Privacy Enhancing Technologies in Social Networks

Kevin Valk[1] and Mark Vijfvinkel[2]

[1] Radboud University
kevin@kevinvalk.nl
[2] Radboud University
m.vijfvinkel@student.ru.nl

1 Introduction

Social networks have a history almost as old as the internet, or at least the World Wide Web, itself. Before the World Wide Web there were bulletin board systems, that allowed people to share information and communicate with each other. The World Wide Web allowed for websites to be created and this resulted into the development of the first social networks[1]. One of the first was known as GeoCities and allowed users to create pages that were placed in 'neighborhoods'. Early 2000s social networks as MySpace and LinkedIn were created. In 2004 Facebook started and in 2005 YouTube. 2006 saw the launch of Twitter and in 2008 Facebook overtook MySpace with monthly visitors. In 2013 Facebook has more than one billion users.

The top ten of social networking sites as of June 2014 are, Facebook, Twitter, LinkedIn, Pinterest, Google Plus+, Tumblr, Instagram, VK, Flickr and MySpace, respectively[2].

However some of these sites have different business models. For example, where Facebook allows users to post messages, photos and chat; Twitter allows users to only send a 140 character message and Pinterest functions more like a digital pin-up board. Therefore a definition is necessary to determine more precisely what a social network is.

The Article 29 Working Party (WP)[3] defines a social network as *"communication platforms which enable individuals to join or create networks of like-minded users[1]."* According to the WP, a social network service (SNS)[4] is an information society service in the legal sense. The WP also provides certain characteristics for a SNS [1]:

- *"users are invited to provide personal data for the purpose of generating a description of themselves or 'profile'"*

[1] http://www2.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html, accessed on 11-06-2014

[2] http://www.ebizmba.com/articles/social-networking-websites, accessed on 11-06-2014

[3] For more information on the Article 29 Working Party we refer to section 3.1.

[4] Social network and social network service are the same and shall be used interchangeably in this paper.

- *"SNS also provide tools which allow users to post their own material (user-generated content such as a photograph or a diary entry, music or video clip or links to other sites)"*
- *" 'social networking' is enabled using tools which provide a list of contacts for each user, and with which users can interact."*

Also SNS *"generate much of their revenue through advertising which is served alongside the web pages set up and accessed by users [1]."*

From the users point of view a social network allows them to share experiences with their contacts, keep in touch with their friends and meet new people for free.

However during the last few years there have been some cases which have raised concerns about privacy in social networks. In section 2 we will elaborate on two cases which address some of these privacy concerns. The following examples will help to illustrate the problems.

Example 1: A user has friends, family members and work colleagues in their contact list. The user has a bad experience at work and in the heat of the moment, publishes some insulting comments on his or her public profile. It is okay for friends and family to see this message, but colleagues might take offense, resulting in the user getting fired. If the user cannot delete the message future job interviews prove in vain, because the initial 'social network screening' shows this message. This can be seen as an infringement of the users relational privacy.

Example 2: From the point of view of the social network it is more profitable to store as much information as possible about a user. The social network might therefore decide not to delete everything the user publishes, but simply not show it on the profile any longer. To the user it seems that the message or photo is indeed deleted, but the social network still stores the message in their database. This might haunt the user years later if this data is released into the public and can be seen as an infringement of platform privacy.

In this paper we will use the definitions used in Article 2 of the Data Protection Directive (DPD) [3]. The definitions are as follows:

- Personal data: Any data relating to a directly or indirectly identified or identifiable natural person
- Data Subject: The natural person belonging to this personal data
- Data Controller: The responsible party that determines means and purposes of processing of personal data (Service Provider)
- Data Processor: Processing personal data on behalf of data controller
- Data Processing: Any operation or set of operations which is performed upon personal data

The rest of this paper is organised as follows. Section 2 will elaborate on the above mentioned examples. In section 3 we will explain which legislation applies to social networks. We will discuss technical solutions to the privacy problems in section 4. Lastly we will conclude with section 5.

2 Privacy issues

In this section we will discuss two cases that help illustrate the privacy concerns regarding social networks.

2.1 Europe versus Facebook

In 2011 a group of students from the University of Vienna filed 22 complaints with the Irish[5] Data Protection Commissioner. They also requested a copy of their user data Facebook had stored in its databases. The copy of the user data consisted of several CD-roms. On each CD there was a PDF with the user data of one user, one PDF was 1200 pages. This user data included data that was thought to be deleted from Facebook by the user.

