Privacy policies in social networks: An Analysis of Facebook, Twitter, Google+ & LinkedIn policies and relevant legislation to determine adequacy in protecting user privacy

Minerva Hoessl

Technical Report

RHUL–ISG–2017–6

10 February 2017

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom
Privacy Policies in Social Networks: An Analysis of Facebook, Twitter, Google+ & LinkedIn Policies and relevant Legislation to determine Adequacy in protecting User Privacy

Supervisor: John Austen

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature:

Date:
I would like to convey my deepest thanks to Dr. Chez Ciechanowicz for taking a chance and believing in me.

Many thanks also to John Austen for the guidance and answering my many questions.
Figures & Tables

FIGURES

Figure 1 Initial Facebook pop-up notification for the application Quizzes ........................................ 13
Figure 2 Further information on what constitutes ‘Public Profile’ information ........................... 13
Figure 3 Average Monthly Active Users from 2010 to March 2016 .................................................. 24
Figure 4 AccountKiller - How to delete your Twitter account ............................................................ 27
Figure 5 Twitter Transparency Report United Kingdom ................................................................. 28
Figure 6 LinkedIn: Optional invitations after synching ................................................................. 46
Figure 7 AccountKiller - How to delete your LinkedIn Account ....................................................... 47
Figure 8 JustDelete.me LinkedIn account deletion ........................................................................... 48
Figure 9 Response from ‘LinkedIn Trust and Safety’ ......................................................................... 49

TABLES

Table 1 Social Network Advertisement Revenues 2014 - 2017 ......................................................... 5
Table 2 Main problems encountered in Facebook, Twitter, Google+ and LinkedIn .................... 65
Table 3 Comparison of the General Data Protection Regulation & Directive 95/46/EC .......... 105
## Abbreviations & Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad</td>
<td>Advertisement</td>
</tr>
<tr>
<td>APP</td>
<td>Application</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GBP</td>
<td>Great Britain Pounds</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>Inc.</td>
<td>Incorporated</td>
</tr>
<tr>
<td>IP Address</td>
<td>Internet Protocol Address</td>
</tr>
<tr>
<td>NSA</td>
<td>United States National Security Agency</td>
</tr>
<tr>
<td>PPD-28</td>
<td>U.S. Presidential Policy Directive 28</td>
</tr>
<tr>
<td>PRISM</td>
<td>Planning Tool for Resource Integration, Synchronization, and Management</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service commonly referred to as ‘Text Message’</td>
</tr>
<tr>
<td>U.K.</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>U.S.</td>
<td>United States of America</td>
</tr>
<tr>
<td>USD</td>
<td>United States Dollar</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Local area wireless computer network</td>
</tr>
</tbody>
</table>
Executive Summary

User numbers on social networks are increasing steadily. Users continue to share a wide variety of personal and public information on the Internet and are becoming more educated and aware of data protection. This is resulting in an increased desire for better Internet privacy. Social networks, on the other hand, are largely driven by marketing revenue and therefore have a need for an ever-increasing amount of user information in order to generate targeted advertisements. It is increasingly apparent that the interests of users and social networks are conflicting.

The purpose of this report is the review of the user policies of four of the top social networks, as well as of relevant pieces of legislation, in order to determine their adequacy in protecting user privacy. Reviewed were the policies of Facebook, Twitter, Google+ and LinkedIn as well as the U.K. Data Protection Act 1998, the Irish Data Protection Act 1988/2003, the Directive 95/46/EC and the newly adopted General Data Protection Regulation 2016/679 and EU-U.S. Privacy Shield.

As a result of the policy reviews several common areas of concern were found. These are content that is ‘public’ by default, massive data collection, data sharing practices, data retention practices and data transfer insecurities. Users have no control over the massive data collection practices of social networks. Legislation in support of limiting data collection from the outset would be required but, for commercial reasons, this is not likely to occur. The problems with social networks’ data sharing practices stem from their own definition of ‘personal data’. Too much information is deemed ‘public’ and thus freely shared. Anomysation of data is used as a crutch to allow user data storage even after the user requests account deletion. Some social networks state that they may never delete user information from their backup servers. These are areas where legislation could support the users’ desire for more privacy rights. However, the effectiveness of the relevant pieces of legislation that were reviewed may only be limited. Generally speaking, relevant legislation favours free flow of information for commercial purposes over increased user privacy. The best effort to improve user privacy was seen in the General Data Protection Regulation (EU) 2016/679 (GDPR). The GDPR will vastly improve the quality of communication between social networks and users. Social networks will be obligated to disclose more concise, easy to understand information and to put a maximum limit on how long data may be stored. However, the GDPR is still seen to favour commercial aspects over user privacy and thus is likely to only increase user privacy by a small margin.
The battle between providing an increased level of user privacy and the free flow of information for commercial purposes will continue. Only collaborative pressure from both governments and users may swing the scale in favour of user privacy over annual profits. More realistically, users who choose to use social networks and are concerned with their privacy must educate themselves by carefully reading the policies of such sites and must realise that any information shared will be available to multiple entities. Unless social networks are introduced on a paid-for membership basis, a higher level of user privacy will not be achievable.

Issues raised in this paper have been updated as much as possible up to July 31, 2016. While writing this paper the United Kingdom (U.K.) has also made the decision to leave the EU (European Union). In the near future this will affect the relevance of EU specific pieces of legislation depending on whether the United Kingdom will adopt such practices or choose to use only U.K. specific data protection requirements. Because of the on-going changes occurring presently, some information or relevancy of information presented in this paper may have changed by the time it is submitted.
Introduction

Currently there are over 7.3 billion people on earth. 3.4 billion of these are said to be active Internet users with approximately 2.3 billion having an active social media account. [SK-16]

Looking at a more local picture, the United Kingdom is estimated to have a population of about 64.9 million with an average of 59 million active Internet users, of which 38 million have active social media accounts. This amounts to approximately 59% of the total population in the United Kingdom. Between January 2015 and January 2016, the average daily use of social media in the U.K. was estimated at 1 hour 29 minutes. This is down from just over 2 hours recorded for the previous year. [SK-15] [SK-16] There are varying social network statistics available on-line. However, it is clear that a large portion of the world’s population has active social media accounts. Social network usage has experienced a steady growth in the past years, as has their revenue.

Revenue from advertising is a tremendously important aspect to social networks. This often seems to result in a reversed sense of priorities whereby revenue is prioritised over user privacy. Lawmakers are well aware that revenue losses, as well as international business relations, have to be a consideration when changing and implementing new privacy legislation. This leaves users of services such as social networks to a ‘use at your own risk’ notion, where they either agree to all terms of the site or must choose not to use the service. A reduction of profits in order to provide a more privacy friendly environment does not seem to be a possibility at this time. Social networks’ priority remains the increase of their revenue.

Figures available via website emarketer.com state the following social network advertising revenue figures from 2014 to a projected 2017 (see Table 1). Figures have been converted to Great Britain Pounds (GBP). [EM-15]

<table>
<thead>
<tr>
<th>Social Network Ad Revenues (in billions GBP)</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>7.78</td>
<td>11.02</td>
<td>14.50</td>
<td>18.26</td>
</tr>
<tr>
<td>Twitter</td>
<td>0.85</td>
<td>1.37</td>
<td>2.00</td>
<td>2.69</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>0.51</td>
<td>0.63</td>
<td>0.76</td>
<td>0.90</td>
</tr>
</tbody>
</table>

Table 1 Social Network Advertisement Revenues 2014 - 2017 [EM-15]

As can be seen, a continued increase in revenue is expected. It is not only profits that drive social media but also the political influence it can have over its users. Nowadays, social media has the power to influence votes more than newspapers do. An article in The Telegraph by Carl Miller, the research director of the Centre for the Analysis of Social Media at Demos, states that, "young people's votes in the 2015 general election were more
influenced by social media than by any other source”. He also aptly stated that, “whilst 2015 was a story of social media controlling more of public life, 2016 will see a battle over who controls social media”. [MC-15] The article is a reflection of the fact that times are changing. Users are becoming more aware that large companies such as Facebook and Google hold their personal information and use it for their own gains. Heightened media coverage of such topics as user privacy and data protection concerns have made users aware that sharing too much information on the Internet can be dangerous. Cyber crime is on the rise and with it the need for more security and protection of privacy. Cyber criminals are getting more skilled at embedding malware, hijacking accounts and using social engineering on social networks to mount attacks. LinkedIn, for example, is used frequently to gain information about companies in order to attempt spear phishing and other types of attacks.

In the Ofcom Communications Market Report from August 2015, social media users were asked whether they agreed with the statement: “I am happy to share information online that a wide audience can see”. Results showed that 57% of social media users disagreed, while 27% neither agreed nor disagreed and only 12% agreed. [OF-15-A] Because most users disagreed with the statement, it is surprising to see that most people continue to post private information on social networks.

This project focuses on the relationship that four of the top social networks, namely Facebook, Twitter, Google+ and LinkedIn, have with user privacy and how the relevant pieces of legislation may affect both the operation of social networks and the privacy of social network users. Based on the analysis of the social networks’ policies, I was able to determine recommendations that may be able to improve user privacy for specific problematic areas. The U.K. Data Protection Act 1998, Irish Data Protection Act 1988/2003, Directive 95/46/EC, General Data Protection Regulation 2016/679 and EU-U.S. Privacy Shield were also reviewed and analysed to determine how these aim to protect user privacy on social networks.

Please note that each social network’s policies and terms have been reviewed at different times. As such, the individual effective dates are stated in the relevant sections. Relevant pieces of legislation reviewed for the purpose of this paper were current as of July 31, 2016. Due to ongoing changes there may be more current versions available at the time of completion of this paper. The reader is advised to keep this in mind when reviewing the information.
Why Facebook, Twitter, Google+ & LinkedIn?

Contents

1 Why Facebook, Twitter, Google+ & LinkedIn?
1 Why Facebook, Twitter & Google+ & LinkedIn?

1.0.1 38 million active social media accounts are being used in the United Kingdom. Of all social networks Facebook, Twitter, Google+ and LinkedIn have been found amongst the most popular in the U.K. and thus have been chosen as subjects for this report. [SK-15]

1.0.2 Statistics about average user numbers tend to vary slightly among the different sites. Thus, the following list is a combination of statistics found on websites wearesocial.com and statista.com. [SK-16] [ST-16-A] [ST-16-F] Generally speaking the top social networks worldwide as of the end of April 2016, including the number of their average monthly active users, are:

- Facebook - 1.65 billion
- Qzone - 646 million
- Tumblr - 555 million
- Instagram - 405 million
- Twitter - 310 million
- Baidu Tieba - 300 million
- Sina Weibo - 222 million
- YY - 122 million
- VKontakte - 100 million
- Pinterest - 100 million
- LinkedIn - 100 million

Note: Current Google+ numbers were not available as Google+ was no longer included in statistics due to the inconsistencies about actual active user numbers. (See section 1.0.4) Numbers available range from 359 million monthly active users reported for December 2013 on the website statista.com [ST-16-G], to 300 million monthly active users as per an article by Kim Speier for Social Media Today, written February 2016. [KS-16]

1.0.3 According to the We Are Social special report *Digital in 2016*, dated January 2016, the top 5 social networks specifically for the U.K. are: [SK-16]

- Facebook
- Twitter
- Instagram
- Google+
- LinkedIn

Instagram has seen a steady rise in popularity in the last year. Since Facebook owns Instagram, it was decided to include LinkedIn in this policy review rather than another Facebook company.
1.0.4 Statistics placing Google+ in fourth place do not account for the lack of users who actually engage with Google+. Were the statistics on actual user engagement, Google+ would likely not be on the list of the top 5 social networks. Google+ has been struggling for years. In its early days Google+ practically forced users into signing up by making it mandatory in order to use YouTube features and by encouraging anyone with a Gmail account to join. This accounted for a rise in user numbers while numbers for actual active users remained low. In a study published in April 2015 by Eric Enge of Stone Temple Consulting, Enge concluded that only approximately 9.7% of Google+ accounts are active and that approximately 90% of accounts have never posted publicly and have no content. \[EE-15\] Even though Google+ may indeed not be an actual part of the top social networks, it has been included in this paper since the privacy policies for Google+ are the same as for Google. As Google is the top search engine used worldwide, its privacy policies are of great importance to a large number of Internet users.

1.0.5 Statistics can never paint an exact picture of social network usage or give a definitive list of the top social networks. They do however give a good approximation of the importance social networks have in today’s culture.
This page has been left blank intentionally.
Facebook

Contents

2.1 Facebook: Introduction

2.2 Facebook: Policy Review

2.3 Facebook: Conclusion
2.1 Facebook: Introduction

2.1.1 Facebook is a social networking service that was created in 2004 by Mark Zuckerberg, a Harvard student at that time. Initially designed as a networking tool only for Harvard students, it quickly spread to other schools and was finally opened to the public in 2006. Facebook is now the largest social network worldwide. In the first quarter of 2016 Facebook had more than 1.65 billion global monthly active users. [ST-16-F] Mobile device monthly active users were estimated at 1.51 billion in the first quarter of 2016. [ST-16-F]

2.1.2 In 2015 Facebook’s estimated net income was over 3.6 billion U.S. dollars (i.e. United States dollars or USD), approximately £2.6 billion, with an overall revenue estimated at over 17 billion U.S. dollars, approximately £12 billion, most of which is derived from advertising sales. [ST-16-E] This is why sharing content publicly on Facebook continues to be of great benefit to Facebook and their advertising revenue.

2.1.3 Facebook has been criticized for its extensive data collection practices used to drive revenue from targeted advertisements. For example, a new feature released by Facebook in early 2016 now lets users share, not just that they ‘like’ a certain post, but how they ‘feel’ about it. As stated in the article “New Facebook Reactions to Expand Data Collection” by Tom Risen for U.S. News: “Facebook’s new emojis give users more ways to share feelings about their posts, but the new reaction tabs that expand on the ‘like’ button also give the site new ways to track user behavior and market content”. [TR-16] New features are seen with skepticism in terms of whether such features were developed for user enjoyment or solely for Facebook to gather yet more information about their users. In recent years, Facebook has also been criticized for making it ever more difficult for users to control their privacy. Facebook provides numerous settings to its users, but because settings are located in different areas and are time consuming to set, they are often underutilized.

2.2 Facebook: Policy Review

2.2.1 Examined for this policy review were Facebook’s Statement of Rights and Responsibilities and Data Policy. These can be located at www.facebook.com/terms and www.facebook.com/about/privacy. [FB-15-A] [FB-15-B] The most current versions of these policies at the time this paper was written have a revision date of January 30, 2015. This policy review specifically covers points of particular importance to user privacy. As such, not all sections of these polices are covered in this review. A more detailed summary of the Statement of Rights and Responsibilities and Data Policy can be found in Appendix A and Appendix B.
2.2.2 By using or accessing Facebook Services the user automatically is seen to have agreed to the terms set out in Statement of Rights and Responsibilities and the Data Policy. No explicit consent is required. The Data Policy applies to all of the Facebook Services that do not make use of their own privacy policy. Facebook Services include Facebook branded and co-branded websites, social plugins such as the Facebook ‘Like’ or ‘Share’ button and other media, software, products and services. [FB-15-A] [FB-15-B]

2.2.3 **Content**

In the Statement of Rights and Responsibilities users are immediately advised that content and information submitted can be controlled using available settings. Content that is set to ‘public’ will be available to everyone. This includes both viewers who are on Facebook as well as off Facebook using search engines. [FB-15-A]

Facebook reserves the right to “*use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of*” any content submitted until the user deletes such contents or deletes the account. [FB-15-A] The Statement of Rights and Responsibilities further advises users that applications used while on Facebook will ask for their own permissions and use their own privacy policies. It is the user’s responsibility to grant or deny permissions to applications asking to access content and information. Users will receive a pop-up notification about what information will be shared with such apps (see Figure 1). Figure 1 demonstrates an example of a Facebook pop-up notification for an application called Quizzes. More detailed information is available by clicking on the information button supplied within the pop-up notification (see Figure 2). At a minimum an app (i.e. application) will gain access to the user’s profile information, which includes the name, profile picture, age range, gender, language, country and other public information as well as the e-mail address.

