I Have a Facebook Account, therefore I Am
- Authentication with Social Networks

Wordcount: 5319

Jessica Schroers

Sint-Michielsstraat 6 box 3443, 3000 Leuven – BELGIUM

[t] +32 16 37 35 91

[e] Jessica.schroers@kuleuven.be

ORCID iD: 0000-0002-3741-8123

Affiliation: Centre for IT and IP Law – KU Leuven - imec

I Have a Facebook Account, therefore I Am

- Authentication with Social Networks

Social login is the use of a social network account to get access to other services. Since the internet in its architecture does not have the possibility to identify the internet user, for many services, social logins are the solution to authenticate users without the need to set up individual identity management systems. Social logins are not useful for all types of services however, and the potential lock-in and lock-out of users needs to be considered.

Keywords: social login; identity management; personal data

Introduction

When internet users want to log in at a website, use free wifi or an app, they are often requested to log in with their Facebook, Google+, Twitter, LinkedIn or other social network account credentials. While in some cases it is still possible to sign up without a social network account, other services are not accessible without one. The rise of ‘social logins’ or ‘soft eIDs’, and their possible implications, did not yet receive a lot of scholarly attention. This paper focuses on the issue of lock-in and lock-out of users due to the use of social login, considering whether the right to data portability might be suitable to address the lock-in effect of social login. In order to see how broad social logins might be used, it is furthermore analyzed whether social logins could legally be used for access to public services.

To frame the wider discussion, the first part of this article gives a short background of online identity management. Afterwards, it analyzes Facebook Connect as an example of social login and considers the use of private identity provider for e-government access. Finally, the potential lock-in and lock-out effect of social logins, with a focus on Facebook Connect, are analyzed.

The missing identity layer in the internet

The internet does not have a built-in function or layer to identify the person browsing the internet. IP addresses identify a computer and, via connected information available from the Internet Service Providers, the person to whom the internet connection belongs. The latter however, does not necessarily have to be the person behind the keyboard. On the one hand this anonymity is one of the central advantages of the internet. On the other hand, considering the increasing use of the internet for everyday use, such as e-commerce and e-government, it is considered problematic that the internet lacks the means to authenticate the internet user, i.e. the person behind the keyboard (e.g. Cameron 2005).

Therefore, identity management systems are used to establish identity on the internet. Service providers can employ their own identity system: they identify the user themselves (usually asking the user to fill in a form with personal information) and provide ‘authentication means’ specific for their service (usually username and password). This is called ‘siloes’ identity management. Given the expansion of e-commerce, the silo solution was considered not to be the best approach as it requires investments from the service provider and the user was burdened with an ever increasing amount of passwords (Smedinghoff 2012).

Hence, other solutions were developed. The identity management landscape is varied¹, however, the ‘electronic identity’ is often provided by a third party. This trusted

¹ Various different identity management systems exist, for different applications (e.g. e-government, e-commerce, games and social media services, company specific internal access systems, etc.). The technology and initiatives are constantly evolving (see for example for an overview of the evolution of standards and technologies for user identity management from 1999 till 2013. (Jøsang 2014)).

third party, an ‘identity provider’², first identifies a person, which means the user will be assigned an electronic identity. Later the identity provider authenticates the electronic identity to relying parties (i.e. service provider) when the user tries to log in at the relying parties service with the electronic identification means given by the identity provider. In the literature it has been pointed out that the identity provider becomes a single point of failure and at the same time an ‘all-knowing’ entity, which knows all user transactions (and can link them across different domains) (e.g. Alpár, Hoepman, Siljee 2011; Hansen et al 2004; Jøsang, Al Zomai, Suriadi 2007). The identity provider can be the government providing an electronic identity card or another eID solution, e.g. the German nPA, Belgian eID or Austrian Bürgerkarte, to its citizens (thereby fulfilling essentially the same role as when it provides identity cards). However, private service providers can also act as identity providers, either as specialized identity providers, or as service providers who provide the authentication function as an additional function on top of their normal business (e.g. Facebook Connect).