The 22 complaints filed with the Irish Data Protection Commissioner consisted of, certain data not being deleted but set to not show on the users page. For example, pokes, postings, messages, tags, friends and pictures. Other complaints included tagging without consent, vague privacy policy, face recognition, posting on other users' pages, etc[6]

There have been no definitive results about this case yet and it is also still ongoing. However this case does provide us with a practical example of platform privacy. Namely, Facebook still retains data even if the user has 'deleted' it.

Moreover, one complaint (posting on other users' pages) also deals with relational privacy. It describes that the user is not aware with whom information is being shared. For example, a post on a friends' wall is subject to that of a friends' privacy settings and not to the settings of the original user.

2.2 Mario Costeja González vs Google

The case of Mario Costeja González vs Google is another practical example of both relational and platform privacy. Although not directly related to social networks.

Mr. González was forced to auction his property because of social security debts. The information about the auction and his name were published in La Vanguardia (Spanish newspaper) in 1998. The newspaper has published editions on the web, including the edition with the auction from Mr. González. In 2009, Mr. González contacted the newspaper to request for deletion of the publication, because when searched for his name on Google, one result was the publication. The newspaper denied the request because the publication was done on the request of Spanish Ministry of Labour and Social Affairs.

Mr. González then proceeded to request Google for deletion of the reference to the article. Google did not comply and thus Mr. González lodged a complaint with the Spanish Data Protection Agency, demanding that both Google and the newspaper remove the data. On 30 July 2010, the Spanish Data Protection Agency rejected the complaint against the newspaper, but accepted the complaint against Google.

[5] The Facebook terms are agreed upon with Facebook Ireland Limited, if a user resides outside of the United States or Canada.

[6] An overview of all the complaints can be found on http://europe-v-facebook.org/EN/Complaints/complaints.html, accessed on 11-06-2014.

Google fought against this complaint before the National High Court of Spain. The High Court postponed the ruling because of a few similar cases regarding the interpretation of the Data Protection Directive (DPD) [3] which the Court of Justice of the European Union was working on. The advocate general at the European Court of Justice, Niilo Jääskinen, gave his opinion on 25 June 2013. The opinion was as follows (summary) [8]:

- Google's business model brought Google within the scope of the DPD.
- Google could not be regarded as a data controller. Google's indexation involves processing personal data, but they do not become the data controller when the processing is carried out in a haphazard, indiscriminate and random manner.
- If the Court did not agree with Google not becoming a data controller then he held that the rights of freedom of information and expression took precedence over the right to be forgotten[7].

The Court of Justice of the European Union ruled in favour of Mr. González [5]. The Court did not agree with the advocate general that Google was not a data controller. Google was now seen as a data controller and therefore Google was responsible. The Court also stated that Articles 7 and 8 of the Charter of Fundamental Rights of the European Union [4] together with Article 14 of the DPD should give the data subject right to access the data and thus request for erasure of the data.

2.3 Problem definition

Relation Privacy covers the consequences the user experiences in their personal environment. In other words, it concerns the privacy of a person regarding the personal information that person shares with their relations. As mentioned, Example 1 in section 1 fits this description.

Platform Privacy covers the consequences the user experiences with respect to a platform. In our case this concerns the privacy of a person regarding the personal information that person shares with the social network. Example 2 in section 1 fits this description.

However, the cases mentioned can show that these two definitions can overlap depending on the point of view. Recall the case of Europe vs Facebook, where posting on other users' pages is subject to that users' policy and not to the policy of the original poster. This would have consequences for that original poster's relation privacy, but it is the social network that does not provide the possibility of messages falling under the poster's policy. The latter point of view shows that this problem can fit into both definitions.

Also in the Europe vs Facebook case it turned out that certain types of personal data were not deleted but set to 'not display'. This can fit in the definition of Platform Privacy, but when the not deleted data becomes public at some point, it might have consequences for the user under the definition of Relational Privacy.

As mentioned the case of Mr. González vs Google is not related to social networks, but to search engines. However it is not hard to imagine a similar

[7] See section 3.2 for more information.

case in the context of social networks. The social network would then be obliged to remove references of posts about users that affect those users in a negative way.