![Quizzes will receive the following info: your public profile and email address.](image1)

**Fig. 1** Initial Facebook pop-up notification for the application Quizzes

![Quizzes will receive the following info: your public profile includes name, profile picture, age range, gender, language, country and other public info.](image2)

**Fig. 2** Further information on what constitutes ‘Public Profile’ information

In Section 3 of the Statement of Rights and Responsibilities Facebook further advises users that it cannot guarantee that use of Facebook is safe. This includes any possible malicious code, harassment of users by other users or any other “*unlawful, misleading, malicious, or discriminatory*” actions. [FB-15-A] It further states in Section...
15 that Facebook does not “control or direct users’ actions on Facebook” and is “not responsible for the content or information users transmit or share on Facebook”. [FB-15-A] In short, use of Facebook Services is at the individual’s own risk.

2.2.4 **Data Collection**

Facebook collects extensive information from and about its users. Data Collection information is covered in Facebook’s Data Policy. [FB-15-B] Information collected as outlined in Section 1 of the Data Policy includes:

- Content and information submitted by users.
- Actions of the user, including content viewed and interacted with.
- Information provided by the user when syncing information with Facebook.
- Content and information provided by other Facebook users about the specific user, such as when they tag a photo or send a message to that user.
- Associates and groups the user is in contact with.
- Extensive device information. The extent of such collection is dependant on permissions granted to Facebook by the user. Information collected includes the “operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers”. [FB-15-B] It also includes location information, as can be ascertained using GPS (Global Positioning System), Bluetooth or Wi-Fi (Local area wireless computer network) signals as well as Internet service provider or mobile operator names, browser type, mobile phone number and IP (Internet Protocol) addresses. [FB-15-B]
- Information collected from applications and websites that use Facebook Services.
- Information collected from partner companies as well as from other companies owned or operated by Facebook.

Information is collected for the purpose of personalising the content and making suggestions to users. It is also used to deliver targeted advertisements and for security reasons such as for detecting suspicious activities. Cookies and other similar technologies are used to collect information for use in authentication, advertising, measurement, analytics, localisation, site functionality, performance measurement and improvement. [FB-16-B]

Overall, the extent of data collection is very similar to Google’s practices of data collection, which also captures any and all information available.

2.2.5 **Data Retention**

In Section 4 of the Data Policy the user is advised of the available tools such as the activity log and option to download all information stored by Facebook. Use of such tools will offer users some control over the different categories of information held by Facebook.
The Data Policy also states that information associated with an account is kept only until the account is deleted. Other data is stored for “as long as it is necessary to provide products and services to you and others”. [FB-15-B] It fails to state the amount of time such information may be stored for. A link is provided to guide users to information if they wish to delete or deactivate an account. After deleting an account it may take Facebook up to 90 days to remove information from their backup servers. However, the account and its information are immediately made unavailable to other Facebook users. [FB-16-D] In both the Statement of Rights and Responsibilities and the Data Policy, Facebook advises users that information shared with Facebook friends may still be available even after the account has been deleted since such information is stored and under control of their friends’ accounts.

2.2.6 Information Sharing and Disclosure

Section 9 of the Statement of Rights and Responsibilities advises users that Facebook will sell the ability to “display your name and/or profile picture with your content or information” to businesses for advertising purposes. [FB-15-A] This means Facebook can use the name, profile picture, content and information of a Facebook user for use with “commercial, sponsored, or related content”. [FB-15-A] It is thus important that users take the time to adjust their ad (advertisement) preference settings.

Section 3 of the Data Policy explains information-sharing practices of Facebook. It reminds users that public information is available to everyone and that users are responsible for adjusting the settings in order to control who has access to their information. It further advises users that they will lose control over submitted content if such content is submitted to a friend’s page. This fact is commonly overlooked and users will freely comment on a friend’s post and sometimes have a short conversation using the comment space, ignoring the fact that this conversation may be publicly viewable and are under the sole control of their friend.

Section 3 also informs users that Facebook will share user information freely amongst companies owned and operated by Facebook. A link provided reroutes the reader to a webpage listing companies owned and operated by Facebook. The companies listed are Atlas (advertising service), Facebook Payments Inc. (Incorporated), Instagram, LiveRail (advertising server and exchange), Moves (mobile app), Oculus (virtual reality developer), Onavo (mobile app developer), Parse (cloud-based application development platform) and WhatsApp. [FB-16-C] Facebook also partners with companies, in which case it does not share any personally identifiable. However, Facebook defines personally identifiable information simply as “information like name or email address that can by itself be used to contact you or identifies who you are”. [FB-15-B]
Definitions of personally identifiable information tend to vary within the United States. According to the U.S. Department of Commerce Office of the Chief Information Officer and as defined by the Office of Management and Budget Memorandum M-07-16, the definition of ‘personally identifiable information’ is “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.”. [CJ-07] [US-09] While the Chief Information Officer includes the combination of information, the California State Online Privacy Protection Act of 2003, Business and Professions Code, Chapter 22 Internet Privacy Requirements, Section 22577, only defines personally identifiable information as individually identifiable information and does not mention that a combination of information could identify an individual. [CL-04] As is evident, opinions differ whether personally identifiable information is only individual pieces of information or also applies to information that can identify an individual when combined with other pieces of information.

Within Europe the notion of ‘personal data’ is used instead of ‘personally identifiable information’. Since Facebook operates out of Ireland, both the Irish Data Protection Act and the U.K. Data Protection Act were compared in regard to their definition of ‘personal data’. [DP-A] [LG-A] Both agree that ‘personal data’ is data that can identify an individual on its own or, as stated in the U.K. Data Protection Act 1998, “from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller”. [LG-A] As a further comparison of definitions, the definition given in the newly adopted General Data Protection Regulation (EU) 2016/679 is that ‘personal data’ is any information that can identify a person “directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”. [EL-16]

Overall Facebook’s definition of ‘personal data’, as stated in the Data Policy, does not accommodate the European understanding of ‘personal data’ even though its European headquarters are based in Ireland and should thus define personal data as is defined by the Data Protection Commissioner in Ireland, until the General Data Protection Regulation comes into full effect in 2018. By only defining personally identifiable information as “information like name or email address that can by itself be used to contact you or identifies who you are” Facebook fails to consider that this is only appropriate for users from California. [FB-15-B] This poses a definite threat to the privacy of users outside of the state of California as Facebook may actually be sharing information that is in fact ‘personal data’ with any of its business partners.
Another concern about Facebook’s information sharing practices, in particular its information disclosure to the United States Government, has recently been a part of a highly publicized court case, Maximillian Schrems v. Data Protection Commissioner (Case C-362/14) that ultimately resulted in the invalidation of the U.S.-EU Safe Harbour Framework in October 2015. [EP-16] Due to information leaked by Edward Snowden that claimed that Facebook was a part of the U.S. PRISM (Planning Tool for Resource Integration, Synchronization, and Management) program, concerns arose that Facebook allows the U.S. to conduct mass surveillance on data of European residents that is stored on Facebook servers located within the United States. PRISM is a surveillance program run by the United States National Security Agency (NSA), which according to documents leaked by Edward Snowden counts amongst its participants companies such as Microsoft, Google, Facebook and Apple. [BB-14] [WI-16-C] Facebook has denied participation in the PRISM program. Facebook’s CEO (Chief Executive Officer) Mark Zuckerberg has stated in a comment posted on Facebook in June 2013 that, “Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our servers. We have never received a blanket request or court order from any government agency asking for information or metadata in bulk”. He continues to state: “When governments ask Facebook for data, we review each request carefully to make sure they always follow the correct processes and all applicable laws, and then only provide the information if is required by law.” [MZ-13] This information is also contained within the Data Policy which states that Facebook may “access, preserve and share” user information when required to do so based on a legal request, government investigation or to detect, prevent and investigate illegal activity. [FB-15-B] A Government Requests Report is available, which includes information about the number of requests received from individual countries and the percentage of requests for which Facebook disclosed some information. For example, requests made by the government of the United Kingdom between July 2015 and December 2015 totaled 4190 requests. Information was disclosed for 82% of these requests. [FB-16-E]

2.2.7 Data Transfer and Use

In Section 16 of the Statement of Rights and Responsibilities, Facebook advises users who are located outside of the United States that by agreeing to the statement they agree that their personal data may be transferred to and processed in the United States. [FB-15-A]

The Data Policy notifies users located within the EEA (European Economic Area), that their information may be transferred to “countries outside of the EEA”. [FB-15-B] When compared to the Statement of Rights and Responsibilities, which solely stated that data may be transferred to and processed in the United States, the Data Policy chooses to leave the exact country uncertain. Thus, it is uncertain if locations include
those outside of the U.S. where Facebook data centers are also located as well as Facebook office locations. According to Facebook, data center locations include only Sweden and the United States. In January 2016, Facebook announced that a new data center is also set to be built in Ireland, with a completion estimate of early 2018. [FL-16] [TF-16] Office locations, however, include a large number of countries including Argentina, Australia, Belgium, Brazil, Canada, China, Colombia, France, Germany, India, Indonesia, Ireland, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Poland, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, United Arab Emirates, United Kingdom, and the United States. [FB-16-F]

Because no definite information is given, the user will not know exactly where their information may be transferred to or processed. The Data Policy further advises that Facebook utilises the U.S.-EU Safe Harbour Framework for the “collection, use and retention of information from the European Union”. [FB-15-B] It however fails to inform users that the Safe Harbour agreement was invalidated in October 2015 and that it should no longer be used for data transfers between the European Union and the United States. Facebook fails to advise its users whether it is using other means in the interim.

2.2.8 Legal Jurisdiction

Legal jurisdiction is defined by Facebook in Section 15 of the Statement of Rights and Responsibilities and is designated to either the “U.S. District Court for the Northern District of California or a state court located in San Mateo County”. [FB-15-A] Any disputes involving users located outside of the United States and Canada should first be directed to Facebook Ireland Limited.

2.2.9 User-Friendly Information

Facebook provides a lot of guidance to its users. Section 8 of the Data Policy, for example, provides a link to a webpage named ‘Privacy Basics' which helps users to understand how best to use their Facebook account and secure their information and content. [FB-A] However, the amount of information available may be overwhelming to most users who are thus unlikely to read all of the advice Facebook provides.

2.3 Facebook: Conclusion

2.3.1 Overall, Facebook’s Statement of Rights and Responsibilities and the Data Policy are written in a user-friendly manner and provide users with a lot of information about Facebook practices.
2.3.2 The main areas where Facebook faces difficulties within their policies are in the areas of data sharing and retention. Here the information is kept vague and does not seem to take the rights of users located outside of the United States and Canada into much consideration. Overall, users must take responsibility to take the time to read information offered by Facebook and to adjust settings accordingly.

Possible problematic areas found in the Rights and Responsibilities and Data Policy

2.3.3 Content - Possible problematic areas
It is of benefit to Facebook when users share content publicly. Thus, it is the user’s responsibility to safeguard their content and information by adjusting the appropriate settings. However, settings are numerous and time consuming and thus many users fail to make all the necessary adjustments.

Applications available on Facebook are another area that may threaten a user’s privacy. Applications use their own privacy policies and will ask for varying degrees of permissions to access a user’s information and content. If users wish to minimise access to and use of their information and content by third-party applications, they should take the time to assess what information an application wishes to access and how such information is used and shared by that application.

2.3.4 Data Collection - Possible problematic areas
Facebook’s data collection practices are extensive. User data is collected not only from the Facebook site but also from third-party sites that partner or utilise Facebook Services. Facebook is also constantly developing new features and technologies to collect more data from users. Users must keep themselves up to date with Facebook’s latest developments and new settings.

2.3.5 Data Retention - Possible problematic areas
According to a separate webpage accessible via a link provided in Section 4 of the Data Policy, Facebook may store some information, including log records, after removing personal identifiers from such information, even after an account is deleted. However, Facebook fails to let the user know exactly what information is kept. It only provides one example, ‘log records’. [FB-16-D] In addition, users who read the Data Policy but do not choose to click on the provided link will not be informed of such residual storage of their information at all. Facebook also fails to state the maximum amount of time such residual information may be stored for and used by Facebook.

2.3.6 Information Sharing and Disclosure - Possible problematic areas
Information sharing is Facebook’s main problematic area. It is the users responsibility to control information sharing as much as possible using the numerous available
settings. Information sharing also occurs when users fail to realise that they cannot control the visibility of comments made on friends’ Facebook posts or when they blindly give access to third-party applications.

Facebook itself shares user information freely amongst companies owned and operated by Facebook. It also shares information with partner companies for which no list is provided. The main area of concern here is Facebook’s definition of personally identifiable information. Because it does not account for the fact that a combination of information may also identify a person, Facebook users cannot be certain that information shared with partner companies will not identify them. The definition used by Facebook is not in accordance with the European definition of ‘personal data’ and thus does not protect the rights of European Facebook users.

2.3.7 Data Transfer and International Use - Possible problematic areas
Facebook presents conflicting information to its users about transferring and processing user data in different locations. The Statement of Rights and Responsibilities advises users that their personal data may be transferred to and processed in the United States, but the Data Policy states that information may be transferred to “countries outside of the EEA” (European Economic Area). [FB-15-A] [FB-15-B] It does not solely specify transfer to the United States. Hence, users do not know which statement is actually correct. The Data Policy also informs users that Facebook utilises the U.S.-EU Safe Harbour Framework for transferring data to the United States. [FB-15-B] It fails to inform users that the framework is no longer a valid method for transferring data from the European Union.

My Recommendations
After analysis of the problematic areas I have determined the following recommendations in order to improve user privacy.

2.3.8 Data Collection - My Recommendations
The best way to limit the ever growing methods and practices of data collection is by protecting users with legislation that limits the amount and type of information companies are allowed to collect and process. Giving more control to users by increasing the number of settings is not a user-friendly approach. The amount of data collection should be limited from the outset.

2.3.9 Data Retention - My Recommendations
Facebook should provide a list of the information that is stored and processed after an account has been deleted. Furthermore, it should clarify the purpose of such usage in more detail. Facebook should add the maximum length of time such information may be stored.
Because Facebook’s definition of personally identifiable information is not adequate for users from the EU, removal of personal identifiers from stored information cannot be seen as adequate enough to protect user identities. Facebook should change its definition of personally identifiable information to a globally acceptable version.