Zarsky and de Andrade make a difference between ‘hard’ eIDs and ‘soft’ eIDs. Hard eIDs are initiatives which strive to duplicate the offline world’s level of security and authenticity in the online realm and are mainly used for e-government and banking (Zarsky and de Andrade 2013). ‘Soft’ eID providers on the other hand have specific social and economic traits which distinguish them from ‘hard’ eID providers. These traits are that the identification process is incidental to the relevant companies overall business plan, that the initial and subsequent identification and verification processes are carried out remotely, and that the company engaged in eID intermediation is operating in a lightly

² Official term used in the literature, though sometimes also other terms are used, e.g. identity intermediary. In fact this role can be divided across different entities, including e.g. a registration and/or an authentication authority.

regulated setting (Zarsky and de Andrade 2013). Accordingly, for soft eID providers often only light regulation and no oversight exists. When the identity provider offers the authentication function as an additional service, this is often done as a means to achieve other objectives (Zarsky and de Andrade 2013).

Example of Facebook Connect/Facebook Login

In this section the example of Facebook Login will be explained and a short data protection analysis on the basis of the General Data Protection Regulation (GDPR) made, considering aspects such as which lawful ground can be used, the purpose limitation, and who is controller and processor in the login constellation. ‘Login with Facebook’ is an example of the earlier mentioned ‘soft eID provider’. Jøsang stated that social websites became ‘de facto’ federated identity providers, ‘although this was never intended when these websites were first started.’ (Jøsang 2014, 73). Facebook Connect was introduced in 2008, with the aim to ‘allow users to “connect” their Facebook identity, friends and privacy to any site’ (Morin 2008). Starting from December 2008, any website could integrate Facebook connect (Facebook 2008). The stated goal was the social component: to ‘transform the Web into a more social place where Facebook’s users could engage in trusted social experiences with their friends’ (Facebook 2008) rather than to provide an electronic identity service.

In 2013, Facebook Connect was rebranded into Facebook Login during the announcement of an updated version of the service, in which mobile apps must ask separately for permission to post on the users Facebook timeline (Facebook 2013). In 2014 an update was announced where people could choose which information an app gets, and the start of development of an Anonymous Login was announced (Facebook 2014). This Anonymous Login would allow people log to in without sharing personal information with the app, yet it apparently never came further than beta (Wagner 2015).

Currently, Facebook Login is one of the most used social logins³ (Statista 2017). It provides the possibility to log in with the Facebook credentials (username-password) at a multitude of services across different platforms, including devices (e.g. IoT, Smart TVs) (Facebook1, Facebook2).

The relying party can request different datasets from the information available on Facebook. Three permissions are always available: public profile, email, and user_friends. 'Public profile' includes information such as the userID (unique numeric string for each app), the person's cover photo, the person's full name, the age range and a link to the person's timeline; 'User_friends' provides access to the list of friends that also use the app, and 'email' provides the person's primary email address (Facebook3, Facebook4).

If considered necessary and if they pass a review from Facebook, relying parties can request more information. Dating application Tinder for instance does not only request the Facebook profile and email address, but also *'interests, likes, gender, birthday, education history, relationship interests, current city, photos, personal description, friends list, and information about and photos of your Facebook friends who might be common Facebook friends with other Tinder users.'* (Tinder 2017)

Data protection legislation requires for every processing of personal data that a lawful ground exists. Generally, the lawful ground for the data processing in case of social logins is consent. Normally, when logging in with a social login at a service for the first

³ From the Statista report 'Social login preference of global internet users as of 2nd quarter 2016' Facebook has a share of 53,1%, Google+ 44,8% and Twitter, LinkedIn and others around 1% or below.

time, the service will ask for consent that certain information will be obtained from the profile.

Another aspect is the proportionality of the data transactions. In principle the information that Facebook transfers with the login is oftentimes the information that is also available on the user's public page. From the online description, Facebook aims to provide a certain level of proportionality, by requiring review of login permissions if they extend beyond the public user profile, user_friends and email.

Facebook states that it uses two criteria for review: utility (it should improve the user experience) and visibility (the use of the data should be directly visible in the app) (Facebook5). Facebook furthermore states that permission requests for data that may be used later are not accepted, all requested data must be visibly used within the service and that service should only request the permissions it really needs (Facebook5). For information requests other than user profile, user_friends and email, the user is also able to uncheck the boxes when logging in for the first time, in order to avoid the sharing of the information.