Both cases show a general problem that can affect the users of social networks, namely; that data is not being deleted. This problem falls under both definitions, as the users will rely on social networks to actually delete their data (Platform Privacy), such that it will not have consequences for them in the future (Relational Privacy).

3 Legal framework

Applying the definitions of data controller and data processor, as mentioned in section 1, to the environment of a social network can be complicated. As users can supply the social network with information, but they can also edit or remove information. This can be their personal data, but also personal data from contacts. For example, tagging[8] a friend in a photo can be a form of data processing happening on somebodies personal data. But who is the controller or the processor? Who determined the purpose of processing in this case? Who did the actual processing?

Not having a clear distinction between controller and processor could pose a problem for the data deletion problem stated at the end of section 2.3. If a user is the controller and/or processor then the user could be responsible for handling the data deletion requests from their contacts. Depending on the amount of contacts and requests this could be impractical for the user.

To help solve the above mentioned questions the Article 29 Working Party wrote an opinion on this matter.

3.1 Article 29 Working Party

The Article 29 Working Party (WP) is an independent advisory and consultative body that gives expert advices to the member states regarding data protection, coordinates global enforcement of national supervisors and gives opinions in regard to protection of personal data.

One of the opinions the WP has written, is about online social networking [1] and focuses on how social networks can operate in compliance of European data protection legislation. It also explains that users of a social network operate within a personal sphere and that therefore the household exemption applies. The household exemption is stated in Article 3 of DPD. It states: *"This Directive shall not apply to the processing of personal data: ...by a natural person in the course of a purely personal or household activity"* [3].

This means that regulations that would normally apply to data controllers do not apply to users. However, the household exemption does not apply in certain circumstances. For example, *"if a SNS user acts on behalf of a company or association, or uses the SNS mainly as a platform to advance commercial, political or charitable goals, the exception does not apply [1]."*

[8] tagging means marking a person or item in a photo

3.2 Data Protection Regulation

The DPD is not sufficient any more as it does not consider important aspects of current technological advances, economic aspects, business models and the value of personal data [7]. Also rules regarding data protection are different across all the member states of the EU. With the Data Protection Regulation the EU wants to put the DPD into a set of regulations that all member states have to uphold and also update it to better match the current demands of data protection. The regulation [6] proposal was released on 25 January 2012 and the Council aims to have it adopted in late 2014. After a transition period of two years the regulation comes into full effect.

The new Data Protection Regulation gives EU residents not only protection inside Europe, but the protection also extends to organisations outside Europe. The latter applies when an organisation processes personal data of EU residents. Furthermore the conceptual right to be forgotten will be 'replaced' by the right to erasure. It is important to note that there does not exist a concrete right like the "right to be forgotten". Article 12(b) of the DPD has a statement about rectifying, erasing or blocking data. The grounds on which data can be deleted is defined as "does not comply with the provisions of the DPD, in particular because of the incomplete or inaccurate nature of the data" [3]. To conclude, the right to be forgotten will not be replaced, but is rather implemented as a more defined right in the draft regulation.

This right will give data subjects the ability to request data removal on a number of grounds which makes it possible to remove personal data more easily in contrast to the limited grounds article 12(b) of the DPD gives.

4 Privacy Enhancing Technologies

4.1 Distributed social networks

As shown section 1 and 2 there can be issues where personal data is owned by someone else than the data subject itself. This is the case with all popular social networks like, Facebook, Google+, Xing, etc. All the personal data the social networks have about a data subject is stored on a server they own. Buchegger et al. coined the idea to introduce a distributed storage for personal data to create a peer to peer (P2P) social network [2].

Such a P2P network has a big difference in regard to the normal client-server kind of setups the current social networks use. There is not a single entity responsible for all data. Instead, there are numerous of different smaller parties that all bear the responsibility of the personal data they have. One can even decide to set up an entity only for one user. With these setup possibilities there is a choice for every user.

Namely if the user wants complete control over his personal data, he can set up his own server. Or the user can give up some control and place his or her personal data by a server the user trusts.

There are other changes concerning traditional social networks described by Buchegger at al. but for our discussions we mainly discuss the fact that the data is stored on a server the user can choose.