2.3.10 Data Transfer and International Use - My Recommendations

Facebook’s Statement of Rights and Responsibilities should reflect the same information as the Data Policy, if data is in fact transferred to more countries than just the United States. The data transfer information provided is also in need of updating. It should state what methods Facebook is currently using for the transfer of data from the European Union to the United States.
This page has been left blank intentionally.
Twitter

Contents

3.1 Twitter: Introduction

3.2 Twitter: Policy Review

3.3 Twitter: Conclusion
3.1 Twitter: Introduction

3.1.1 Twitter is a social networking platform that ranks second after Facebook in the United Kingdom. [SK-16] It allows users to post messages that can be viewed either publicly or can be kept private between two users or a selected group of users.

3.1.2 Twitter was created by Jack Dorsey, and its co-founders Evan Williams, Biz Stone and Noah Glass, and was first launched in July 2006 only 3 months after its creation. It was Jack Dorsey who came up with the idea of using SMS-type messages (i.e. Short Message Service-type messages, commonly referred to as ‘Text Messages’). Thus, Twitter was developed using a maximum of 140-character posts called ‘Tweets’. The 140-character limit was set because mobile carriers at the time allowed only a maximum of 160 characters per SMS message. 20 characters were used for the username and 140 characters for the post. This allowed users to communicate within only one SMS and prevented messages from being split into several texts. [PR-09] [DS-09] [TW-15-C] [WI-15-A]

3.1.3 As of March 2016, Twitter has approximately 310 million active monthly users (see Figure 3). 79% of which are from accounts outside of the United States. [TW-16-C] [WI-15-A] Twitter has international offices in Amsterdam, Bangalore, Berlin, Bogota, Brussels, Cologne, Dubai, Dublin, Hamburg, Hong Kong, Jakarta, London, Madrid, Melbourne, Mexico City, Milan, Mumbai, New Delhi, Osaka, Paris, Rio de Janeiro, São Paulo, Singapore, Sydney, Seoul, Tokyo, Toronto and Vancouver. [TW-16-C]

![Average Monthly Active Users from 2010 to March 2016](image)

Fig. 3 Average Monthly Active Users from 2010 to March 2016 [ST-16-C] [TW-16-C]

3.1.4 Figure 3 demonstrates the figures of monthly active users from 2010 to March 2016. As is evident, Twitter has recently seen a stall in the growth of total active users. Facebook by comparison is approximately 5 times the size of Twitter at 1.59 billion users, while Twitter has lingered at around the 300 million active monthly users since the beginning of 2015. [MI-16] [LM-16] [ST-16-C] One possibility for this decline is that younger users may be moving away from Twitter, preferring use of Snapchat and Instagram instead. [DS-16]
3.2 Twitter: Policy Review

3.2.1 Twitter’s User Agreement includes the Terms of Service, Privacy Policy and Twitter Rules. This policy review includes the Terms of Service and Privacy Policy only. It does not include the Twitter Rules, as these are not relevant to user privacy issues. The Terms of Service and Privacy Policy reviewed for this paper have an effective date of January 27, 2016 and can be located at twitter.com/tos and twitter.com/privacy. [TW-16-A] [TW-16-B] A more detailed summary of the Terms of Service and Privacy Policy can be found in Appendix C and Appendix D.

3.2.2 By accessing or using Twitter services, the user gives automatic consent to the Terms of Service and Privacy Policy.

3.2.3 Content
Twitter states that use of content posted on Twitter is solely at the user’s own risk. If, for example, a user clicks on a malicious link within a Tweet, Twitter will not be held responsible for any harm done due to clicking on that link. For content submitted by the user, Section 5 of the Terms of Service advises the user that Twitter can “use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute” any content submitted by the user to companies who partner with Twitter. [TW-16-A] Such content only includes information that is deemed ‘public’ by Twitter.

Twitter advises the user on several occasions, both in the Terms of Service and in the Privacy Policy, that information submitted to the Twitter website is ‘public’ by default. As per Twitter’s Privacy Policy “public information includes the messages you Tweet; the metadata provided with Tweets, such as when you Tweeted and the client application you used to Tweet; the language and time zone associated with your account; and the lists you create, people you follow, Tweets you mark as likes or retweet, and many other bits of information that result from your use of the Twitter Services”. [TW-16-B] It does not supply a full list of information deemed ‘public’ by Twitter. The Privacy Policy also advises its users that they “should think carefully about what you are making public”. [TW-16-B] Given the information provided by Twitter, it is apparent that Twitter deems a lot of information ‘public’ by default. This needs to be considered, to understand the possible consequences of Twitter’s data sharing practices.

3.2.4 Data Collection
Twitter collects a wide variety of information. Sources for this information include “various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services (the “Twitter Services”)” and “other third parties”. [TW-16-B] Information collected by Twitter includes the user’s interaction with the site, as well as
their “IP address, browser type, operating system, the referring web page, pages visited, location, mobile carrier, device information (including device and application identifiers), search terms, and cookie information”. [TW-16-B] Every time the user interacts with any Twitter Service, including simply visiting a website that uses a Twitter button or widget, all available information is collected and processed by Twitter. The purpose for the gathering of such detailed information is to provide targeted advertisements, make topic suggestions and personalise the content that is displayed to users.

3.2.5 Location Information
The user’s location information is not made public unless the user chooses to show their location in their Tweets. However, even when the user chooses not to use location information in their Tweets, Twitter does collect location information. This is done using the user’s IP Address, GPS, wireless network, or cell tower information. This information is used to allow Twitter to show the user locally relevant topics and advertisements.

3.2.6 Data Retention
As per the Privacy Policy, the log data collected is either deleted or “any common account identifiers” removed after a maximum of 18 months. [TW-16-B] Such anonymisation of data can be somewhat controversial. Twitter’s policy only states that “account identifiers” will be removed. These would include the username, email address or the full IP address. [TW-16-B] However, the use of data anonymisation may not guarantee that the information left will not identify a user when combined with other available information. In 2014, Kristof van Quathem and Dan Cooper wrote an article for Covington’s Inside Privacy website, named “European Regulators Set Out Data Anonymization Standards” [KQ-14], which addresses several important issues on anonymisation as pointed out by the Article 29 Working Party. The Article 29 Working Party is a group of representatives from the European Commission, the European Data Protection Supervisor and national data protection authorities who advise the commission on data protection matters and promote the use of Directive 95/46/EC. In the article, the Working Party stated that most anonymisation techniques “carry risks” and that data will still be considered personal data if it can somehow be associated with a living individual. [KQ-14] It reads: “According to the Working Party, unless the original data is destroyed, the data controller continues to have the ability to attribute it to the relevant individual, either directly or by inference. The inability of the recipient of the “anonymized” data to do this is irrelevant; the data remains personal data.” [KQ-14] It goes on to clarify that “removing directly identifying elements in itself is not enough to ensure that identification of the data subject is no longer possible. It will often be necessary to take additional measures to prevent identification”. [KQ-14] The Information Commissioner’s office (ICO) is also aware of the risks involved with data anonymisation and thus published guidance on the
subject in the “Anonymisation: managing data protection risk code of practice” issued under Section 51 of the Data Protection Act 1998. [IC-12] It is difficult to anonymise data effectively especially considering that Twitter’s understanding of what should be deemed ‘public’ versus ‘private’ information is already questionable.

When a user decides to delete their Twitter account, the account is at first only deactivated for a grace period of 30 days. This gives the user a chance to reactivate their account in case they change their mind or if the deletion was done accidentally. As soon as a user deactivates the account, it will no longer be available to other Twitter users. After 30 days Twitter will delete the account, which may take up to one week to be completed. Users are advised that any of their information saved by external entities, such as search engines, for example, will still be available online even after the account has been deleted. [TW-16-B] A popular third-party service used to facilitate account deletions, AccountKiller, instills confidence in the actual deletion of information by Twitter by providing a note to users stating, “it seems your info (information) will actually be deleted” (see Figure 4). [AK-A]

3.2.7 **Optional Services**

In the Privacy Policy, users are also advised of the consequences of using optional services such as single-sign on via third-party sites or syncing their address book with their Twitter account in order to find their friends on Twitter. Such actions are purely optional and thus the user is responsible for consequences when using such services.

3.2.8 **Information Sharing and Disclosure**

The Privacy Policy not only encompasses information collection and use, but also the sharing and disclosure of such information. As clearly stated in the policy, Twitter does not disclose private information except as stated within the Privacy Policy. Disclosure of private information may occur if it is deemed necessary in order to comply with a law, regulation, legal process or governmental requests. Twitter may also share personal information with service providers, who may only use such information according to instructions given by Twitter. [TW-16-B] In Twitter’s Transparency report the user will find information about government requests for
account information or content removal, copyright notices, e-mail privacy and trademark policy violation notices. Where applicable the report states whether or not Twitter has taken any action on the received requests. [TW-15-A] Figure 5 depicts an example of government requests received from the United Kingdom from January 2012 to December 2015. It does, however, not list the exact details of the requests. [TW-15-B]

![United Kingdom Information Requests](image)

**United Kingdom**

**Information Requests**

<table>
<thead>
<tr>
<th>REPORT</th>
<th>ACCOUNT INFORMATION REQUESTS</th>
<th>PERCENTAGE WHERE SOME INFORMATION PRODUCED</th>
<th>ACCOUNTS SPECIFIED</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012: Jul 1 - Dec 31</td>
<td>427</td>
<td>71%</td>
<td>556</td>
</tr>
<tr>
<td>2013: Jan 1 - Jun 30</td>
<td>299</td>
<td>39%</td>
<td>1,041</td>
</tr>
<tr>
<td>2014: Jul 1 - Dec 31</td>
<td>116</td>
<td>34%</td>
<td>371</td>
</tr>
<tr>
<td>2015: Jan 1 - Jun 30</td>
<td>78</td>
<td>46%</td>
<td>200</td>
</tr>
<tr>
<td>2016: Jul 1 - Dec 31</td>
<td>55</td>
<td>44%</td>
<td>117</td>
</tr>
<tr>
<td>2017: Jan 1 - Jun 30</td>
<td>26</td>
<td>15%</td>
<td>29</td>
</tr>
<tr>
<td>2018: Jul 1 - Dec 31</td>
<td>25</td>
<td>4%</td>
<td>27</td>
</tr>
<tr>
<td>2019: Jan 1 - Jun 30</td>
<td>11</td>
<td>18%</td>
<td>11</td>
</tr>
</tbody>
</table>

NOTE: The data in these reports is as accurate as possible, but may not be 100% comprehensive. It may be necessary to side-scroll to see all the table columns depending on the screen resolution.

Fig. 5 Twitter Transparency Report United Kingdom [TW-15-B]

3.2.9 Twitter Services and Third Parties

Twitter’s Terms of Service and Privacy Policy apply not only to the Twitter website, but to all Twitter Services. A link to a Twitter Help Center page is provided, where a list of Twitter Services and corporate affiliates is available. [TW-15-D] (Please refer to Appendix C for the detailed list.) Even though Twitter’s corporate affiliates are covered under Twitter’s Privacy Policy, they may have additional terms, which will be supplied by each individual company. [TW-15-D]

Third parties are also mentioned in the Privacy Policy with an explanation that these may include “search engines, developers, and publishers that integrate Twitter content into their services, and institutions such as universities and public health agencies that analyze the information for trends and insights”. [TW-16-B] For example, Twitter also has a partnership and shares publicly viewable information with IBM. Twitter data is used in IBM’s analytics solutions, such as Watson Analytics Plus. [FA-15] [CM-14] A partial list of Twitter mergers and acquisitions can be viewed on Wikipedia. [WI-16-A]

The availability of third-party Twitter analytics websites, such as Followerwonk or Twitonomy, makes it apparent that information is widely shared and easily accessible by such websites. Twitter allows such sites to conduct in-depth analysis of each user account. By comparison, such deep analytics are not possible on other social networks and thus it seems that Twitter more openly shares a wide variety of
information that enables the profiling of Twitter users, including information such as the times the user is most active, associates most tweeted and maps showing their followers' locations. Twitter's information sharing practices are a definite threat to their users' privacy.

3.2.10 Data Transfer and Use

Another area that can lead to confusion is the area of data transfer. The Privacy Policy states that “Irrespective of which country you live in, you authorize us to use your information in, and as a result to transfer it to and store it in, the United States, Ireland, and any other country where we operate. Privacy and data protection laws in some of these countries may vary from the laws in the country where you live”. [TW-16-B] The last sentence was only recently added when the policy was updated on January 27, 2016, perhaps in an effort to clarify that laws applicable depend on the country where the data is stored. Possible countries where user data may be stored, processed and used are not only the United States and Ireland, but also in Australia, Belgium, Brazil, Canada, China, Colombia, France, Germany, India, Indonesia, Italy, Japan, Mexico, Netherlands, Singapore, South Korea, Spain, United Arab Emirates and the United Kingdom. [TW-16-C] It is without question, that the privacy and data protection laws will vary from EU data laws in some of these countries.

Data transfer information is not put into a practical context for Twitter users and is thus hard to understand. However, European individuals are advised to inquire about data protection issues at Twitter’s European headquarters in Ireland.

3.2.11 Legal Jurisdiction

Jurisdictional information provided in the Terms of Service and Privacy Policy is also written in a way that most users will find confusing. In Section 12 of the Terms of Service it is stated that: “Terms and any action related thereto will be governed by the laws of the State of California without regard to or application of its conflict of law provisions or your state or country of residence.” [TW-15-A] Reading such a statement and being unaware of jurisdiction clauses can easily lead the reader to believe that laws in their country of residence may not be applicable. However, users are also advised that if they live outside of the United States, the agreement is made between them and the Twitter International Company located in Dublin, Ireland. To the average user such statements may seem confusing since it first stated that no matter where a user is located only California law applies, only to immediately contradict this by informing users located outside of the U.S. that the agreement is made with Twitter International Company located in Ireland. Information is not presented in a user-friendly manner and does not aim to help users understand what laws apply. Explanatory information is missing that would clarify the meaning of jurisdiction clauses.
3.3 Twitter Conclusion

3.3.1 Overall, Twitter provides users with a lot of guidance. It makes it very clear that by default information submitted to Twitter is public, unless the user controls this in their settings. However, settings are not available for all information and Twitter advises users to be careful when posting information they know to be public. The user will be aware that information is strictly public when no settings option is given for that particular type of information.

Possible problematic areas found in the Terms of Service and Privacy Policy

3.3.2 Public by Default - Possible problematic areas
Users who do not read the Privacy Policy may be unaware that most information submitted to Twitter is public by default. Users are also only given limited options to control their information. Twitter is thus able to freely share a significant amount of information with third parties. It is the social network’s interpretation of what information is considered ‘public’ versus ‘personal’ that poses a threat to user privacy.

3.3.3 Data Collection - Possible problematic areas
Twitter collects, processes and stores a large amount of information about each user. According to Twitter, data will be either deleted or common account identifiers removed after a maximum of 18 months. However, successful data anonymisation is difficult to achieve. Because of the amounts of information gathered as well as Twitter’s interpretation of what constitutes ‘public’ versus ‘personal’ data, available information may still lead to identification of an account or a user when analysed together with other information. Unless done correctly, data anonymisation may be ineffective in protecting users.

3.3.4 Information Sharing - Possible problematic areas
Public information is shared with a wide variety of entities that extent far beyond Twitter. This is made apparent by the effectiveness and in-depth user profiles created by third-party analytics websites, including Twitonomy, Followerwonk, Foller.me, Tweetpaths, Sleeping Time, and Mentionmapp. It is unknown why Twitter chooses to allow such detailed access to user information. When compared to Facebook, Google+ or LinkedIn, Twitter is the only social network that allows such public analytics of user information.