Another important aspect in data protection legislation is the identification of controller and processor, since the responsibilities are allocated to these roles, and the controller is the main party responsible to comply with the provisions of the GDPR. Since both the social network identity provider and the relying party determine the purposes and means of the processing of the personal data, they can most likely both be considered controllers. Even though the means are partially the same, since they both use the Facebook API, every controller has a separate purpose. They have not jointly defined means, since the API is unilaterally defined by Facebook and the relying party decides to install it and defines its further use of the received information. As this is unlikely to be

considered a common set of operations, they are most likely separate controllers. (Art.29 WP, 2010).⁴

This has some effects. For example can people revoke the permissions at a later point in time in their Facebook interface (Facebook6). This will not necessarily have a direct effect on the information in the database of the relying party. The latter will need to be contacted separately. With regard to the accuracy of information or other data subject rights, the user can contact Facebook for the information on Facebook, but will have to contact the relying party in order to exercise their right regarding the information in the database of the relying party.

Use of Facebook Login for e-government access?

Even though various identity management systems exist, for most systems the usage figures are not very high, which is often attributed to the ‘chicken-and-egg problem’ (Bruegger and Roßnagel 2016): Relying parties will only implement the necessary technical requirements to authenticate with a specific identity management system if enough users will use it, while users will only get a specific online identity to authenticate if it can be used at enough services. For Facebook Login this is not a problem,

⁴ However, since the assessment of controller is a factual assessment, it is also possible that they could be considered joint controllers. E.g. the AG in case C-210/16 considered the administrator of a fan page on Facebook as joint controller of the processing of personal data that is carried out for the purpose of compiling viewing statistics for that fan page (Opinion of Advocate General Bot, delivered on 24 October 2017, Case C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, nr 77). However, in that case both the administrator and Facebook use the viewing statistics, while in case of social login it seems that Facebook simply transfers the information to the relying party and therefore it is more likely a case of separate controllers.

as the user base already exists and therefore it is attractive for relying parties to integrate the option to log in with Facebook. Since Facebook Login does not suffer the problem of many other identity management systems as it already has a big user base, could it also be a solution for e-government login?

Many governments have built or are building their own electronic identity systems. Some of these systems are purely for e-government purposes, some can also be used outside of e-government, and some, instead of developing a governmental eID, provide the framework to allow private eIDs for their e-government systems. It is possible that a private party provides an identity management system for e-government use and many countries involve private parties (e.g. UK, US). For example in Belgium new legislation has been enacted in order to allow citizens to use private electronic identities for eGovernment access (Belgian eID law 2017).

On an EU level, in 2014 the eIDAS Regulation on electronic identification and trust services was introduced to provide ‘a common foundation for secure electronic interaction between citizens, businesses and public authorities’ (eIDAS Regulation 2014). The eIDAS Regulation provides a broader legal framework than the previous eSignatures Directive, referring in the first part to electronic identities and in the second to trust services (including not only electronic signatures but also several other electronic trust services). The scope of the part of the eIDAS Regulation relating to electronic identities, however, is limited only to notified eIDs. These eIDs have been notified by the Member State to the European Commission and then included in a list in order to be used for accessing cross-border online public services. Other Member States must then recognize and accept the notified eIDs for their e-government services.

Martin and de Andrade (2013) analyzed the benefits and drawbacks of using social networking services for e-government purposes. Important drawbacks which they

identified are the unreliability of the registration, threats to anonymity and pseudonymity, the exclusion of parts of the population who do not use social network services as well as security, privacy, jurisdictional and liability issues. They consider that the drawbacks largely outweigh the benefits, which consist mainly in the fact that social networking services have a large user base, infrastructure reliability, social acceptance and cost-effectiveness. Considering the existing security and privacy protections, social network logins should only be considered for low-risk, low-value and non-sensitive transactions (Martin and de Andrade 2013). However, they criticized that the draft eIDAS Regulation did not consider the public sector use of social network based eIDs and stated that social network based eIDs could be used if the social network provider would either use more reliable profile data or check against official data sources, and built in additional security and privacy protections (Martin and de Andrade 2013).

The final eIDAS Regulation provisions refer to private providers only in the recitals 13 and 17, stating that Member States can decide if they involve the private sector in the provision of electronic identification means and whether they want to notify them. They also recommend that Member States should encourage the private sector to voluntarily use notified electronic identification means.

