pursuant to Article 25 of the Data Protection Directive, personal data may be transferred only to third countries which guarantee an adequate level of data protection (Art. 25, 1) DP Directive; Art. 21 Law). In assessing the level of adequacy particular consideration shall be given to "*the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country*" (Art. 25, 2) DP Directive) [23]. If the recipient country is not considered to ensure an adequate level of protection, the transfer may be still possible and allowed according to Article 26 of the Data Protection Directive. This could be the case when the data controller offers the adequate safeguards themselves through e.g. appropriate contractual clauses; or under the derogations provided by the first paragraph of Article 26, e.g. unambiguous consent of the data subject [24].

5. CONCLUSION

This paper studied the requirements for the use of social login features used by companies to verify the trustworthiness of workers trying to access their company networks.

In Belgium, the personal data being processed by the discussed mobile application are protected by the Belgium Privacy Law, which implemented the general EU Data Protection Directive 95/46/EC. For the protection of the personal data of Belgian employees, the Belgian Collective Bargaining Agreement No. 81 is applicable. Contractors are excluded from the scope of this CBA No. 81. The protection of their personal data falls under the general protection of the Belgian Privacy Law.

Informed consent could be the most relevant legal basis to make a processing legitimate. Before the users may give their consent, they should be informed on the specific purpose for which their personal data are processed, which data will be processed (and why these data), who will have access to the data, and how long the data will be stored. Regarding the processed data, it was considered that in the professional context of MUSES, LinkedIn is a more appropriate social network to retrieve user information from than Facebook because of the inherent professional purpose of LinkedIn user profiles. With regard to the retention of the data,

a distinction is made between the information retrieved from the social network profiles as such, and the personal data resulting from the reputation computation by MUSES. The storage of the reputation data is necessary for the purposes of the processing because this information stays relevant for the application until the next update, say the next login, even in a long time. Nevertheless, the user could ask for the erasure of the personal data.

6. ACKNOWLEDGMENTS

The research leading to these results has received funding from the EU ICT Seventh Framework Programme (FP7) under grant agreement number 318508, project MUSES (Multiplatform Usable Endpoint Security) [16].

7. REFERENCES

[1] T. El Maliki and J.-M. Seigneur, "A Survey of User-centric Identity Management Technologies," in *The International Conference on Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007*, 2007, pp. 12–17.

[2] "OAuth." [Online]. Available: http://oauth.net/. [Accessed: 03-Aug-2013].

[3] "OpenID." [Online]. Available: http://openid.net/.

[4] "janrain." [Online]. Available: http://janrain.com/. [Accessed: 04-Aug-2013].

[5] "Gigya." [Online]. Available: http://www.gigya.com/. [Accessed: 04-Aug-2013].

[6] S. Marsh, "Formalising Trust as a Computational Concept," Department of Mathematics and Computer Science, University of Stirling, RP 1994.

[7] V. Cahill, E. Gray, J.-M. Seigneur, C. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. di M. Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen, "Using Trust for Secure Collaboration in Uncertain Environments," *IEEE Pervasive Computing*, vol. July-September, 2003.

[8] J. Golbeck and J. Hendler, "Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-based Social Networks," in *the 14th International Conference on Knowledge Engineering and Knowledge Management*, 2004.

[9] J.-M. Seigneur, "Online e-Reputation Management Services," in *Computer and Information Security Handbook*, 2nd edition, Morgan Kaufmann, 2013.

[10] "Klout." [Online]. Available: http://klout.com. [Accessed: 04-Aug-2013].

[11] D. De Bot, *Verwerking van persoonsgegevens*. Kluwer, 2001.

[12] C. Kuner, *European data protection law: corporate compliance and regulation*. Oxford University Press, 2007.

[13] P. Valcke, P. Jan Valgaeren, and E. Lievens, "Sociale media. Actuele juridische aspecten," presented at the Intersentia, Antwerpen, 2013.

[14] H. Graux, "Privacybescherming op sociale netwerken: heeft u nog een privéleven?," in *Sociale media. Actuele juridische aspecten*, Antwerpen, 2013.

[15] F. Hendrickx, "Sociale media en privacy in het arbeidsrecht," *Status Publ.*, 2013.

[16] "Multiplatform Usable Endpoint Security." [Online]. Available: http://www.musesproject.eu. [Accessed: 14-Jul-2013].

[17] European Commission, "Directive 95/46/EC, further referred to as DP Directive or Data Protection Directive, OC L 281/31, 23.11.95." [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:pdf.

[18] Belgian Government, "Belgian Law of 8 December 1992 on the privacy protection in the relation to the processing of personal data, B.S. 18 March 1993," 1993. [Online]. Available: https://www.law.kuleuven.be/icri/publications/499Consolidated_Belgian_Privacylaw_v200310.pdf. [Accessed: 02-Sep-2013].

[19] Belgian Government, "Belgian Collective Bargaining Agreement No. 81 of 26 April 2002 on the privacy protection of employees regarding the surveillance of their electronic online communication," 2002. [Online]. Available: http://www.internet-observatory.be/internet_observatory/pdf/legislation/collective_agreement_privacy_nl.pdf. [Accessed: 02-Sep-2013].

[20] European Commission, "Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187," 2011. [Online]. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[21] European Commission, "Recital 17 e-Privacy Directive; Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187, 26," 2011. [Online]. Available: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf. [Accessed: 02-Sep-2013].

[22] European Commission, "Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context," 2001. [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf. [Accessed: 02-Sep-2013].

[23] European Commission, "List of by the Commission recognized adequate Countries." [Online]. Available: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm. [Accessed: 02-Sep-2013].

[24] European Commission, "Frequently asked Questions relating to Transfer of Personal Data from the EU/EEA to Third Countries." [Online]. Available: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf. [Accessed: 02-Sep-2013].