4.1.1 Discussion

The advantage of a distributed social network is decentralised storage of personal data and that the user has more control over their personal data. When setting up a server for only one user, that user will get complete control over their data. However, a distributed social network has a completely different business model than a centralised social network like Facebook. Taking Diaspora*[9] as an example for a distributed social network, to further develop, Diaspora* relies on donations rather than behavioral advertising. It is our opinion that this creates a lot less revenue, resulting in development progressing slowly and staying behind major social networks.

Also the amount of effort to set up Diaspora* is more than creating an account on a centralised social network. This will also prevent a distributed social network to reach the masses.

We find it very unlikely that centralised social networks will change towards a distributed social network model, because this will not correspond with their business plan. Because the development is slow, behind on the features, for example apps on a smartphone and somewhat of an effort to setup, it will be difficult for a distributed social network to gain a big following.

In our opinion gaining a big following is necessary for people to switch to a distributed social network or demand a more distributed approach from their current social network. While this PET definitely sounds interesting and has some potential, we think that it will only satisfy a niche market.

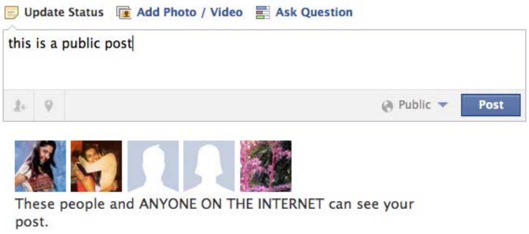
4.2 Privacy nudging

“Anecdotal evidence and scholarly research have shown that a significant portion of internet users experience regrets over their online disclosures” [10]. Humans are certainly not perfect and more so when they are browsing the web. This is also shown in the paper Privacy Nudges for Social Media. In the paper the writers propose technologies that could create paternalistic interventions to mitigate regret when sharing data on the internet. For example, a boss calls an employee and demands the employee to do something directly. The employee is offended by this and in the heat of the moment, posts his or hers displeasure on a social network. Unfortunately the employee has his colleagues and boss listed as contacts, whom can now see the message. This can cause anything from a small uproar up to the employees’ dismissal.

Wang et al. created a prototype system with Facebook as a test case to prevent such mishaps. In the rest of the paper they name such mishaps regret. The proposed implementation has three different types of technologies (nudges). All of the types the researchers describe can be mixed together in the final implementation.

[9] Diaspora* is an implementation of a P2P social network [11]

4.2.1 Profile Picture Nudge



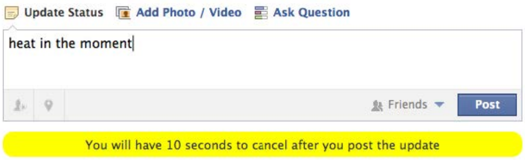
this is a public post

These people and ANYONE ON THE INTERNET can see your post.

Figure 1: Change to Facebook showing the profile picture nudge

It turns out that one of the causes of regret is that people often do not know what their audience is when sharing information. This can be because of not keeping track of who all the friends are or just not being aware of the fact that everybody can see the post (privacy settings). Because of this, Facebook users share information to more recipients than only the intended recipient. To counter this Want et al. implemented a simple overview of the audience underneath the post field on Facebook. Beneath the post field there are five random profile pictures of friends that will be able to see the post and a clear and simple textual explanation who can see the post when posted.

4.2.2 Timer Nudge



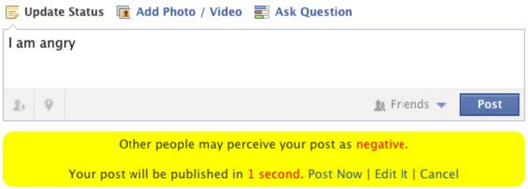
heat in the moment

You will have 10 seconds to cancel after you post the update

Figure 2: Timer nudge before clicking the "Post" button

As shown in the example given in the introduction of this PET. Sometimes information is shared in the heat of the moment to obtain easy gratification. This could not be the intended effect but was biased because of the "spur of the moment" action. To prevent such heated information from getting posted online. The researchers created a simple system that presents the user with a yellow bar beneath the post field of Facebook. Whenever the user clicks on the "Post" button it will not be sent to Facebook directly, but instead there is a grace period of X seconds. After the grace period is expired the information is send to Facebook normally. Within the grace period, the user can reflect on their post and decide to cancel the post or post it as originally.