A Member State could notify a private eID solution which it recognizes for its own e-government services, so that the citizens could use it to access e-government services across the EU (art. 7 (a) (iii) eIDAS Regulation). However, the notifying Member State has to ensure certain requirements, including the adherence to standards and the online availability of authentication means (art. 7 eIDAS). In addition, they should accept liability for the notified electronic identification scheme regarding intentional or negligently caused damage in a cross-border transaction due to the failure

to ensure the eID data is attributed to the right person or the availability of the online authentication (art. 11 jo. Art. 7 (d) and (f) eIDAS). Therefore, it is unlikely that Member States would notify a foreign social network provider.

However, on a national level, countries could use social network logins for access to e-government services if national legal requirements are fulfilled. Considering the earlier mentioned issues it is however currently unlikely that social logins could be used for public services requiring a reliable identification⁵.

The spider in the web

The use of one social network account for accessing other services is convenient for the user. However, it places the social network identity provider in the middle of the web which has certain disadvantages.

From a security point of view it is beneficial that the user has to remember less passwords, and therefore might use one strong password to keep the central account secure. On the other hand this concentration is also the weakness, since it provides a central point of attack and as soon as the login to the social networking account has been obtained, various other services are available to the attacker. Facebook requires in its

⁵ However, it might still be considered, e.g. the UK NHS: Marshall, Chris. 2016. Guest blog: Identity in health – getting to know you. January 12th 2016 <http://transformation.blog.nhs.uk/guest-blog-identity-in-health-getting-to-know-you> and providers might use more reliable identification in future (e.g. Airbnb uses a combination of the offline identity (e.g. copy of ID card) and online identity (e.g. Facebook login) to authenticate it's users (Airbnb verified ID: Airbnb. 2013. Introducing Airbnb verified ID. 30.4.2013. <https://blog.airbnb.com/introducing-airbnb-verified-id/>). In principle, Airbnb could then again become an identity provider with a more reliable identification than e.g. Facebook.

terms and conditions that the ‘you will not share the password [...], let anyone else access your account or do anything else that might jeopardize the security of your account’(Facebook 2015). Especially the requirement of not doing anything that might jeopardize the security of the account puts a rather broad and vague burden upon the user.

The central position of the social network provider makes it possible to have an overview of the services where the user logs in. At the side of the relying party, even though in principle the userID received from Facebook is unique per relying party, it would still be possible to link the person’s full name and e-mail address across different relying parties or use one of the possibilities that Facebook provides to map users across different apps (Facebook7), which is in principle only provided in case the apps are owned and operated by the same business entity. On the side of Facebook all the logins at different services can be linked to one account. Not even the proposed anonymous login would have changed this, as Facebook would still have received the information regarding which websites the user logs in, only the relying party would not have received information beyond that the user has a Facebook account. On the other hand this knowledge by Facebook enables the user to have an overview of the services for which the Facebook Login has been used/to which services the personal Facebook account is connected. Exactly which information Facebook receives when a user logs in at another website is not publicly specified. In Facebook’s privacy policy it states that Facebook collects information when third-party websites and apps with Facebook services (such as Facebook Login) are used, including information about the visited websites and apps, the use of Facebook Services on these websites and apps, and information that the developer or publisher of the app or website provides to Facebook (Facebook 2016a).

The increased use of social logins can have other disadvantageous effects. For example, the increase of service providers that require a social login to use their services

results in an exclusion of everybody who does not have a social network account, or whose account has been terminated/disabled for some reason. At the same time it creates a certain lock-in effect. Users cannot simply delete their Facebook account, as this would deter their access to various completely unrelated services on the internet where they signed up with the account. This will be further analyzed in the next sections.

Lock-in

One aspect that needs to be taken into account in case of social networks is the network effect. The network effect exists when the value of a network increases with the amount of users joining the network (Gebicka & Heinemann 2014). In relation to social networks, it is considered a multi-sided network effect, whereby increasing numbers of users result in additional value from the platform for advertisers (Graef 2015). 'Markets in which multi-sided businesses operate are typically quite concentrated, since it is necessary to have a critical mass of customers on both sides before the platform can be successfully launched' (Graef 2015) which is the chicken-and-egg problem mentioned earlier.