3.3.5 Data Transfer and International Use - Possible problematic areas
From the information provided, the user would not be able to determine where exactly their data is being transferred and if their data will be protected adequately in such locations.
My Recommendations

After analysis of the problematic areas I have determined the following recommendations in order to improve user privacy.

3.3.6 Public by Default - My Recommendations

Too much information is deemed as ‘public’. Twitter should revise what information is considered ‘public’ and should provide a full list of these categories. Third parties should not have access to information that allows them to analyse and publish profiles of Twitter users.

3.3.7 Data Collection - My Recommendations

Twitter collects, processes and stores a large amount of information that is mainly used to supply users with targeted advertisements and to customise their experience on the site. The problem identified was in connection to Twitter’s data anonymisation practices. Because Twitter has weak standards when it comes to designating information as either ‘public’ or ‘private’, data anonymisation must be done thoroughly and correctly in order to provide any protection to Twitter users. Twitter should ensure that the data that remains cannot be used to identify an individual either on its own or in conjunction with other data stored by Twitter.

3.3.8 Information Sharing - My Recommendations

As other social networks do not allow third parties to analyse their users, it would be recommended that Twitter follow suit and also eliminate the excessive accessibility of user information. This would eliminate analysis of user accounts and the open publishing of such information.

3.3.9 Data Transfer and International Use - My Recommendations

It should be made explicitly clear to the user as to where their data is being used and stored. A list of countries where Twitter operates should be included in the Privacy Policy. Twitter should also give assurance that data is being stored and processed using data protection practices that are to a standard appropriate for EU residents.

3.3.10 User-Friendly Policies - My Recommendations

Overall Twitter should ensure that the entire user agreement is user-friendly and easily understood. Currently, some of the information in the Terms of Service is not user-friendly and the average reader may not understand what the information actually means in a practical context.
Google+

Contents

4.1 Google+: Introduction

4.2 Google+: Policy Review

4.3 Google+: Conclusion
4.1 Google+: Introduction

4.1.1 Google+ is a social network that is operated by Google Inc., a subsidiary of Alphabet Incorporated. It originally launched in June 2011, after three failed attempts by Google at launching social networking sites. These attempts included Orkut in 2004 (retired in 2014), Google Friend Connect in 2008 (retired in 2012) and Google Buzz in 2010 (retired in 2011). [WI-15-B]

4.1.2 Since its launch, Google+ has not been performing well. The number of active users remains low. Statistics for the total number of Google+ users are hard to come by. In 2015 the total number of Google+ members was said to be approximately 2.5 billion. [FG-15] Google+ member numbers are high only due to the fact that users automatically end up with a Google+ account because of their existing Gmail account or for use with YouTube. However, the majority of these members do not use their Google+ account. According to Eric Enge of Stone Temple Consulting, it is estimated that only approximately 9.7% of Google+ accounts are actually active. [EE-15]

4.1.3 Even though Google+ most likely should not be listed in the top 5 social networks, the review of its Terms of Service and Privacy Policy is of importance since Google uses the same Terms and Privacy Policy across its range of services.

4.2 Google: Policy Review

4.2.1 This policy review includes Google’s Terms of Service and Privacy Policy. The Terms of Service reviewed for this paper have an effective date of April 14, 2014, while the Privacy Policy’s effective date is as of March 25, 2016. Please see Appendix E and Appendix F for a more detailed summary. Archived versions of the Privacy Policy are available on www.google.com/policies/privacy/archive. [GO-16-C]

4.2.2 Google’s Terms of Service are located at www.google.com/policies/terms. [GO-14-A] Its scope is kept intentionally broad as it includes all services provided by Google and hence is applicable to the services provided by Google+.

4.2.3 The Privacy Policy governs the way information is collected, the reasons for its collection and how the information may be used. It applies to all services offered by Google Inc. and its affiliates. Affiliates include, for example, YouTube and Google services provided on Android devices and on other websites, such as their advertising services. The current version of Google’s Privacy Policy is available at www.google.com/policies/privacy. Older versions are available for viewing at www.google.com/policies/privacy/archive. [GO-16-A]
4.2.4 **Content**

In the Terms of Service, the user is advised that Google may use any content submitted for a variety of purposes. Google reserves the right to “use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content”. [GO-14-A] Even when the user discontinues use of Google services, Google retains the right to use previously submitted content. Both the Terms of Service and Privacy Policy advise users that automatic analysis will be performed on any submitted content. The results are used to customize search results, for advertising purposes and for spam and malware detection.

The Terms of Service and Privacy Policy also advise users that Google reserves the right to include user profile names and profile photos in advertisements. For example, photos submitted to Google+ may be used as background on Google products. Google advises users that they can change their settings if they do not wish their name and photo to appear in advertisements. [GO-16-A] [GO-16-B] Further settings are available to users to control various other aspects of their experience while using Google services. Direct links to additional information are provided. Users are presented with numerous changeable settings including how to control targeted advertising, relevancy of search results, deleting web history and account privacy settings. [GO-16-A]

4.2.5 **Data Collection**

Google collects information from any area it has access to. This includes information submitted by the user as well as information gathered from the use of any of the Google services. Information collected is used for the purpose of improving Google services, customising search results and advertisements, and to improve security. [GO-C] Cookies and other similar technologies, such as Google Analytics and the DoubleClick cookie, are used to gather information. [GO-16-A]

Device Information that is collected while accessing Google services includes operating system information, hardware type/model and settings, unique device identifiers such as an IMEI (International Mobile Equipment Identity) number, phone number and mobile network information, type of browser used and language preferences. Location information is gathered using a variety of sources such as IP address, GPS, Wi-Fi access points and mobile network towers. Location information is also collected from search queries by using locations that the user is showing an interest in. This includes any information that infers the user is either interested in a particular location or might be at that location. [GO-A]
It is important to note that information is collected both while the user is signed in and also when not signed in. Such information can include contacts the user added, calendar events, photos, videos or documents uploaded. [GO-B] Google may associate any information gathered with a user’s Google Account. If collected information is combined with a user’s account it will be designated ‘personal’ information and treated as such under the policy. [GO-16-A] A new feature added to the current Privacy Policy is that users may now opt out of certain customisations done by Google when the user is not signed-in. This means that users can control whether or not they want to allow targeted advertisements and search results that are based on their past search queries.

4.2.6 Data Retention
Within the Privacy Policy users are informed that information deleted from Google services, will not immediately be deleted from all active servers and that it may not be deleted at all from Google’s backup servers. [GO-16-A] The user thus can only assume that Google retains all information indefinitely.

If a user wishes to delete their Google+ account the account will most often only be downgraded. This is due to the fact that the Google+ account is most likely linked to the user’s general Google account since a single Google account can be used for Gmail, YouTube and Google+. As users most likely do not want to lose all accounts, accounts are downgraded rather than deleted. A complete deletion of the main Google account is also available if desired.

When a Google+ member decides to downgrade their account, not all information on their Google+ account will be affected. Any information that is tied to another Google service will remain. For example, no photos will be deleted. Any photos added to the Google+ account will still be available on Picasa. Chat content, as well as Google Local reviews will also still be available. This is due to the fact that such information is connected to other services such as Hangouts, Google Talk or Google Maps. The users would thus have to visit each service individually if they wish to delete the content. Events users have created or replied to will also not be deleted. [GP-16-B] Users must be signed into a Google+ account in order to have access to the above information.

4.2.7 Information Sharing and Disclosure
Google does not share what is deemed ‘personal’ information with anyone outside of Google unless it is with the explicit consent of the user, for account maintenance, for processing provided by Google’s affiliates and other trusted parties or for legal reasons. [GO-16-A] A Transparency Report is available to provide users with further information about governmental requests. The report includes how many requests were received and how many of such requests were honored. In the first half of 2015,
for example, Google received a total of 35,365 requests of which 3146 requests were made in the United Kingdom. [GO-15-A] [GO-15-B]

Information that does not personally identify an individual may be shared with any of Google’s partners such as advertisers and publishers. [GO-16-A]

4.2.8 Google Services and Affiliates

Google does not provide a list of Google services and corporate affiliates. Hence, users will not know exactly with whom their publicly viewable information is shared. Google has acquired many companies over the years. A partial list of Google’s mergers and acquisitions can be viewed at Wikipedia. The list is updated as new information becomes available. [WI-16-B]

4.2.9 Data Transfer and Use

Google does not explicitly mention the transfer of user data in either of their Terms of Service or Privacy Policy. The Privacy Policy advises users that, “Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live”. [GO-16-A] The transferring of data to such servers is not mentioned. The only information found regarding data transfer is outdated and is available using a link provided in the “Compliance and cooperation with regulatory authorities” section of the Privacy Policy. Information on this webpage is dated November 21, 2014 and explains that Google complies with the U.S.-EU Safe Harbour agreement but does not inform the reader that the agreement has been invalidated in October 2015 and what other measures Google is using in the interim. [GO-14-B]

Google also does not provide a full list of data center locations. The list provided by Google only includes locations in Belgium, Finland, Ireland, Netherlands, Singapore, Taiwan and the United States. [GD-A] According to an article by Rich Miller, written for the Data Center Knowledge website in 2012, it was speculated that Google has many other data centers and that such a list would include but not be limited to Belgium, Brazil, Canada, China, France, Germany, Ireland, Italy, Japan, Netherlands, Russia, Switzerland and the United Kingdom. [RM-12] More current information could not be found. Other possible locations may be in countries where Google operates its offices. A list of office locations is available on Google’s Careers page and includes a total of 48 countries around the world. [GC-A] As a result of the limited information provided by Google, there is no way for users to know exactly where their information is stored and processed.
4.2.10 **Legal Jurisdiction**

Similar to the other social networks discussed in this paper, jurisdictional information provided in the Terms of Service is not put into a context that an average reader would understand. The user is notified that the laws of California, United States will apply to any disputes and that jurisdiction is set to the courts of Santa Clara County, California. Google also only supplies the California address as point of contact for all of its users. It does not inform users located outside of the United States whether there exists another point of contact.

4.3 **Google+: Conclusion**

4.3.1 Overall, Google provides information in a user-friendly manner. It advises users, where possible, of settings that can be adjusted and is open about its retention of information. Topics lacking information are data transfers and server locations. Otherwise, a lot of information is available to users to inform themselves about how Google operates and what settings and options are available to control information gathered or publicly viewable. However, the time investment required is substantial and thus it is highly unlikely that most users will read all of the available information.

4.3.2 Google has become the powerful search engine it is today because of its aggressive information collection practices. Information is collected, analysed and associated with a specific user at every possible opportunity.

Possible problematic areas found in the Terms of Service and Privacy Policy

4.3.3 **Public by Default/Content - Possible problematic areas**

Google’s right to use the content submitted by a user continues even when the user discontinues using Google services. Users who do not read the Terms of Service will not be aware of this. Another area they may be unaware of, if they do not read the Terms of Service, is that Google can include user profile names and photos in advertisements. Settings are available to control this, but the information may be displayed to the public for some time before the user realises it and changes the appropriate settings. Google supplies a large amount of information to users, which is however only useful to those who take the time to read it. It is thus left to the users to educate themselves accordingly.

4.3.4 **Data Collection - Possible problematic areas**

Google is a master of gathering and analysing information. Information is collected from any available source. The monitoring of search queries is a definite threat to user privacy as every move made on Google is tracked, analysed and associated to the user’s account whenever possible.
4.3.5 Data Retention - Possible problematic areas
Users wishing to downgrade or delete a Google+ account face more of a challenge than other social network account deletions. This is due to the fact that different components of a Google+ account are hosted by separate Google services and are thus not deleted automatically, but must be deleted by visiting the individual services.

Another problematic area is that the Privacy Policy informs users that, “after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems”. [GO-16-A] This is a clear threat to user privacy, as users who delete their account expect information to be deleted and not for it to be stored indefinitely.

4.3.6 Information Sharing - Possible problematic areas
As with the other social networks reviewed for this paper, Google also informs users that personal information will be shared with its “affiliates or other trusted businesses or persons”. [GO-16-A] However, an exact list of entities is not provided. Google has not only had numerous acquisitions over the years, but also invests heavily in companies such as Uber, for example. Users will not know if such partial ownership would also constitute the sharing of their personal information with such entities.

4.3.7 Data Transfer and International Use - Possible problematic areas
Google+ is the only social network reviewed for this paper that does not explicitly mention the transfer of user data in either of the Terms of Service or Privacy Policy. A link, called “self regulatory frameworks” provided within the “Compliance and cooperation with regulatory authorities” section of the Privacy Policy [GO-16-A], leads to a webpage that has not been updated since November 21, 2014 and provides outdated information about the U.S.-EU Safe Harbour agreement. [GO-14-B] Whereas Google is very thorough in most areas of its Privacy Policy, this area seems to have been subject to a major oversight. Further to this oversight, Google also does not provide a full list of server locations. Overall, Google keeps issues of data transfer and international processing vague.

4.3.8 Legal Jurisdiction - Possible problematic areas
According to Google’s Terms of Service and Privacy Policy it only operates out of one headquarter, which is located in California, United States. It does not inform users of a data controller elsewhere that may be responsible for information of users located outside of the United States.

4.3.9 User-Friendly Language - Possible problematic areas
Throughout the Privacy Policy extra information is provided to readers to explain certain sections of the policy. This is however not done for the Terms of Service.
My Recommendations

After analysis of the problematic areas I have determined the following recommendations in order to improve user privacy.

4.3.10 Data Collection - My Recommendations

Google informs users that it will gather information from any possible source and is well known for its extensive data collection practices. In my opinion, only governmental measures can help to limit the amounts of data organisations are allowed to collect and process. Purposes for data collection must be more specific, so that excessive data collection can be prevented. Currently, very broad categories are used that allow a lot of leeway and thus give too much freedom to organisations in terms of the amount of information collected and methods used.

4.3.11 Data Retention- My Recommendations

Deleting a Google+ account should be made easier. A user should have to consult only one dashboard type webpage that will let them delete content from all components of their Google+ account.

Google also does not state the maximum length of time data is stored for. The fact that Google may never delete information off its backup servers should not be an acceptable practice.

4.3.12 Information Sharing - My Recommendations

An exact list of entities with which information may be shared is not provided to users. Google has had numerous acquisitions over the years. It also invests in numerous companies. Users should be informed whether such investment also results in the sharing of their personal information with such companies.

4.3.13 Data Transfer and International Use - My Recommendations

Google lacks to clearly explain that user data may be transferred to any of their server locations. Compliance to the U.S.-EU Safe Harbour agreement is mentioned, but the information is outdated and does not to list the methods currently used by Google to transfer data. Users should have access to a list of countries to which their data may be transferred.

4.3.14 Jurisdiction - My Recommendations

Google should inform its users on whether there is a data controller for EU residents or make it clearer that the only data controller for worldwide users is located in California, United States.
4.3.15 **User-Friendly Language - My Recommendations**

To make information of a legal nature easier to understand, Google could employ the same methods in the Terms of Service as are already used in the Privacy Policy. Extra information can be added in sections that are likely hard to understand. This would allow Google to continue using wording necessary for legal purposes, but also help the average reader to understand what such information means in a practical context.
This page has been left blank intentionally.
LinkedIn

Contents

5.1 LinkedIn: Introduction

5.2 LinkedIn: Policy Review

5.3 LinkedIn: Conclusion
5.1 LinkedIn: Introduction

5.1.1 LinkedIn is a social network for professionals and companies with emphasis on business and work related topics. Members of LinkedIn post their resume information and a professional looking photograph. As such it is different from Facebook, Twitter and Google+ where individuals share personal posts and photos.