4.2.3 Sentiment Nudge



I am angry

Other people may perceive your post as negative.

Your post will be published in 1 second.

Figure 3: An example of how a post could be perceived

The sentiment nudge is an addition to the timer nudge. Research shows that regrettable posts on Facebook often contain negativity, profanity, or sensitive topics like alcohol and sex [10]. Wang et al. used and open-source sentiment-analysis module to analyse the content of the post. When the user is presented with the timer, the user is also presented with a textual representation of how others could perceive the post. The module uses the AFINN-111, which is a list of 2,477 English words and phrases manually rated as negative or positive, on a scale between -5 and 5. For each word in the post the score is added to a global total. A positive total value could then be interpreted as a positive post, while a negative total value could be interpreted as a negative post.

4.2.4 Discussion

The paper presents good results, where almost every test subject had prevented regrettable posts. In our lecture the general consent was that the nudges are good technologies to prevent information from becoming public, that on second opinion was not intended to be published. Our opinion is in line with the general consent of the discussion on this subject. It is well known that it is very hard to completely remove information from the internet. With a system in place that helps users to prevent data from even reaching the internet. That will save a lot of work for different parties and regret for the user. For example, when someone would post a racist remark on Facebook, that gets picked up by Google, then the poster would have to delete it from Facebook and also file a request for deletion to Google. This request includes a lot of private information about the user and it will certainly cost more than ten seconds to file the request. While a simple timer on the Facebook posts could prevent this from occurring all together. In the discussion in our lecture, the problem on how to make this accessible to all users was raised. At the moment this prototype exists of browser plugins and Facebook addons. Thus the normal Facebook user will probably not necessarily take the time or have the knowledge to install everything. From the discussion it became clear that Facebook themselves could even be tempted to implement this feature, because it will show goodwill and therefore even attract more users to Facebook. However it might also increase the amount of personal data Facebook, or any social network using this PET, can collect. The decision of not posting a message, but revising it and then publishing it, will provide a social network with more insight into the behaviour of the user. This will create more revenue for the social network, but it might also lead to more privacy infringement of the user. We are of the opinion that this PET shows potential, but should be used with caution and maybe not be implemented by social networks, but kept as a browser plugin.

4.3 Sticky Policies

One way to allow users to have more control over their personal data would be the use of sticky policies. Sticky policies are machine-readable policies that ‘stick’ to personal data. The policy defines what processing is allowed to happen to that data.

A social network itself, for example Facebook, is a vast network that spans several countries. Third party applications also use the social network to collect and process personal information. Therefore personal information can be transferred across several organisations and locations, and be subject to different forms and purposes of processing. The advantage of a sticky policy is that the user of a social network can predetermine what happens to their personal data even when it travels across multiple organisations. A sticky policy mechanism can therefore be seen as a form of platform privacy, as defined in section 2.

4.3.1 Technical details

A user could use a sticky policy to specify the following [9]:

- The use of personal data, for example processing of location information or types of market research
- Allow the data to be used on only a specific platform
- The third parties that are allowed to process the users information
- Blacklists or deletion/minimization of personal data after a certain time
- Trusted authorities

Figure 5 shows the management of the sticky policy mechanisms. Below we will relate the sticky policy mechanism described in [9] to a social network setting.

A social network needs a framework that defines their preferences and policies. The user is able to apply policies to certain items or subsets of personal data.

For example, the social network would define a policy to automatically delete photos after two weeks, one year or never. The user would then be able to choose from these three options for each photo or all photos.

A user(client)-side component allows for the policies to be created and attaches the policy to the users personal data and TAs (also chosen by the user from a list provided by the social network). The personal data is then encrypted and send together with the sticky polices to the social network.

The encryption/decryption process works as follows [9], see figure 5. The user creates a policy and a symmetric key K. The key is used to encrypt the personal data. It is possible to encrypt different parts of the data using different symmetric keys. This allows for different parts of the data to be revealed. For example, only a name is revealed but not age. The following message is then send to the social network [9]

- The personal data (encrypted with key K);
- the sticky policy;
- key K;
- the policy hash

This message is encrypted with the public key of the TA and signed with user's private key (note that this is not key K). It is now possible to verify the source of the policy, its integrity and binds key K to the data and the policy. The message is then send to the social network.