Another aspect are the switching costs for users. Spencer, Weber, Waller (2012) referred to the 'stickiness' of online social networks, referring also to Facebook Connect as a way to increase switching costs for users. This effect together with the network effect results in a 'serious possibility that Facebook already has market power over current users who are, or feel, locked-in to the system.' (Spencer, Weber and Waller 2012). Network effects and data lock-in may even make it likely that Facebook is a market by itself (Spencer, Weber and Waller 2012).

As Graef (2015) mentions, the 'inability of users to move their data to another social network' has attracted attention from scholars and from the European Commission which included a right to data portability in the draft GDPR.

The final GDPR introduces a new right to data portability in article 20 GDPR. This right is intended to facilitate switching between different service providers (Art. 29 Data Protection Working Party 2017). Therefore the question arises whether the right to data portability could provide a solution for the lock-in of social network users? The right of data portability in essence means a right to receive the personal data, which the data subject gave to the service provider. The user should receive the information in a structured, commonly used and machine-readable format and it should be possible to transmit this data to another controller (art. 20 GDPR), whereby the scope of the data portability provision is restricted to processing operations which are based upon the data subject's consent or on a contract (Art. 29 Data Protection Working Party 2017). The data that needs to be provided by the controller is data which concerns the data subject, which has been provided by the data subject (either directly or indirectly, for example access logs) and which does not adversely affect the rights and freedoms of others (Art. 29 Data Protection Working Party 2017). This shows that the right to data portability is not useful against the lock-in effect of a social network log-in, as it provides a right to obtain the data, not a right to the provision of a specific service.

Graef (2015) compared the right to data portability with the right to number portability introduced in the EU telecommunication sector and points out several weaknesses of data portability as the situation in online social networks is more complicated. Considering that the possession of a phone with a certain telephone number is sometimes used as authentication credential, could a similar system as number portability be considered for social network log-in? In case of number portability telephone numbers are assigned by public authorities and then merely allocated to users by the telecom operators, therefore the portability relates only to questions of how fast and against which price it should be possible (Graef 2015). In

most cases it requires mainly a change in a central reference database upon which the telecom operators update their own databases (Electronic Communications Committee 2010, 8). After the number has been ported, normally the first telecom provider is not involved in the number anymore.

The issue for social network login is that generally the identity provider is involved in the authentication, i.e. for example when Facebook Login is used then Facebook needs to verify that the user is indeed a Facebook user and transfer the required information to the relying party. Due to this involvement of the identity provider in every authentication, the electronic identity of the user cannot simply be ported. Other technologies exist whereby the credentials can be independent from the identity provider (e.g. attribute based credentials), however, these are currently not used in case of social network login.

On a side note, it should be mentioned that social network login can be useful for data portability requests at the service provider level, e.g. if a user wants to transfer playlists from one music streaming provider to another. This however relates to the fact that the service provider needs to authenticate the data subject which makes a data portability request, whereby the existing authentication procedure, e.g. a social login, that has been used for signing up, can be used for this purpose (Art. 29 Data Protection Working Party 2017). Data portability is also useful if the user wants to transfer the provided information from one social network provider to another, e.g. from Facebook to Google+. However, such a transfer does not mean that in future the user automatically can login with their Google+ account at service providers where they signed up with their Facebook account. The connected account needs to be separately replaced at every service where they signed up with their Facebook account, and the service provider is not obliged to provide different ways to sign up. The relying party

trusts the social network provider as an identity provider, and includes the technical requirements so that the user can log in with their social network account. Therefore, the control over which login possibilities are available for example for a website or an app, lies with the relying party providing the website or app, and not so much at the side of Facebook, who only provides the possibility to integrate the authentication service.

Accordingly, the data portability provision of the GDPR will not provide a solution to the lock-in effect of Facebook Login. Whether it could be addressed by competition law, or should at least be considered a factor in an analysis of Facebook's position from the competition point of view cannot be analyzed in this paper.

Gebicka & Heinemann (2014) state that until social media has gained fundamental significance, the companies should be free to develop their products since 'from a consumer entertainment point of view, having as many features as possible greatly contributes to the value of the website.' (Gebicka & Heinemann 2014), and the user is free to choose to use Facebook.