5.1.2 LinkedIn started as an idea of Reid Hoffman, who went on to recruit colleagues Allen Blue, Jean-Luc Vaillant, Eric Ly and Konstantin Guericke. In May 2003, LinkedIn was officially launched. [LI-A] LinkedIn is older than both Twitter, launched in 2006 and Facebook, created in 2004 but also launched in 2006. It generates its revenue by selling user information to recruiters, through advertising and from premium subscriptions. In June 2016, Microsoft announced that it will be acquiring LinkedIn for an estimated $26.2 billion US dollars (approximately £19 billion). [MN-16] [ST-15]

5.1.3 As of April 2016, LinkedIn had a total of 433 million members. However, only 100 million of these are said to be monthly active users. [ST-16-D] In the United Kingdom LinkedIn has approximately 20 million members. [ST-16-B] Currently, LinkedIn ranks fifth in the United Kingdom's top social networks after Facebook, Twitter, Instagram and Google+. [SK-16]

5.2 LinkedIn: Policy Review

5.2.1 This policy review includes the LinkedIn User Agreement and Privacy Policy dated effective as of October 23, 2014. The User Agreement is located at linkedin.com/legal/user-agreement, the Privacy Policy at linkedin.com/legal/privacy-policy. [LI-14-A] [LI-14-B] A LinkedIn account is not required in order to have access to the information. A more detailed summary of the User Agreement and Privacy Policy can be found in Appendix G and Appendix H.

5.2.2 LinkedIn informs its users immediately at the beginning of the User Agreement that users agree to and are entering into a legally binding agreement by “registering, accessing or using” LinkedIn services. [LI-14-A] Such LinkedIn services include “LinkedIn, SlideShare, LinkedIn Pulse, related mobile apps, developer platforms, premium services, or any content or information provided as part of these services”. [LI-14-A] If the user resides in the United States the agreement is with the LinkedIn Corporation. If the user resides outside the United States then the agreement is with LinkedIn Ireland.

5.2.3 Content
Within the User Agreement LinkedIn advises its users that by default, only applying for jobs and using InMail are ‘private’. All other information is ‘public’. If users wish to
control who sees their posted information they can adjust their account settings accordingly. LinkedIn will also expose a user when viewing other LinkedIn profiles. LinkedIn will send members a notification when their profile has been viewed and who has viewed it. Settings are available to remain private while viewing other LinkedIn member profiles.

LinkedIn reserves the right to “use, copy, modify, distribute, publish, and process, information and content” that a user provides to any of its services without notifying or needing further consent from the user. [LI-14-A] Such information includes any feedback or suggestions given to LinkedIn by the user. LinkedIn will, however, obtain the user’s consent before giving third parties the right to publish such content.

5.2.4 **General Data Collection**

Information is collected any time a user interacts with any of the LinkedIn Services or visits a site that uses LinkedIn’s cookies or social plugins. This is the case whether the user is a LinkedIn member or just a visitor. Information collected includes the name, e-mail address, mobile number, location, previous jobs, education and any other information the user chooses to add to their LinkedIn profile. Device information collected includes the IP Address, computer or mobile operating system, web browser used, mobile device identifier and name of the Internet service provider or mobile carrier. Location information may also be collected. Companies used by LinkedIn to gather information include DoubleClick, BlueKai, Lotame, Google Analytics, Quantcast, Nielsen, ComScore and Eloqua. Information collected is used by LinkedIn mainly to serve relevant advertisements and content. LinkedIn gives users the option to opt out of such customised advertisements.

It should be noted that when a user is logged in or identified by one of the LinkedIn cookies, any information collected will be associated with that user’s account and used to customise advertisements and content. This occurs even when the user is not logged in but when a cookie can make a positive identification based on device or other information that is collected and logged.

5.2.5 **Collection of Information from Synching**

An entire section within the Privacy Policy is dedicated to advising users of data collection practices when the user chooses to sync with external content such as their address book, mobile device contacts or calendar. LinkedIn will collect all possible information including e-mail addresses and phone numbers. As per Section 1.4 of the Privacy Policy information collected via syncing is used by LinkedIn to identify the user’s “contacts that are already members of our Services” and for “providing a template to send invitations on your behalf to your contacts that are not Members”. [LI-14-B] Thus, the action of synching will cause the member’s contacts to receive
emails from LinkedIn, unless the user adjusts such options appropriately at the time the syncing takes place.

Users should furthermore be aware that communications initiated via LinkedIn services, such as sending connection invitations to other members, may expose the user’s e-mail address or mobile number as the name and primary email address will be visible in the header of the message. However, a request for an introduction will only list the user’s name but will not include the e-mail address.

In 2013, LinkedIn’s practices of using information collected when a user decides to sync external services has resulted in a class action lawsuit against LinkedIn. Four LinkedIn members accused LinkedIn of accessing their e-mail accounts without their permission and using the contacts in their address books to send e-mail invitations using the members’ names. If LinkedIn received no response it would continue to send two more reminder e-mails. It was these reminder e-mails that caused the problem. The judge in the case agreed that the repeat emails could damage the reputation of the LinkedIn users since to the recipient, it would look like that person not LinkedIn is sending such excessive amounts of invites. The case resulted in a USD $13 million (approximately £9.8 million) settlement in October 2015. [JR-15] [MD-15] [SL-15] As a result of this lawsuit and as part of the settlement, LinkedIn now gives users control of whether invitations will be sent or not. Figure 6 demonstrates the option given to users after they have synced an e-mail account with LinkedIn. It gives users the choice to either allow LinkedIn to send invitations to specific contacts, or to skip invitations entirely. Thus, it is now up to the user to control the invites sent.

![LinkedIn Optional Invitations](image)

**Fig. 6 LinkedIn: Optional invitations after synching**

### 5.2.6 Data Retention

Sections 3.1 and 3.2 of the Privacy Policy address issues of data retention. Section 3.1 states: “If you close your account(s), your information will generally be removed from the Service within 24 hours. We generally delete closed account information and will de-personalize any logs or other backup information through the deletion process within 30 days of account closure, except as noted below.” [LI-14-B] It is not immediately clear that “except as noted below” actually refers to Section 3.2 and not...
to the note at the end of Section 3.1. The note located at the end of Section 3.1 informs users that any information shared with others, or that others may have copied and saved, may still be visible after account deletion. If the user was a member of a group then the content submitted to that group will remain visible, however the user who posted it will be shown as ‘unknown’. It further advises users that information gathered by search engines will be visible until the cache is refreshed. [LI-14-B]

Section 3.2 goes on to explain that LinkedIn will “keep your information for as long as your account is active or as needed”. [LI-14-B] This type of statement is in keeping with LinkedIn’s generally ambiguous approach. Reasons given as to why LinkedIn may keep information even after an account has been closed include providing user services, complying with legal and regulatory obligations, for reporting and trend analysis and for plugin impression data. [LI-14-B] In Section 3.2 the user will be referred back to Section 3.1 in terms of closed account deletion. Because of the way these two sections are written the reader will bounce from Section 3.1 to Section 3.2 and back to Section 3.1. At the end of reading both sections users will most likely believe that their account information will probably not be deleted because the information provided is vague and unclear.

AccountKiller, a popular website often used to facilitate the closing of various online accounts, conveys a warning to users looking for LinkedIn account deletion information. The warning reads: “Your personal info may not be erased after using the deletion link” (see Figure 7). [AK-B] Although, the portion of the User Agreement that is then quoted by AccountKiller is incorrect and does not reflect the current User Agreement, the warning itself conveys the sentiment users are likely to feel after reading Sections 3.1 and 3.2 of the Privacy Policy.

![AccountKiller](https://example.com/accountkiller.png)

**Fig. 7** AccountKiller - How to delete your LinkedIn Account [AK-B]

On another similar website, Justdelete.me, the user is also faced with a warning about LinkedIn account deletion. The warning states: “There are reports that LinkedIn
continues to email people with a closed account. You may need to contact customer services to delete account instead of just closing it” (see Figure 8). [JD-A]

![LinkedIn MEDIUM]

Fig. 8 JustDelete.me LinkedIn account deletion [JD-A]

These popular account deletion websites convey the problems of LinkedIn’s data retention information. The only thing that remains after reading the information provided by LinkedIn is a definite sense of uncertainty.

5.2.7 Information Sharing and Disclosure

According to the Privacy Policy, LinkedIn only shares personal information with third parties with the user’s consent, by user instruction, as required by law, to enforce the User Agreement or as is “reasonably necessary” to provide LinkedIn services. [LI-14-B] It is the vagueness of “reasonably necessary” that provides much flexibility to LinkedIn. According to Section 2.5 of the Privacy Policy, information is shared “across our different Services, among companies in the LinkedIn family”. [LI-14-B] and personal information may be shared “with our affiliates (meaning entities controlled by, controlling or under common control of LinkedIn)”. [LI-14-B] For example, and to put this into a practical context, this would most likely mean that user information will be shared with Microsoft in the near future since Microsoft will own LinkedIn. Users should be aware of this since some may not wish to share their information with Microsoft.

An attempt was made to obtain a list of affiliates and the companies in the LinkedIn Family by contacting LinkedIn directly, to see how LinkedIn would react to such a request. Figure 9 contains the e-mail response received from LinkedIn. The response as stated in Fig. 9 reads:

“Thanks for contacting us. We have received your request for data regarding the LinkedIn Privacy Policy. Unfortunately, we do not have a list that we can currently provide you with, with your informal request for data. LinkedIn will only provide such information pursuant to valid legal process enforceable in the United States. For requests originating outside of the United States, such valid legal process includes a
letter rogatory procedure or process issued under an applicable Treaty for Mutual Legal Assistance in Criminal Matters.”

Fig. 9 Response from ‘LinkedIn Trust and Safety’

As is apparent by the response from LinkedIn, even upon request, obtaining a list of companies that are part of the LinkedIn Family is not easily possible. The user is left with only a partial list of LinkedIn acquisitions that can be found on Wikipedia (https://en.wikipedia.org/wiki/LinkedIn) and includes companies such as Lynda.com, Rapportive, Careerify, Bizo and Connectifier. [WI-15-C]

5.2.8 Data Transfer and Use

Section 2.17 of the Privacy Policy states that information may be transferred and processed outside of the country in which members reside, in locations where LinkedIn, its affiliates or service providers operate. Even when accounting for only LinkedIn office locations, which do not include locations for any affiliates or service providers, user information may possibly be transferred to and processed in Austria, Australia, Brazil, Canada, France, Germany, Holland, India, Ireland, Italy, Japan, China, Singapore, Spain, Sweden, United Arab Emirates, United Kingdom and certainly the United States. [LI-16-C]

Section 4.2 further informs users that LinkedIn operates under the Safe Harbour Agreement. A note is added to update this information. The additional information reads: “Note: The U.S.-EU Safe Harbor Framework is no longer recognized as a legal mechanism to transfer personal data from the EU to the US. LinkedIn Ireland uses other legal mechanisms, including standard contractual clauses.” [LI-14-B] A link is provided to obtain further information, which advises users that LinkedIn will be using contractual clauses for data transfers between the European Union and the United States because of the invalidation of the Safe Harbour Agreement. [LI-16-B] According to the Article 29 Working Party the use of such standard contractual clauses is deemed acceptable as an interim solution. [EC-15-A] The problem here is
not with the provided information, but with fact that new information was added to the policy. Because the updated information must have been added to the Privacy Policy in or after October 2015 when the Safe Harbour agreement was declared invalid, it is peculiar that the date of the Privacy Policy’s last revision remained October 23, 2014. As the change is rather significant in nature, it could not be determined why the policy revision date was not updated at the time the note was added to the policy. Users who may notice this discrepancy may wonder if any other details were also changed or added without advising users and/or updating the policy revision date.

5.2.9 Legal Jurisdiction

Jurisdictional information provided in the User Agreement is not presented in a user-friendly manner. Most readers would not have knowledge of jurisdiction clauses and thus would not understand what the section is about. LinkedIn designates the state courts of Santa Clara County, California, U.S. for any legal proceedings. If users outside of the United States wish to present a legal dispute to LinkedIn, this should be addressed to LinkedIn Ireland in Dublin. [LI-14-A]

5.2.10 Right to Access Information

The right to request the personal information held by LinkedIn is presented to users in Section 3.1 of the Privacy Policy. It states, “You can request your personal information that is not viewable on your profile or readily accessible to you (for example, your IP access logs) through LinkedIn’s Help Center.” [LI-14-B] LinkedIn Help further advises users of what information is available to them. [LI-16-D] Available information includes but is not limited to:

- Date and time the account was created, closed or reopened.
- Ads clicked on.
- Ad targeting criteria.
- Certifications submitted by the user for their LinkedIn profile.
- Comments made by the user including the date the comments were made.
- All LinkedIn Connections.
- Imported contacts.
- E-mail addresses currently or previously associated with the account.
- All endorsements and recommendations.
- All messages including those in the trash and sent folder.
- Phone numbers associated with the account.
- Photos submitted to LinkedIn.
- A list of recent searches conducted on LinkedIn. [LI-16-D]

5.2.11 Security of LinkedIn based Communications

At the end of the Privacy Policy LinkedIn advises its users that communications made via LinkedIn services are not encrypted and hence users should not use such means to communicate confidential information. [LI-14-B]
5.3 LinkedIn: Conclusion

5.3.1 Generally speaking LinkedIn’s tendency is towards using vague and ambiguous language within its Privacy Policy. This leaves the reader unsure and with a feeling of not having much control over what LinkedIn does with their account information.

Possible problematic areas found in the User Agreement and Privacy Policy

5.3.2 Public by Default - Possible problematic areas
As per the User Agreement, by default only applying for jobs and using InMail are ‘private’. All other information is ‘public’. LinkedIn will also notify members when someone has viewed their profile. Users who are not aware of this may for a time expose their information publicly before adjusting their settings accordingly.

5.3.3 Data Collection - Possible problematic areas
LinkedIn collects information from any user, whether a member or not, who interacts with any of the LinkedIn Services or visits websites that use LinkedIn’s cookies or social plugins. A problematic area here is the fact that LinkedIn will associate information collected with a user’s account even when the user is not logged in, but is positively identified by one of LinkedIn’s cookies. An uninformed user may deliberately choose not to log in, thinking that any pages viewed will not be associated with their account. This may be due to a concern of connecting specific topics or interests with their account. A failure to clearly notify users of such data collection and associating practices will result in connecting the browsing habits the individual wished to remain private to their LinkedIn account.

5.3.4 Data Retention - Possible problematic areas
When it comes to information about data retention LinkedIn uses vague and ambiguous wording that is not easily understood by the average reader. Users are given no certainty that their account information will actually be deleted.

5.3.5 Information Sharing - Possible problematic areas
As with other social media sites LinkedIn users will not know the full extent of with whom their information is shared. It is ultimately up to LinkedIn to decide with whom it chooses to share its users’ information. Even upon request, LinkedIn refuses to provide a full list of the companies in the LinkedIn family.

5.3.6 Legal Jurisdiction - Possible problematic areas
The information provided by LinkedIn in its User Agreement is not presented in a way that ensures that all readers will understand its meaning in practice.
5.3.7 **Data Transfer and International Use - Possible problematic areas**

User information may be transferred and processed anywhere LinkedIn, its affiliates or service providers operate. A list of all possible locations is not provided. Even upon request, LinkedIn does not supply a list of its affiliates and therefore such entities and their locations remain unknown.