At this moment the social network does not have access to the personal data. The social network must then interact with the selected TA and promise that it will adhere to the policy. The message from the social network to the TA consists of the sticky policy and the encrypted shared keys [9]. The TA can determine the likelihood the promise is fulfilled by checking a blacklist or reputation system or verifying system properties. This creates an audit trail that is available to the user and TA in case of policy violation.

If the TA is satisfied the social network can keep its promise, it will release the keys (key K) to the social network. The message from the TA to the social network consists of key K appended to the policy hash and encrypted with the public key of the social network. Only now the social network is able to decrypt the personal data and verify the policie's integrity.

Figure 4 shows an overview of the sticky policy mechanisms across several parties [9]. A social network might have a third party providing a form of processing or allow applications that separately collect data. When the social network wants to provide personal data to a third party it has to send this encrypted and with the same policy as the user provided. For the third party to gain access to the personal data it also has to be verified by the TA, before the TA provides the keys.

4.3.2 Discussion

Sticky policies provide a user with more control over their personal data as it travels across multiple parties. It also allows for an audit trail for the user and the trusted authority at the time a policy is violated.

However, the main disadvantage of a sticky policy scheme is trust, more specifically that all the involved parties will keep their 'promises'. From the moment that the social network can decrypt the personal data, the social network has full control over the personal data. The social network can, for example, decide not to comply with the user's policy, but send the decrypted personal data to a third party. This can be a third party that the user actually specified as forbidden in its sticky policy. The third party can also apply operations that the user specified as not allowed.

The trusted authority is also able to decrypt the personal data. Thus next to the social network, the user also has to trust the trusted authority.

As already mentioned the social network will gain full access to the data and needs to keep a promise in order to comply with the sticky policy. As soon as the promise is broken the role of the trusted authority, who checks the promises and policies, can be omitted. This leaves room for discussion on the presence of a TA in general. Social networks that want to show a more active role in ensuring privacy can adopt a sticky policy scheme and make it mandatory for third parties to abide by it. It could also be achieved through client-side software or a peer-to-peer mechanism [9]. However with the help of legislation, social networks can be obligated to comply with a sticky policy standard. This standard would help an organisation, e.g. a data protection authority, to enforce data protection legislation. The legislation would have to be translated to a sticky policy that a social network has to comply with. The social network could add to policy, but not weaken it. The data protection authority would be able to check if promises are broken by randomly surveying the social network, enforcing fines in case of violation and manage the reputation of the social network.

5 Conclusion

The general problem in this paper is that users of social networks are not in control of their own personal data. For a user this can have consequences with respect to their relation privacy or platform privacy. We have described three potential solutions to this problem. However, each PET does not solve the problem completely.

A distributed social network offers a solution when the storage location of personal data might lead to an infringement of privacy. For example, personal data stored in a nation under a dictatorship. Using a distributed social network where the storage location can be chosen by the user can help, as a location might be chosen in a nation with better privacy legislation. The downsides of a distributed social network is the difficulty of setting it up and the potentially slow development, because of the different business model compared to non-distributed social networks.

Privacy nudging shows the most potential and would be the easiest to implement as a browser plug-in or by the social network itself. In the latter case however, it might actually lead to more infringement of the user's privacy.

Sticky policies show potential in a wide variety of applications, but rely too much on all parties keeping their 'promises'. It is our opinion that, with strong legislation or at least a trusted authority with means to enforce a sticky policy scheme, this PET could work. If only in hindsight when a policy is violated. In other words, if a user can prove that his policy is violated and this can be confirmed by a trusted authority, then this could be used as evidence in a court case.

However, the CNIL[10] vs Google case has shown that fines are low with respect to privacy cases. In this particular case the fine was a 150000 euro's[11], which is very little for a billion dollar company. If these types of fines stay low, then the use of PETs is trivial.

In our opinion a combination of PETs, more up-to-date or foreseeing legislation (although the latter will be improbable) and strong enforcement might solve the problem of lack of control over personal data in social networks.