Lock-out

People who do not have a social network account will sometimes not be able to access online services. For most relying parties it will be a business decision whether they use only one social login or also integrate other authentication possibilities, depending mainly on their customer base. This would be different in case public services would use social login, as generally public services should be accessible to the public, not only to the parts of the public that possess a social media account. This aspect would need to be considered in case the public service would base their processing on necessity for compliance with a legal obligation or necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (art. 6 (1) c and e GDPR), but especially if consent

would be used as lawful ground for the data processing of the social login. Consent requires that it must have been freely given and recital 43 of the GDPR specifies that in case the controller is a public authority it is unlikely that the consent was freely given. Therefore, in order to ensure that the consent was freely given, it would be necessary that other options are available to access the e-government service, so the user is not forced to use a social login. The question whether consent is indeed freely given can also be relevant in case of private relying parties, as art. 7 (4) GDPR indicates that ‘tying’ the provision of a service to consent to the processing of personal data that is not necessary for the performance is ‘highly undesirable’ (Article 29 Working Party 2017a). Obtaining information from Facebook might often be necessary for providing the service, however, sending information to Facebook might be questionable in this context. Therefore, not only to ensure that also people without a social media account can access, but also to ensure that the consent is indeed free, it would be advisable for relying parties to give different access possibilities.

Another lock-out issue is that people who have a social network account and used it to sign up at services lose the access as the social network provider decides to terminate the account. When Facebook and other social login providers decide to terminate the account there is not a real option to object to the decision. As the terms and conditions are quite broad, in principle many reasons for termination can be found.⁶ In case of non-

⁶ For example often the strict real name policy can be a reason for termination, as the author Salman Rushdie found, Wilson, Cherry. 2011. ‘Salman Rushdie able to use own name on Facebook after identity conflict.’ 14.11.2011, <https://www.theguardian.com/technology/2011/nov/14/salman-rushdie-facebook-identity>. Other examples: Leydon, Chris. 2013. ‘What happened when I got my Facebook account disabled.’ 15.1.2013, <https://thenextweb.com/facebook/2013/01/15/what-happened-when-facebook-disabled-my-account/>, McCue, Matt. 2012. ‘What I Learned When

compliance with the terms and conditions, Facebook can stop providing the Facebook service partially or completely (Facebook 2015), generally without prior notice. This broad clause is considered to most likely fall under the Unfair Terms Directive, and for example in Belgium it is considered unlawful, with the exception of cases of ‘force majeure’ (Van Alsenoy et al. 2015), but, except for users from Germany, the terms and conditions have not yet been changed.

For users whose place of residence is Germany special rules apply regarding dismissal for cause, including the requirement of an appropriate time limit and provision of notice (Facebook 2016). These special rules are the result of a case brought before a German court, where among other parts of Facebooks terms and conditions, the termination clause was invalidated (Landgericht Berlin 2012; Van Alsenoy et al. 2015). When German residents infringe terms and conditions, the termination of their account is only allowed after a warning or an obligation to remedy has expired unsuccessful. Taking into account the interests of both parties, only if the user refuses to fulfil its obligations or if there are special circumstances justifying it, an immediate termination is possible (Facebook 2016).

For users who are not German residents, the termination is enacted immediately and the user is informed of it by email or when trying to open the Facebook account. In case of termination, the user will generally not be able to access the unrelated services for which he registered using the Facebook account, though it might be possible to regain access with the help of the customer support of the service.

Facebook Disabled My Account.’ 3.2.2012, <http://www.optimizationtoday.com/social-media/what-i-learned-when-facebook-disabled-my-account/>. See also (Van Alsenoy et al. 2015) for more examples of Facebooks reasons for termination.

As the user loses access to other, unrelated, services when the Facebook account is terminated, it would be advisable to provide all users, not only the German ones, with a notice when the account is about to be terminated. This notice could also provide the information on the related services for which social logins were used, and how to change these in order to be able to still get access to the other services.

Providing this kind of information would not only decrease the lock-out effect but could also be useful regarding the previously mentioned lock-in effect, and accordingly it would be helpful to also provide it when the user terminates the account. Furthermore, considering the right to data portability in the GDPR, the notice could inform the user regarding the possibility to extract their personal data before the account is terminated.

Conclusion

Social network logins are increasingly used to authenticate internet users when they want to login for online services, whereby Facebook is currently the biggest social network login provider. To see how broad social network logins could be used it has been analysed whether they could also be used for e-government services, considering the analysis of Martin and de Andrade (2013) and the now final eIDAS Regulation. Considering the deficits, social logins in their current form should not be used for e-government access, or only for systems where it is not relevant whether the user is reliably identified and when other ways to access the service are available.