5.3.8 **Revision Date - Possible problematic areas**

Because LinkedIn added a note about the Safe Harbour agreement in late 2015 and the date of the current version of the Privacy Policy remained at October 23, 2014, this oversight may breed suspicion in users’ minds. The user can no longer be confident or trust LinkedIn that no other changes were made to the same document.

5.3.9 Overall, LinkedIn’s overriding problem is poor communication. Wording is vague and ambiguous. Changes are made to the Privacy Policy without notifying users either by direct notification or by at least updating the revision date of the document.

**My Recommendations**

After analysis of the problematic areas I have determined the following recommendations in order to improve user privacy.

5.3.10 **Public by Default - My Recommendations**

At the time of registration users should be made aware of the type of information that will be ‘public’ by default, and that their identity will be exposed when viewing other members’ profiles. A short message should be displayed as soon as the account has been established. This will better protect user privacy, even when users choose not to read the User Agreement or Privacy Policy.

5.3.11 **Data Collection - My Recommendations**

Because LinkedIn uses numerous and varied methods to collect information, it is able to identify a user even when the user is not logged in. It can thus associate any information gathered with the user’s LinkedIn account. This practice should be determined as excessive data collection by legislation and should be disallowed in order to allow users to retain some privacy while browsing the Internet when not logged into social network accounts.

5.3.12 **Data Retention - My Recommendations**

The main problem with the information provided by LinkedIn about its data retention is that the language used is vague. It is not made clear what actually happens to user information. LinkedIn should be forced to state clearly and understandably whether they do or do not delete account information and provide a maximum period of time information is retained.
5.3.13 Information Sharing - My Recommendations

As seems to be standard practice amongst the social networks reviewed for this paper, social network users will most likely never know with whom their information is shared. Currently companies are not forthcoming enough. When a user requests a full list of companies with whom personal information is shared, such a list should be made available without question since knowledge of this may affect the user’s agreement or disagreement with the User Agreement and Privacy Policy. Appropriate legislation is needed to force companies to comply with such user requests.

5.3.14 Legal Jurisdiction - My Recommendations

Additional information is required especially for readers who reside outside of the United States in order for everyone to be able to understand the meaning of the information provided by LinkedIn about legal jurisdiction. A few explanatory sentences would suffice to explain what the information is about.

5.3.15 Data Transfer and International Use - My Recommendations

Since user information may be transferred and processed in various countries, LinkedIn should inform its users of all possible locations where data may be transferred. This will allow users to make a decision if such transfer is acceptable to them.

5.3.16 Revision Date - My Recommendations

The addition of a note or any editing done to the Privacy Policy should constitute a change to the revision date of the document so that users know that changes have been made.
This page has been left blank intentionally.
Relevant Legislation

Contents

6.1 Relevant Legislation: Introduction

6.2 Data Protection Legislation

6.3 General Data Protection Regulation (EU) 2016/679

6.4 EU-U.S. Privacy Shield

6.5 Relevant Legislation: Conclusion
6.1 Relevant Legislation: Introduction

6.1.1 There are several relevant pieces of legislation that are of importance to safeguarding user privacy in relation to social networks. These are the U.K. Data Protection Act 1998 [SH-08], the Irish Data Protection Act 1988/2003 [DP-09], the Directive 95/46/EC [SH-08] and the recently adopted General Data Protection Regulation 2016/679 [EL-16] and EU-U.S. Privacy Shield [EC-16-B].

6.1.2 Legislation attempts to monitor, control and enforce the way organisations collect and process data, while still allowing data to be shared as freely as possible in the interest of commerce.

6.2 Data Protection Legislation

6.2.1 In the United Kingdom the Data Protection Act 1998 applies to the processing of personal data. However, before the General Data Protection Regulation (GDPR) came into effect and in accordance with Directive 95/46/EC, the data protection law that is applicable to European users is that of Ireland where most social networks have their European headquarters. Facebook, Twitter and LinkedIn list designated data controllers in Ireland and as such come under Irish data protection law, namely the Data Protection Act 1988 and Data Protection (Amendment) Act 2003. Google solely lists California, United States as its headquarter location and point of contact for all of its users. Hence, it is unclear exactly what data protection law applies to user information of EU residents.

6.2.2 The Irish Data Protection Act 1988/2003 is very similar to the U.K. Data Protection Act 1998. [DP-09] [SH-08] As such, it is not a difference in the terms within the act but in the interpretation and enforcement of such terms that distinguishes Irish data protection from U.K. data protection. It is the lack of enforcement that has drawn criticism of Ireland's data protection in the past. Companies are less likely to incur penalties in Ireland than they would in other European Union member states. The 2015 Financial Times article, "U.S. tech groups spawn a fight between Europe’s data regulators", by Duncan Robinson and Murad Ahmed, reiterates Ireland’s forgiving attitude and complains that the Irish Data Protection Commissioner provides guidance rather than enforcements to such companies. [DR-15] It is hoped that a common framework, namely the General Data Protection Regulation, will alleviate this problem when it is fully implemented in 2018.
6.3 General Data Protection Regulation (EU) 2016/679

6.3.1 Regulation (EU) 2016/679, known as the General Data Protection Regulation (GDPR), has been adopted as of April 27, 2016 and replaces Directive 95/46/EC. It will come into full effect on May 25, 2018 to give organisations sufficient time to make the necessary adjustments in order to comply with its requirements. A copy of both the GDPR and the Directive can be located on the EUR-Lex website. [EL-16] [EL-95] Note: For the purpose of this chapter the term ‘data subject’ will be used instead of or along with the term ‘user’. Data subject, as defined by the GDPR is “an identified or identifiable natural person”. [EL-16]

6.3.2 The GDPR is meant to improve the outdated Directive 95/46/EC, which at the time of its development could not account for the significant increase in the collection and processing of personal data that is apparent today. Added to this is the fact that, over the years, users have made more of their personal information available on the Internet but yet expect a high degree of privacy. This poses a challenge on a worldwide level, as information is no longer contained within users’ immediate area but is internationally accessible. The purpose of the Directive and GDPR is to protect individuals’ personal data in terms of the processing of such data and to allow for the free movement of personal data between European Union member states. Because Directive 95/46/EC is not a regulation, there has been a lack of consistent compliance with the Directive due to differences in the interpretation and implementation of the Directive. The GDPR is a ‘regulation’ and hence legally enforceable in all European Union member states. It is hoped that this should provide consistency across member states.

6.3.3 A comparison was made of Directive 95/46/EC and the GDPR. Even though only areas of notable change have been included in the comparison table to minimise the length of the final table, the table that resulted was too long to include within this chapter. Thus, the comparison table is available in Appendix I. As is apparent from the comparison, there are several areas of particular importance to users of social networks that have been added or revised in the GDPR. These are briefly discussed in Sections 6.3.4 to 6.3.11.

6.3.4 **Definition Changes/Additions include:**
(Full definitions of the listed terms are available in Appendix I.)

**Personal Data** - ‘Genetic’ factors and ‘identifiers’ were added, including location data and online identifiers. Social networks must now be aware that such information is deemed as personal data, which may affect the collection, storage and processing practices of such information.
**Processing** - The definition now includes both operations performed upon personal data, as well as on ‘sets of personal data’. ‘Structuring’ of data was added as one of the possible operations performed on such data and the operation of ‘restriction’ replaced ‘blocking’.

**Consent** - The term ‘unambiguous’ was added. As such consent now means, “any freely given, specific, informed and unambiguous indication of the data subject's wishes”. [EL-16]

**Profiling** - The term ‘profiling’ is a new addition. It has been defined as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”. [EL-16]

### 6.3.5 Territorial Scope

A significant change in the GDPR is that the regulation now also applies to data controllers who are not located within the European Union but who offer goods or services to or monitor the behaviour of data subjects residing in the European Union. This was not the case with Directive 95/46/EC, where only the applicable national law of the member state, that the data controller was located in or where the controller made use of data processing equipment, applied.

### 6.3.6 Notifications by the Data Controller to the Data Subject

Under the GDPR the data controller must now provide more information to data subjects about the personal data collected. New additions of categories, which must also be included in such notifications, are:

- Intention to transfer personal data as well as “the existence or absence of an adequacy decision by the Commission” or information about safeguards used for the data transfer. [EL-16]
- Data retention information.
- Rights of the data subject to withdraw consent or make complaints.
- Automated decision-making, including profiling and the logic behind their use.
- Informing the data subject whether providing personal data is a necessary requirement and consequences if the data subject fails to supply the data.

The GDPR also imposes upon data controllers that the information provided must be easily accessible, concise and in clear and plain language that is easy to understand. Ambiguous language, as is used by LinkedIn currently, would thus be contrary to the GDPR. This is a significant change that improves overall transparency. Data controllers will be held to a higher level of accountability to data subjects.
6.3.7 **Special Categories of Personal Data**

Special categories of personal data now include the additional categories of genetic data, biometric data and data concerning a person’s sexual orientation. The need for explicit consent to process such information remains the same as in Directive 95/46/EC. [EL-95] This area will be of concern to Facebook who uses facial recognition technology and has been collecting such data to enable easy tagging of friends in photos. This will now only be possible if the user gives Facebook explicit consent to process such data.

6.3.8 **Consent**

‘Consent’ in most cases is still sufficient to be ‘unambiguous’ and not ‘explicitly’ given. Consent includes ‘conduct’ which demonstrates the data subject’s agreement. This covers the way most social networks operate, as use of their services automatically demonstrates agreement to their terms and policies.

Consent is a difficult area. If it were required to be ‘explicit’, it would make use of the Internet into a tick-box heavy environment that would severely hinder the enjoyment of its use. Thus, a certain flexibility is required and reasonable. Users must take responsibility for the protection of their personal data by being proactive and reading available user agreements and policies. Using ‘explicit’ consent alone would not provide a better level of protection and is not practical.

6.3.9 **Pseudonymisation**

The use of anonymisation of personal data is encouraged in the GDPR and anonymous information is exempt from data protection principles. However, the data controller must be certain that such information cannot identify a person with the use of additional information. If this is or may be the case, the exemption will not apply. It is the responsibility of the data controller to ensure that any additional information that could be used to identify a person is kept separate and secure.

Practices to protect data subjects using pseudonymisation have been questionable in the past. In a paper outlining their position on the regulation, European Digital Rights (EDRi) voiced their concern about the use of anonymisation: “In EDRi’s opinion the new regulation should account for the challenge of achieving true anonymisation of data in the context of all available identification techniques and the prevalence of databases that enable crosschecks and re-identification of seemingly anonymous data.” [ED-16] Encouraging use of pseudonymisation by exempting such anonymous information from data protection principles makes data management easier for organisations but is a gamble for individuals whose personal data is being stored.
6.3.10 **Data Transfer**
Various options are presented to organisations for the acceptable transfer of personal data. By presenting these diverse options, the regulation clearly supports and aims to facilitate the free flow of information.

6.3.11 **Profiling**
According to the regulation, data subjects must now be informed of the existence of automated processing, including profiling. Recital 24 states that processing of data is considered ‘monitoring’ when a person is “tracked on the Internet” and “particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes”. [EL-16] Recital 70 continues to state that a data subject has the right to object to profiling used for direct marketing. The protection from profiling practices is important. Such practices not only determine the kind of advertisements shown to users, but also enable the existence of websites, such as Twitter analytics websites, that profile Twitter users and make such information publicly available.

6.3.12 Overall, the most important change that affects social network users is the territorial scope. Other important areas of the GDPR that will affect social networks are the changes and additions to definitions, the inclusion of identifiers as personal data, the notifications a data controller must provide to users and that such notifications must be easily accessibly and easy to understand. When it comes to profiling, the GDPR has taken an important step by including this practice and giving the user the right to object to such processing. Whether the new regulation increases user privacy remains to be seen. Social networks can easily built relevant information into their policies to which users will very likely consent. However, the user will have more rights in terms of control over their personal data. Users who read the policies will have a better understanding of how their data is used and for how long it may be stored. Because organisations will be forced to give the user much more detailed information, they are more likely to be held accountable by users who will be better educated and more aware of their rights.
6.4 EU-U.S. Privacy Shield

6.4.1 Prior to October 2015 the U.S.-EU Safe Harbour Framework was used to facilitate data transfers from the European Union to the United States. However, the Edward Snowden revelations exposed the inadequacy of the agreement and prompted the case of Maximillian Schrems v. Data Protection Commissioner (Case C-362/14), which ultimately resulted in the agreement’s invalidation on October 6, 2015.

The main concern of Max Schrems that prompted his actions, was the information disclosure and mass surveillance conducted by the U.S. government on European user data. [GC-16] However, unless U.S. laws are changed the new Privacy Shield will have limited if any effect on such practices. In the interim social networks have been using contractual clauses which, according to Max Schrems, should also be disallowed if the Safe Harbour Framework was found insufficient. [DR-16] Whether the use of contractual clauses remains acceptable is currently being investigated.

On July 12, 2016, the European Commission adopted the new EU-U.S. Privacy Shield, replacing the invalidated Safe Harbour agreement. [EC-16-B] Until the GDPR goes into effect the Privacy Shield will operate under the requirements of Directive 95/46/EC. The Commission will assess and make necessary adjustments to the Privacy Shield once the GDPR is in effect. It is planned that the Privacy Shield will be in effect for one year at which time its effectiveness will be analysed at the first annual review. Starting on August 1, 2016, companies will be able to self-certify as compliant with the EU-U.S. Privacy Shield. Such certification will need to be renewed annually. [EC-16-B] [EC-16-D] The new EU-U.S. Privacy Shield reveals several notable changes from the Safe Harbour agreement listed below in Sections 6.4.2 to 6.4.5.

6.4.2 More accountability to comply
Companies will be held accountable and will be monitored for compliance with the new Privacy Shield. Those wishing to transfer data onward, after it has been transferred to the U.S., will have to abide by stricter rules for such onward transfers and will remain liable if recipients of such data fail to comply. The U.S. Department of Commerce will enforce Privacy Shield commitments made by companies. [EC-16-A]

6.4.3 Assurance in regard to U.S. government access
When it comes to issues of the alleged mass surveillance conducted by the United States government, a letter from Robert Litt, second General Counsel of the Office of the Director of National Intelligence, to the U.S. Department of Commerce and the International Trade Administration explains the way the United States government conducts surveillance and attempts to provide assurance to the Commission that mass surveillance is only being conducted in a controlled and, whenever possible,
focused manner. The letter provides information on surveillance practices and applicable U.S. laws that govern such practices. It states that signals intelligence activities are conducted only for “legitimate and authorized national security purposes” and that the Presidential Policy Directive 28 (PPD-28) of 2014 dictates that “collection be as tailored as feasible and that signals intelligence collected in bulk can only be used for specific enumerated purposes”. [EC-16-A] Information provided in regard to the PPD-28 confirms that the U.S. government “must collect bulk signals intelligence in certain circumstances in order to identify new or emerging threats and other vital national security information that is often hidden within the large and complex system of modern global communications”. [EC-16-A] Data collected using signals intelligence activities may be retained for up to 5 years. The information provided by Robert Litt thus confirms the existence of ‘bulk’ surveillance and that analytics are used to scan for specific topics or areas of interest. Data or the inclusion of specific topics in signals intelligence surveillance can be requested only if such a request complies with the Foreign Intelligence Surveillance Act. However, this act merely restates that surveillance should be as targeted as possible, if feasible.