[10] Commission Nationale de l'Informatique et des Libertés, is the french data protection authority

[11] http://www.theguardian.com/technology/2014/feb/10/googles-link-french-privacy-fine-crashes-watchdog-cnil, accessed on 19-06-2014

Appendix A:

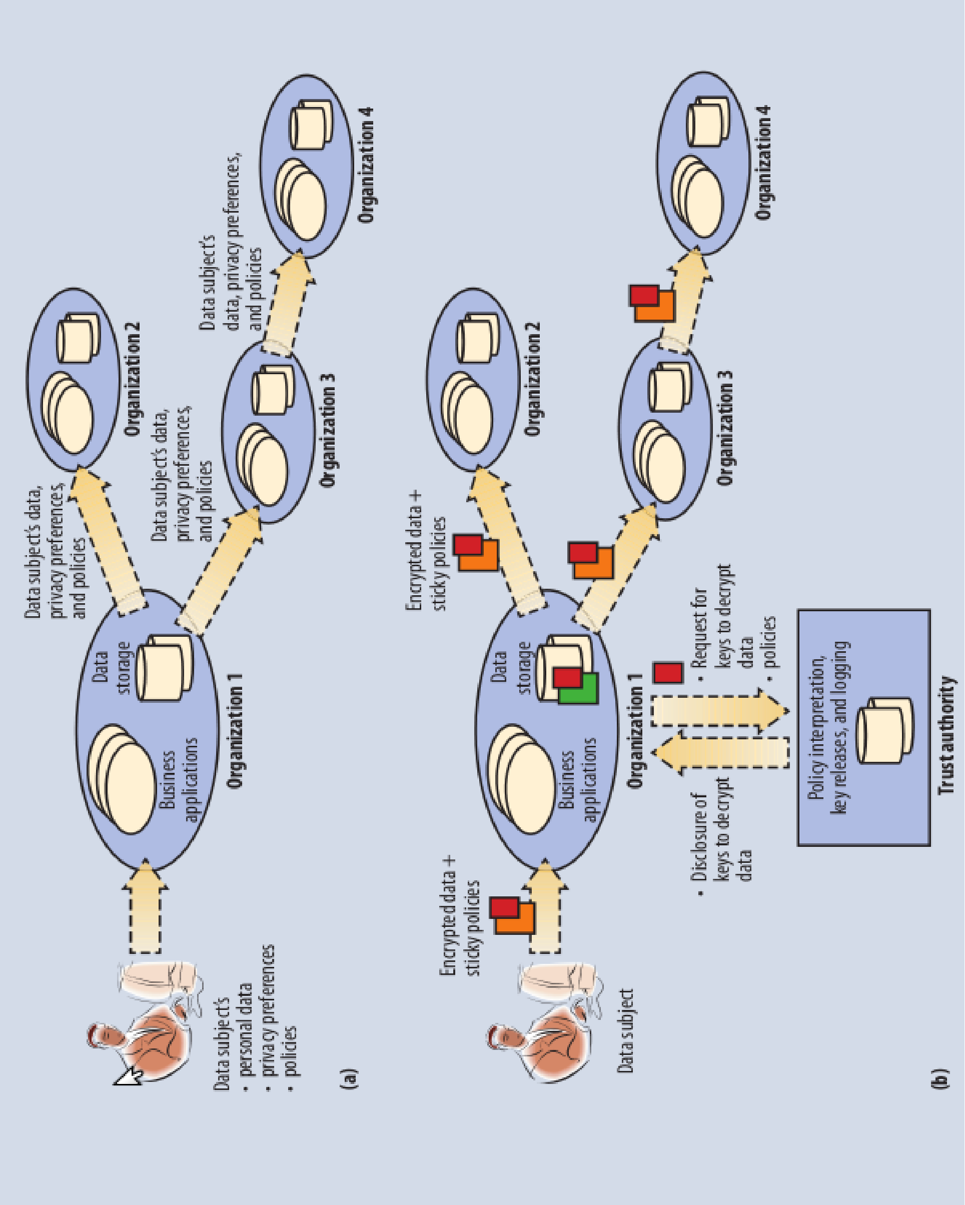

Data subject's
• personal data
• privacy preferences
• policies
(a)
Business applications
Data storage
Organization 1
Data subject's data, privacy preferences, and policies
Organization 2
Data subject's data, privacy preferences, and policies
Organization 3
Data subject's data, privacy preferences, and policies
Organization 4
Data subject
Encrypted data + sticky policies
Business applications
Data storage
Organization 1
Encrypted data + sticky policies
Organization 2
Organization 3
Organization 4
• Disclosure of keys to decrypt data
• Request for keys to decrypt data
• policies
Policy interpretation, key releases, and logging
Trust authority
(b)

Figure 4: "*High-level scenario and related management of sticky policies. (a) High-level scenario involving data disclosures across organizations. (b) Overview of sticky policy approach.*" [9].