An important issue regarding social network logins is the fact that users can essentially be locked in their use of a social network provider as it is necessary for their access to other services, and locked out from these other services in case they do not want to use a social network service or if the social network provider, whose account is used for access, terminates their account. It was assessed whether data portability could

provide a solution to this issue, however, given the involvement of the identity provider in the authentication of a user, users cannot simply port their social network login. Considering termination it has been assessed at the example of Facebook, that all users should be informed beforehand of a termination of their account and given the possibility to change the login for services where they signed up with their Facebook account.

In order to obtain freely given consent and avoid a user lock-in, it is important that a user can sign up at services via other login possibilities than Facebook Login, and a user can decide to stop using Facebook and manually register/link the account at a service provider with another way to log in, or simply not to use the service provider as it is not an important service. In case this is not given anymore, for example if due to the network effect Facebook becomes the biggest identity provider and is e.g. also used for relevant services, this might need to be considered from the side of competition as well as data protection legislation. However, the party which would need to be addressed might not be the identity provider, but the relying parties using the identity provider to give access to their services.

References

- Alpár, Gergely, Jaap-Henk Hoempan, Johanneke Siljee. 2011. The Identity Crisis – Security, Privacy and Usability Issues in Identity Management. ArXiv.
<https://arxiv.org/abs/1101.0427>.
- Article 29 Data Protection Working Party. 2010. Opinion 1/2010 on the concepts of “controller” and “processor”. Adopted on 16.2.2010,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.
- Article 29 Data Protection Working Party. 2017. Guidelines on the right to data portability. WP 202 rev.01, Adopted on 13 December 2016, as last Revised and adopted on 4 April 2017.

- Article 29 Data Protection Working Party. 2017a. Guidelines on Consent under Regulation 2016/679. WP 259, Adopted on 28 November 2017.
- Belgian eID law. 2017. 8 July 2017 - Wet inzake elektronische identificatie. B.S. 9.8.2017. http://www.ejustice.just.fgov.be/mopdf/2017/08/09_1.pdf#Page7 .
- Bruegger, Bud and Heiko Roßnagel. 2016. Towards a Decentralized Identity Management Ecosystem for Europe and Beyond. In: *Open Identity Summit 2016, Lecture Notes in Informatics (LNI)*, edited by D. Hühnlein, H. Roßnagel, C. Schunck, M. Talamo, 55-66. Bonn: Gesellschaft für Informatik.
- Cameron, Kim. 2005. The Laws of Identity. As of 5.11.2005, <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf> .
- De Andrade, N. N. G. 2012. Towards a European eID regulatory framework. Challenges in constructing a legal framework for the protection and management of electronic identities. In: *European data protection: in good health?*, ed. S. Gutwirth, P. De Hert, R. Leenes and Y. Pullet, 285-314. Dordrecht: Springer.
- eIDAS Regulation. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. OJ L 257, 28.8.2014.
- Electronic Communications Committee. 2010. Number Portability Efficiency: Impact and analysis of certain aspects in article 30.4 of the Universal Service Directive and general remarks on NP efficiency. ECC Report 155. Luxembourg, November 2010. <http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP155.PDF>.
- Engemann, C. 2016. Digitale Identität nach Snowden - Grundordnungen zwischen deklarativer und relationaler Identität. In *Der digitale Bürger und seine Identität*, edited by G. Hornung, C. Engemann, 23-63. Baden-Baden: Nomos.
- Facebook. 2008. Facebook Expands its Social Platform across the Web Through General Availability of Facebook Connect. 4.12.2008, <https://newsroom.fb.com/news/2008/12/facebook-expands-its-social-platform-across-the-web-through-general-availability-of-facebook-connect/>.
- Facebook. 2013. Updates to Facebook Login. 22.8.2013, <https://newsroom.fb.com/news/2013/08/updates-to-facebook-login/>.