Overall, the letter only assures the reader of the fact that mass surveillance does in fact occur under certain circumstances, but that it is preferably focused and targeted. Hence, the Privacy Shield does not give assurance to EU residents that the U.S. will not conduct surveillance on data transferred to social network servers located in the United States. It fails to have much of an impact on the original concerns that ultimately resulted in the invalidation of the Safe Harbour agreement. The Article 29 Working Party also stated its disappointment at the “lack of concrete assurances” in the document titled Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield. [EC-16-C]

6.4.4 Ombudsperson mechanism
An ombudsperson will be appointed as the point of contact for EU authorities in regard to signals intelligence gathering. EU residents will have to address concerns to their local authorities first, who will then contact the ombudsperson. Catherine Novelli, the Under Secretary of State, has been designated as the ombudsperson and will report directly to John Kerry, the Secretary of State. [EC-16-A] Of concern is that the ‘independent’ ombudsperson is very much a part of the Department of State and is considered ‘independent’ simply because she is not part of the national intelligence services. In the article, “Data regulators reject EU-US Privacy Shield safe harbour deal”, by Samuel Gibbs for the Guardian, the Article 29 Working Party has also voiced concerns over the lack of independence of the appointed ombudsperson. [SG-16]

6.4.5 Annual Review
The Commission together with the U.S. Department of Commerce will review how well the Privacy Shield is functioning on an annual basis.
6.4.6 Overall, the EU-U.S. Privacy Shield is still riddled with significant problems. The main of which are the limited assurance provided by the U.S. government in regard to their surveillance practices and the questionable independence of the ombudsperson appointed to handle disputes. However, a benefit of the new Privacy Shield is in the area of onward transfer of personal information where it will provide better data protection than previously provided under the Safe Harbour Agreement. It also provides European individuals with better ways of submitting potential disputes with either the individual companies or with the U.S. intelligence gathering practices and the use of personal data accessed via these practices.

In Max Schrems’ opinion, as stated to Fortune magazine, the “Privacy Shield does not ensure that Europeans’ personal data will only be processed for narrowly defined purposes, as EU law requires”. [DM-16] It is likely that the Privacy Shield will eventually be challenged since the issues that resulted in the invalidation of the Safe Harbour agreement are not yet addressed sufficiently enough.

6.5 Relevant Legislation: Conclusion

6.5.1 Legislation aims to find a compromise between the protection of personal data and the free flow of information for commercial purposes. As such, protection of personal data will remain largely the responsibility of social network users who must take responsibility for the information they choose to share on the Internet.

6.5.2 The main benefit of the current and forthcoming pieces of legislation is that social networks will have to give users more detailed and easier to understand information on how and why data is collected, processed and stored. However, it is very likely that much of the new requirements will be built into social network policies and will thus be a part of the consent given by social network users. Those having used social networks for a long period of time are unlikely to delete accounts due to such additions to the policies.

6.5.3 Overall, the GDPR may therefore only have a limited effect on user privacy but will force social networks to provide more information to users, who will ultimately be responsible for deciding whether the collection, processing and storage of their data is acceptable to them or whether they will discontinue using such services. The data transfer issues addressed by both the GDPR and EU-U.S. Privacy Shield will not, as they stand currently, be able to control access to European users’ personal data by foreign governments such as the United States.
Conclusion

User privacy on social networks is a complex issue that is interwoven with revenue driven commercial aspects. Data collection and its analysis is now at a massive scale, allowing social networks and search engines to build comprehensive profiles of the individuals using their services. Emerging technology will continue to make data collection methods more aggressive and effective. These new technologies pose an ever-increasing challenge to user privacy, which nowadays extends far beyond information that is shared on social networks. Data is collected from all over the Internet, using information gathered from search engine queries, cookies and other similar technologies. Any such information collected could then potentially be associated with the user’s social network account. Whether the entertainment value of social networks will override a person’s need for privacy remains to be seen.

The main concerns to user privacy found when reviewing the policies of Facebook, Twitter, Google+ (Google) and LinkedIn were similar for each network. Table 2 summarises the main issues encountered for each social network reviewed.

<table>
<thead>
<tr>
<th></th>
<th>Facebook</th>
<th>Twitter</th>
<th>Google+</th>
<th>LinkedIn</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content</strong></td>
<td>Public by default.</td>
<td>Public by default. Twitter labels the majority of information ‘public’, including Tweet metadata.</td>
<td>Public by default. Information submitted may be stored indefinitely even when a user discontinues using Google services.</td>
<td>Public by default. Information collected may be associated with a user’s account, even when the user is not logged on, when LinkedIn can positively identify the user by other means.</td>
</tr>
<tr>
<td><strong>Data Collection</strong></td>
<td>Excessive - New technologies and features, disguised as user experience enhancing additions, are in fact developed to gather more and more information.</td>
<td>Excessive. All accessible information is collected using various sources and methods.</td>
<td>Excessive. All accessible data is analysed and may be associated with a particular user if that user can be positively identified.</td>
<td>Users will not know with exactly whom their information is shared. Even upon request, LinkedIn does not supply a list.</td>
</tr>
<tr>
<td><strong>Information Sharing &amp; Disclosure</strong></td>
<td>Weak definition of ‘personal data’ brings uncertainty as to what information is being shared.</td>
<td>Information deemed ‘public’ by Twitter is shared with third parties allowing them to analyse and profile Twitter users.</td>
<td>Data is shared with Google affiliates and other trusted partners. Unclear how far reaching the sharing practices are.</td>
<td>LinkedIn uses vague and ambiguous wording. User will be unable to determine LinkedIn’s exact data retention practices.</td>
</tr>
<tr>
<td><strong>Data Retention</strong></td>
<td>Unclear. Does not state maximum period of time user data is possibly stored for.</td>
<td>Gives no reason to its users for why continued storage is necessary.</td>
<td>May not remove information from their backup systems. No time limits given for data retention. Deleting Google+ account is difficult.</td>
<td>LinkedIn uses vague and ambiguous wording. User will be unable to determine LinkedIn’s exact data retention practices.</td>
</tr>
</tbody>
</table>
Table 2 Main problems encountered in Facebook, Twitter, Google+ and LinkedIn

As is evident, similar problems were found in all four social networks. Hence, the recommendations I was able to make can be summarised for the reviewed social networks as follows:

**Content**
Generally, content is ‘public’ by default until the user changes available privacy settings. The user should be warned of this fact when signing up for a social network account, without having to read the policies. As was seen with Twitter, too much information seems to be defined as ‘public’ information and thus shared with third parties. In Twitter’s case this allows for extensive analysis and profiling of its users.

**Data Collection**
Data collection is a difficult issue. Governments continue to allow extensive data collection. The amount of data collection should be limited from the outset. Data collection, for the purpose of gaining revenue through advertisements, is a practice that results in a clear threat to user privacy. Without government support in this matter, users will only be able to stop or minimise such practice by boycotting use of social networks or by aggressively refusing targeted advertising.

**Information Sharing**
The main problem seen in information sharing is the definition that is used by social networks for what constitutes ‘personal data’. Facebook’s weak definition of what ‘personal data’ is enables the social network to share information that users may not assume is being shared. Twitter also uses its own interpretation of what is deemed ‘public’ versus ‘personal’ information, which thus enables the profiling of European users and exposure of such information on a global level. The definition used for ‘personal data’ or, as is the case for United States companies, ‘personally identifiable information’ should be the same across all social networks.

Information is also shared with numerous unknown entities. Upon user request, users should be entitled to obtain a detailed list of what type of information is shared with what
entities. Organisations should not be able to refuse such a request since such entities are a part of the privacy policy agreement made with the user.

**Data Retention**

Some user information is being stored and processed even after the user requests account deletion. It is not clear exactly what information is kept and why. User-friendliness is lacking when it comes to information provided to users on data retention practices. This was seen in all four social networks. LinkedIn was the worst offender in this regard, using highly vague and ambiguous wording. Deletion of an account should mean the complete deletion of all user information. Account deletion should also be made easier and less complex.

Thanks to the General Data Protection Regulation, the maximum retention time must now be clearly indicated. Therefore social networks will need to incorporate this information within the next two years.

**Data Transfer**

Users should be entitled to clear and concise information as to where their data is transferred and processed. A list of locations, or at the very least of the countries, should be available to users. It should also be made clear to users, that governments of the listed countries may be able to gain access to user information. The newly adopted EU-U.S. Privacy shield was shown to still present significant inadequacies in terms of data transfer to the United States. However, onward transfer practices have been enforced and will provide better data protection than previously in the U.S.-EU Safe Harbour agreement. Organisation will be responsible for assuring the same level of data protection is provided in all locations the data is transferred to.

**Information provided to Users**

In an odd move Google fails to provide European users with a point of contact within Europe. It solely provides details for its headquarters located in California, United States. Another odd move is made by LinkedIn, which made changes to their Privacy Policy without changing the revision date of the policy. Users will not be aware that a change was made. This causes users to continue use of LinkedIn services under a new agreement without being notified or aware that terms have changed. Such a practice should not be allowed.

Most of the recommendations I presented are based on providing more information to users, who are then responsible for deciding whether they still wish to use the service or not. It comes as no surprise that this is also the area recognised by the GDPR, which now aims to increase the amount and quality of information provided to users. However, the GDPR fails to include information that should also be made accessible, such as a detailed list of entities with whom user information is shared and a list of all locations where data is transferred and processed. At the very least such information should be made available to users upon
request. Without legally enforcing the right to request such information, organisations are not likely to cooperate.

Current and new pieces of legislation aim to balance both user privacy and the commercial flow of information. However, privacy and commercial aspects are in direct conflict. Thus, legislation will never be the sole answer. It simply does its best to keep both sides as happy as possible, with it being apparent that commercial aspects are favoured over providing increased user privacy.

The way social networks operate will only change based on either user pressure or governmental pressures, as otherwise the overwriting drive will continue to be the drive to maximise revenue. Because of this, the sharing of user information will continue to be an important part of their business operation. As so aptly written by Matthew Bailey in the book Complete Guide to Internet Privacy, Anonymity & Security: “If an Internet service is free, you are not the customer, you are the product”. [MB-15] Users must not forget that social networks need them to survive. If users wish to reform how social networks collect and use their information, boycotting the service would most likely be the best approach in order to force change. Another possible option would be to establish social networks that operate on a paid-for membership basis. This would eliminate the need for user data collection for revenue generation, as well as the nuisance to users of excessive advertisements.

User privacy is in a constant battle with commercial profits. If users accept any and all policies provided to them by social networks, such companies will continue to use this lack of involvement to their benefit. Social networks are aware that the majority of their users will never read the provided policies. Ultimately, user privacy is in the hands of the users. It is time users take responsibility for their activities on the Internet and the lack of interest in policies. Just because the Internet is accessed from the comfort of our homes and/or privately owned devices does not mean that the Internet itself is a private place. The Internet is a public place. To expect a high degree of privacy is simply unreasonable.
Bibliography


[ED-16] EDRi, Position on the Regulation 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), 2016, https://edri.org/files/1012EDRi_full_position.pdf, [Accessed on June 20 2016]


Bibliography continued


[FB-A] Facebook Privacy Basics, Facebook’s mission is to make the world more open and connected, https://www.facebook.com/about/basics, [Accessed on June 13 2016]


Bibliography continued


Bibliography continued


Bibliography continued


Bibliography continued


Bibliography continued


Appendices

Contents

Appendix A - Facebook: Statement of Rights and Responsibilities Summary

Appendix B - Facebook: Data Policy Summary

Appendix C - Twitter: Terms of Service Summary

Appendix D - Twitter: Privacy Policy Summary

Appendix E - Google: Terms of Service Summary

Appendix F - Google: Privacy Policy Summary

Appendix G - LinkedIn: User Agreement Summary

Appendix H - LinkedIn: Privacy Policy Summary

Appendix I - Comparison of GDPR (EU) 2016/679 and Directive 95/46/EC
This page has been left blank intentionally.
APPENDIX A

Facebook: Statement of Rights and Responsibilities
Summary

Facebook’s Statement of Rights and Responsibilities can be located at https://www.facebook.com/terms. A Facebook account is not required in order to view it. The version reviewed for this paper has the effective date of January 30, 2015. [FB-15-A] The Statement of Rights and Responsibilities is based on the ten Facebook Principles and governs all Facebook Services, including all Facebook branded and co-branded websites, social plugins such as the Facebook ‘Like’ button and other media, software, products and services. The ten Facebook Principles, available at www.facebook.com/principles.php, are:

1. Freedom to Share and Connect
2. Ownership and Control of Information
3. Free Flow of Information
4. Fundamental Equality for all People using Facebook
5. Social Value (Freedom to build trust and reputation)
6. Open Platforms and Standards
7. Fundamental Service (Free to use)
8. Common Welfare
9. Transparent Process
10. One World (World-wide availability) [FB-16-A]

The user automatically agrees to the terms by using or accessing Facebook Services. No explicit consent is required. Sections relevant specifically to user privacy concerns are:

**Section 1: Privacy** - The user is encouraged to read the Facebook Data Policy, which will advise users of how Facebook collects and uses content and information.

**Section 2: Sharing Your Content and Information** - Users are advised that content and information submitted can be controlled using available settings. Facebook has the right to “use, run, copy, publicly perform or display, distribute, modify, translate, and create derivative works of” any content submitted until the user deletes such content or the account. [FB-15-A] This excludes any content that was shared with other Facebook users, which would still be available on Facebook even after the owner of such content has chosen to delete it. Facebook may use user feedback that was directly submitted, without compensation to the user who submitted it. Any applications used on Facebook will ask for their own permission from the user. It is thus up to the user to either allow or deny access to their information by such applications. Content set to ‘public’ will be available not only to all Facebook members but also to those visiting Facebook.

**Section 3: Safety** - Facebook cannot guarantee that using Facebook is safe. This includes
any possible malicious code, harassment of users by other users or any other “unlawful, misleading, malicious, or discriminatory” actions. [FB-15-A]

Section 4: Registration and Account Security - Within Section 4 Facebook aims to prevent the creation of false and duplicate accounts. However, it is well known that Facebook and other social media sites are full of false accounts and that such sites cannot do much to prevent such account creation.

Section 5: Protecting Other People's Rights - In Section 5 Facebook reserves the right to remove content that it deems in violation of the Statement of Rights and Responsibilities.

Section 9: About Advertisements and Other Commercial Content Served or Enhanced by Facebook - The user gives Facebook permission to use their “name, profile picture, content, and information in connection with commercial, sponsored, or related content”. [FB-15-A] It goes on to explain this in a more practical context advising the user that by giving such permission it allows “a business or other entity to pay us to display your name and/or profile picture with your content or information”. [FB-15-A]

Section 13: Amendments - Facebook will notify users when changes to the terms are made. The user may review and comment on the updated terms and will demonstrate acceptance of such terms by choosing to continue to use Facebook Services.

Section 15: Disputes - Within this section Facebook advises users of the chosen legal jurisdiction. As such any claims made will be handled “exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County”. [FB-15-A] It further states that Facebook does not “control or direct users’ actions on Facebook” and is “not responsible for the content or information users transmit or share on Facebook”. It states: “We are not responsible for any offensive, inappropriate, obscene, unlawful or otherwise objectionable content or information you may encounter on Facebook. We are not responsible for the conduct, whether online or offline, of any user of Facebook.” [FB-15-A] Users are advised that use of Facebook Services is at their own risk.