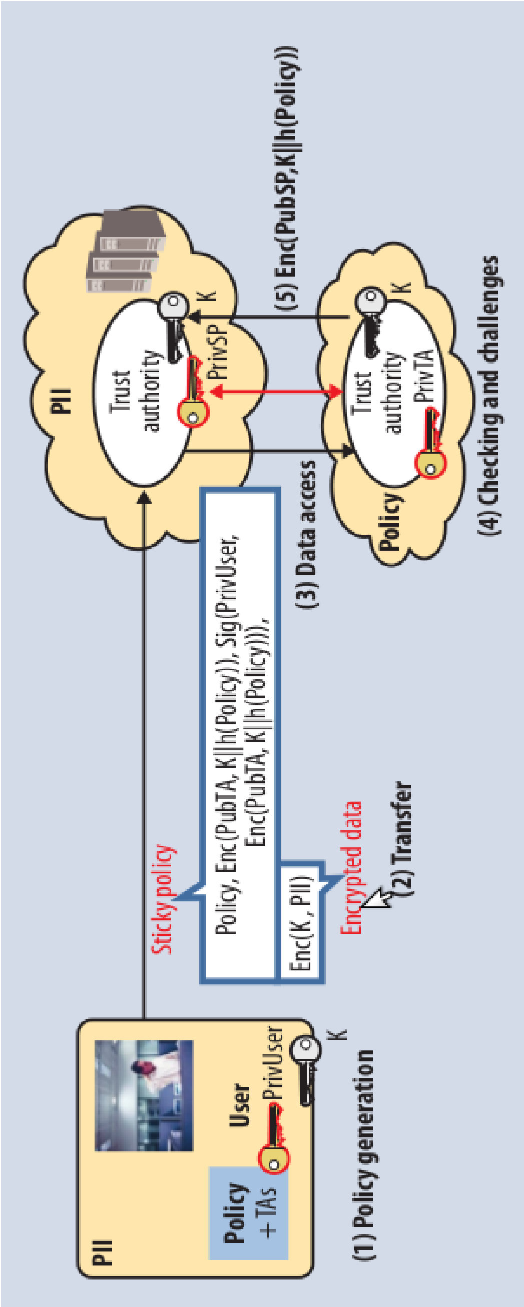


Figure 5: "*Core mechanisms underpinning the management of sticky policies. (1) Creation of sticky policies at the user side. (2) Sending sticky policies and data to the service provider. (3) Sending sticky policies to the agreed trust authority to get access to data. (4) Service provider interacts with trust authority to satisfy sticky policy constraints. (5) Getting cryptographic keys for use in accessing the data.*" [9].

References

[1] Article 29 Data Protection Working Party. Opinion 5/2009 on online social networking, June 2009. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[2] S. Buchegger and A. Datta. A case for P2P infrastructure for social networks - opportunities and challenges. February 2009. http://www.peerson.net/papers/wons09p2psn.pdf.

[3] Council of Europe. 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. *Official Journal of the EC*, 1995. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[4] Council of Europe. Charter of Fundamental Rights of the European Union. *Official Journal of the EC*, 2000. http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[5] Court of Justice of the European Union. Google spain sl, google inc. v agencia española de protección de datos, mario costeja gonzález, May 2014. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[6] European Commission. on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[7] European Commission. Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century. 2012. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf.

[8] N. Jääskinen. Opinion of advocate general Jääskinen - Case C-131/12, June 2013. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=138782&occ=first&dir=&cid=45442.

[9] S. Pearson and M. C. Mont. Sticky policies: An approach for managing privacy across multiple parties. *Computer*, 44(9):60–68, September 2011. http://dx.doi.org/10.1109/MC.2011.225.

[10] Y. Wang, P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor. Privacy nudges for social media: An exploratory facebook study. pages 763–770, 2013. http://dl.acm.org/citation.cfm?id=2487788.2488038.

[11] I. Zhitomirskiy, D. Grippi, M. Salzberg, and R. Sofaer. Diaspora*, 2010. https://diasporafoundation.org/.