- Facebook. 2014. Introducing Anonymous Login and an Updated Facebook Login.
30.4.2014, <https://newsroom.fb.com/news/2014/04/f8-introducing-anonymous-login-and-an-updated-facebook-login/>.
- Facebook. 2015. Legal Terms. Last changed 30.1.2015,
<https://www.facebook.com/legal/terms>
- Facebook. 2016. Für Nutzer mit Wohnsitz in Deutschland. Last changed 2.2.2016,
<https://www.facebook.com/terms/provisions/german/index.php>.
- Facebook. 2016a. Facebook Data Policy, Last changed 29.9.2016,
<https://www.facebook.com/about/privacy/>.
- Facebook1. Add Facebook Login to Your App or Website.
<https://developers.facebook.com/docs/facebook-login/>.
- Facebook2. Facebook Login for Devices.
<https://developers.facebook.com/docs/facebook-login/for-devices>.
- Facebook3. Permissions Reference – Facebook Login.
<https://developers.facebook.com/docs/facebook-login/permissions#reference-public-profile>.
- Facebook4. Graph API Version 2.10. <https://developers.facebook.com/docs/graph-api/reference/user>.
- Facebook5. What is Login Review?. <https://developers.facebook.com/docs/facebook-login/review/what-is-login-review>.
- Facebook6. Permissions with Facebook Login.
<https://developers.facebook.com/docs/facebook-login/permissions/overview>.
- Facebook7. Mapping Users Across Apps and Pages.
<https://developers.facebook.com/docs/apps/for-business>
- Gebicka, Aleksandra and Andreas Heinemann. 2014. Social Media & Competition Law.
World Competition 37 no. 2 :149–172.
- General Data Protection Regulation (GDPR). 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. OJ L 119, 4.5.2016.
- Hansen, Marit, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, Michael Waidner. 2004. Privacy-Enhancing Identity Management. *Information Security Technical Report* 9 no. 1: 35-44.

- Hansen, Marit, Andreas Pfitzmann, and Sandra Steinbrecher. 2008. Identity Management throughout One's Whole Life. *Information Security Technical Report* 13 no. 2:83–94. <https://doi.org/10.1016/j.istr.2008.06.003>.
- Jøsang, Audun. 2014. Identity management and trusted interaction in Internet and mobile computing. *IET Information Security* 8 no. 2: 67–79.
- Jøsang, Audun, Muhammed Al Zomai, Suriadi Suriadi. 2007. ACSW '07 Proceedings of the fifth Australasian symposium on ACSW frontiers - Volume 68, eds. L. Brankovic, P. Coddington, J.F. Roddick, C. Steketee, J.R. Warren, and A. Wendelborn, 147. Darlinghurst: Australian Computer Society, Inc.
- Landgericht Berlin. 2012. Judgement of 6 March 2012, Az. 16 O 551/10, <http://openjur.de/u/269310.print>.
- Martin, A.K. and N.N.Gomes de Andrade. 2013. Friending the taxman: On the use of social networking services for government eID in Europe. *Telecommunication Policy* 37 no. 9: 715-724.
- Morin, Dave. 2008. Announcing Facebook Connect. 9.5.2008, <https://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect/>
- Smedinghoff, Thomas J. 2012. Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review* 28: 532-541.
- Statista. 2017. Social login preference of global internet users as of 2nd quarter 2016. <https://www.statista.com/statistics/459601/preferred-social-login-id-global/>.
- Van Alsenoy, Brendan, Valerie Verdoodt, Rob Heyman, Ellen Wauters, Jef Ausloos, Günes Acar. 2015. SPION From social media service to advertising network - A critical analysis of Facebook's Revised Policies and Terms. Draft 25 August 2015 v1.3. <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-3.pdf>.
- The Telegraph. 2012. Companies asking for Facebook passwords for future employees. 20.3.2012. <http://www.telegraph.co.uk/technology/facebook/9155368/Companies-asking-for-Facebook-passwords-for-future-employees.html>.
- Tinder. 2017. Tinder Privacy Policy, last updated 26.10.2017. <https://www.gotinder.com/privacy>.

Wagner, Kurt. 2015. Whatever Happened to Facebook's Anonymous Login? 6.3.2015.
<https://www.recode.net/2015/3/6/11559878/whatever-happened-to-facebooks-anonymous-login>.

Zarsky, Tal Z., and Norberto Nuno Gomes de Andrade. 2013. Regulating Electronic Identity Intermediaries: The Soft EID Conundrum. *Ohio State Law Journal* 74:1335.