Section 16: Special Provisions Applicable to Users Outside the United States - Users located outside of the United States are informed that by agreeing to this statement they agree that personal data may be transferred to and processed in the United States.

Section 18: Other - Users located outside of the United States or Canada are advised that the agreement in their case is made specifically with Facebook Ireland Limited.

At the conclusion of the Statement of Rights and Responsibilities users are reminded that, “by using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time”. [FB-15-A] Users are thus reminded both at the beginning and at the end of the statement that the Data Policy applies in regard to content and information collection and use.
APPENDIX B

Facebook: Data Policy Summary

Facebook’s Data Policy is available at www.facebook.com/about/privacy. It governs the collection and use of content and information collected. The following policy summary uses the Data Policy with the effective date of January 30, 2015. [FB-15-B] The Data Policy applies to all of the Facebook Services but does not apply to those that make use of their own privacy policy. It covers a total of 8 specific sections.

**Section 1: What kinds of information do we collect** - Section 1 provides a list of information collected by Facebook.

- Content and information submitted by users.
- Actions of the user, including content viewed and interacted with.
- Content and information provided by other Facebook users about the specific user, such as when they tag a photo or send a message to that user.
- Associates and groups the user is in contact with.
- Information provided by the user when they choose to sync information with Facebook.
- Extensive device information “from or about the computers, phones, or other devices where you install or access our Services”. [FB-15-B] The extent of such collection is dependant on permissions granted to Facebook by the user. Information collected includes the “operating system, hardware version, device settings, file and software names and types, battery and signal strength, and device identifiers”. [FB-15-B] It also includes location information, as can be ascertained using GPS, Bluetooth or Wi-Fi signals as well as Internet service provider or mobile operator names, browser type, mobile phone number and IP addresses.
- Information collected from applications and websites that use Facebook Services, including Facebook’s ‘Like’ button or advertising services supplied by Facebook on third-party websites.
- Information collected from partner companies as well as from other companies owned or operated by Facebook.

**Section 2: How do we use this information?** - Information collected is used for a variety of purposes such as to personalise and localise the content displayed to users, to make suggestions, to deliver targeted advertisements and for security reasons such as for detecting suspicious activities. Facebook uses cookies and other similar technologies to facilitate the collection of information for such uses. Information is gathered for both Facebook members and non-members no matter whether a member is signed-in or not. The Facebook Cookie Policy is available for review at www.facebook.com/policies/cookies. The purpose for cookie usage includes authentication, advertising, measurement, analytics, localisation, providing site functionality, performance measurement and improvement.
Devices use similar cookies or methods and may store an identifier on the device to, for example, associate that device with a specific user. [FB-16-B]

Section 3: How is this information shared? - Users are advised that they have control over who is able to view any communications made on Facebook. Users are reminded that public information is accessible to everyone, be it on or off Facebook. Such information can, for example, be located by using search engines. Control over submitted information is lost when the user decides to comment on a friend's post. In this case, it is that friend who has control over who will see such comments. The user must be aware that the visibility of comments made on friends' posts may be set to 'public'. Friends may also share information about a specific user, in which case that user will also not have control over the visibility settings of such information.

Third-Party applications available via the Facebook site use their own policies and will ask users for specific access permissions. It is up to the user whether to give these applications access to the requested Facebook information.

Within the Facebook companies, user information is shared freely. A link is provided within the Data Policy to the webpage listing the companies owned and operated by Facebook. These companies include Atlas (advertising service), Facebook Payments Inc., Instagram, LiveRail (advertising server and exchange), Moves (mobile app), Oculus (virtual reality developer), Onavo (mobile app developer), Parse (cloud-based application development platform) and WhatsApp. [FB-16-C]

When Facebook partners with companies, it does not share any personally identifiable information with such companies. However, the Data Policy defines personally identifiable information as “information like name or email address that can by itself be used to contact you or identifies who you are”. [FB-15-B] Thus, only information that can on its own identify an individual is considered to be personally identifiable information by Facebook. This would mean that information, that could in combination with other information identify individuals, may in fact be shared with such companies with whom information is shared for the purposes of providing advertising, measurement and analytics services. Information is also shared with vendors, service providers and other partners used by Facebook to support their services such as for technical support or payment services.

Section 4: How can I manage or delete information about me? - The user is presented with various tools to control the information stored. Tools available include the activity log and the option to download all information stored by Facebook. This allows the user to see and control the information by either deleting it or changing the appropriate settings.

In terms of data retention the Data Policy states that Facebook stores “data for as long as it is necessary to provide products and services to you and others”. [FB-15-B] Information associated with an account is kept only until the account is deleted. For detailed information the user is referred to a different webpage via a link provided. [FB-16-D] On this webpage the
user is informed that an account can either be deleted or temporarily deactivated. When deleting an account the user is reminded that information shared with Facebook friends may still be available even after the account has been deleted since such information is stored on their friends’ accounts. Users are further advised that it may take up to 90 days until information is deleted from Facebook’s backup systems. However, immediately after the user deletes the account the information will no longer be accessible to others. Facebook will retain some information including log records for technical purposes. Information kept is disassociated from any personal identifiers. It is not stated for how long such information is kept. [FB-16-D]

Section 5: How do we respond to legal requests or prevent harm? - Facebook reserves the right to “access, preserve and share” user information either for the detection, prevention or investigation of illegal activities or for legal requests. [FB-15-B]

Section 6: How our global services operate - Even though the U.S.-EU Safe Harbour Framework has been invalidated, Facebook still only list this framework for the “collection, use and retention of information from the European Union”. [FB-15-B] It does not inform users of the fact that this agreement has been invalidated in October 2015 and whether other means are being used in the interim for data transfer from the EU. Users located within the European Economic Area are only informed that their information may be “transferred to countries outside of the EEA for purposes discussed in the Data Policy”. [FB-15-B]

Section 7: How will we notify you of changes to this policy? - Facebook informs its users that it will notify users before changes to the data policy are made. Users will then have to opportunity to comment on the new version of the policy.

Section 8: How to contact Facebook with questions - United States or Canadian users are asked to contact Facebook Inc. in California, United States. For users living in other countries the point of contact is Facebook Ireland Ltd. in Dublin, Ireland. Section 8 also supplies a link to a webpage named ‘Privacy Basics’ which helps users to understand the workings of their Facebook account. It provides detailed information in five categories. [FB-A]

1. What Others See About You - Includes visibility settings of posts, profile information, likes and comments. Tagging photos and deleting or deactivating the account.

2. How Others Interact With You - Includes the timeline, unfriending and blocking users, controlling who can like or comment on posts, removing tags in photos and allowing Facebook to use facial recognition technology.

3. What You See - Includes managing what is shown on the news feed and setting ad preferences.

4. How to Keep Your Account Secure - Includes passwords, logging in and out, hacked accounts, information about spam and phishing, and government information requests.
5. Facebook and Advertising - Includes more in-depth information about the type of advertisements the user will see while using Facebook as well as on third-party sites that use Facebook ad preferences.

Facebook provides a lot of information to its users. However, a considerable time investment is required if a user wishes to read all provided information and to adjust the many available settings.
APPENDIX C

Twitter: Terms of Service Summary

Twitter provides a User Agreement, which includes the Terms of Service, Privacy Policy and Twitter Rules. The User Agreement can be located at twitter.com/tos. There is no need to log into Twitter or to have a Twitter account in order to access the information. Twitter Rules are not covered within this summary, as they do not pertain to user privacy issues. The rules are limited to the type of content allowed and what constitutes unacceptable user behaviour. The summary below is of the information contained within the Terms of Service with an effective date of January 27, 2016. [TW-16-A] The following sections of the Terms of Service are of relevance to the privacy of Twitter users.

In the introduction to the Terms of Service, Twitter advises users that the terms listed apply not only to the Twitter website, but also to other services including other websites and applications that are within the scope of Twitter Services. A link is provided to a Twitter Help Center webpage that supplies a list of Twitter Services and corporate affiliates. [TW-15-D] Twitter Services include Curator (a tool that allows media publishers to find and collect the best topic specific Tweets), Digits (provides user authentication services), Periscope (a live-streaming video app) and TweetDeck (used to monitor Tweets in real time). Twitter’s corporate affiliates are listed as Crashlytics (a reporting service for the functioning of mobile applications), MoPub (advertising solution for mobile publishers), Niche (connects brands with social media celebrities to endorse their products), SnappyTV (a video sharing platform), TapCommerce (analyses user activity on mobile devices for customised advertisements), Tell Apart (analyses usage patterns used for targeted marketing) and Vine (a video-sharing platform).

By accessing or using the said services the user automatically agrees to and is bound by Twitter’s Terms of Service.

Section 1: Basic Terms - Twitter clearly informs the user that most of the content posted by the user will be public by default. It advises users to make necessary adjustments in their account settings in order to control who will be able to view their content. By agreeing to the Terms of Service the user gives Twitter and its third-party providers permission to place advertising on the Services. Such advertisements may be specific to the content provided or any other information gathered.

Section 2: Privacy - Any information provided to Twitter is subject to their Privacy Policy. Twitter asks users to consent as follows: "You understand that through your use of the Services you consent to the collection and use (as set forth in the Privacy Policy) of this information, including the transfer of this information to the United States, Ireland, and/or other countries for storage, processing and use by Twitter." [TW-16-A] At this point the user
should refer to the Privacy Policy before being able to consent to this statement, as the Terms of Service do not include information about the collection and use of user information.

**Section 4: Content on the Services** - Twitter does not monitor or control any content on the site. As such, the user is advised that use of the site or of content posted on the site is at the user’s own risk. The user may be exposed to a variety of information including information that is offensive or deceptive.

**Section 5: Your Rights** - Even though the user retains rights to the content posted, Twitter reserves the right “to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such content in any and all media or distribution methods”. [TW-16-A] Twitter will also be able to submit any content to “other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such content on other media and services”. [TW-16-A]

**Section 8: Restrictions on Content and Use of the Service** - Twitter reserves “the right to access, read, preserve, and disclose any information” as deemed necessary. [TW-16-A] This includes for legal reasons or by governmental request. Twitter will only disclose personally identifying information to third parties in accordance with their Privacy Policy. [TW-16-A]

**Section 11: Disclaimers and Limitations of Liability**

A. **The Services are Available “As-Is”**
Twitter will not be held responsible for the accuracy or security of content or any harm that may result to the user from using the Services or contents.

B. **Links**
Twitter shall not be held responsible for any provided links. The user assumes all risk when choosing to use such links.

**Section 12: General Terms**

B. **Controlling Law and Jurisdiction**
The controlling law and jurisdiction of the Terms of Service are set for San Francisco County in the state of California, United States.

C. **Entire Agreement**
When Twitter revises its Terms of Service it is up to Twitter to decide whether such a revision is substantial enough to warrant notification of such revision. Even without notification, users are bound by these new terms if they continue to use the service. Users are advised that if they live in the United States the agreement is made with Twitter Inc. located in San Francisco, California. If they live outside of the United States, the agreement is made with Twitter International Company located in Dublin, Ireland.
The Twitter Privacy Policy is contained within the User Agreement and regulates the way Twitter collects, uses and shares user information. It can be accessed either via twitter.com/tos or twitter.com/privacy. The summary below is of the information contained within the Twitter Privacy Policy with an effective date of January 27, 2016. [TW-16-B]

Twitter states that it collects information from: “Various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services (the “Twitter Services”) as well as from their partners and “other third parties”. [TW-16-B] The same link that was provided in the beginning of the Terms of Service is also provided at this point, to direct users to a Twitter Help Center page providing a list of the Twitter Services and corporate affiliates. [TW-15-D] (Please see the beginning of Appendix C for the detailed list.) Corporate affiliates listed are covered under the Privacy Policy but may have additional terms, which should be consulted for each individual company.

By using the services the user gives consent to the “collection, transfer, storage, disclosure, and use” of the user’s information as it pertains to the Twitter Privacy Policy. [TW-16-B] The user authorises Twitter to transfer, store and use the information in the United States, Ireland and any other countries where they operate. Twitter further advises users that the “privacy and data protection laws in some of these countries may vary from the laws in the country where you live”. [TW-16-B] Twitter Inc. in San Francisco, California, controls the information of users living in the United States, while Twitter International Company in Dublin, Ireland controls the information of users living outside of the United States.

**Information Collection and Use**

**Account and Contact Information:**
Personal information is required to create an account. This includes the user’s name, username, password, e-mail address, or phone number. Publicly viewable are only their name and username. Twitter advises the user that it is acceptable to either use their real name or a pseudonym. By providing Twitter with a phone number the user agrees to receive text messages from Twitter.

**Optional Additional Information:**
When the user chooses to use their Twitter login to sign into a third-party application by using Digits by Twitter, they authorise Twitter to share the user’s contact information with the third-party application.

Users are also advised that by changing their privacy settings on their account, they can control whether other Twitter users can locate them using their email address or phone
number. Twitter also provides specific settings to allow the user to control who can see profile information. However, such settings may not be able to control all information. Information that cannot be controlled via these settings will be ‘public’ by default.

If users choose to sync their address book with Twitter, in order to locate their friends on the site, they must be aware that Twitter may use their address book to personalise content or make suggestions based on the imported contacts. However, the user can delete their imported contacts at any time if they choose to do so.

Public Information:
Information that is ‘public’ by default includes Tweets, Tweet metadata including the time the Tweet was made and client application used, language and time zone of the account, lists the user creates, users followed, Tweets liked or retweeted and other information not further specified by the policy. The user is advised that when sharing content the user “should think carefully about what you are making public”. [TW-16-B]

Location Information:
It is up to the user to choose whether to share their location information in their Tweets and profile. However, Twitter may use information from the device used in order to establish location. This may utilise the user’s IP Address, GPS, wireless network or cell tower information. Such information may be used to deliver locally relevant content.

Links:
Twitter records any links that are clicked on by the user. This is done for the purpose of keeping statistical information as well as for providing targeted advertising.

Cookies:
Cookies and similar technologies are used to collect information. This monitors how users interact with the site as well as web traffic routing. Reasons given for such information collection are to “customize and improve our Services”. [TW-16-B]

Log Data:
Log data received by Twitter includes “IP address, browser type, operating system, the referring web page, pages visited, location, mobile carrier, device information (including device and application IDs), search terms, and cookie information”. [TW-16-B] Such information is gathered every time a user interacts with any of the Twitter Services. This includes simply visiting a website that uses a Twitter button or widget. Purpose for logging a large variety of information is to display targeted topic suggestions, content and advertisements to users. Log data will be either deleted or “any common account identifiers” removed after a maximum of 18 months. [TW-16-B]

Third Parties and Affiliates:
Information gathered by third-party services and corporate affiliates may be shared with Twitter in order for Twitter to customise advertisements for its users.
Information Sharing and Disclosure

Twitter will disclose information when instructed to do so by the user. For example, this can be the case when the user wants to log in on a third-party website using their Twitter login. Twitter may also share personal information with service providers. Such service providers are subject to the Privacy Policy and may only use such information according to instructions given by Twitter. Information may also be disclosed if it is deemed necessary to comply with "law, regulation, legal process or governmental request". [TW-16-B] The user is advised that information disclosure may also occur when other Twitter users mention or tag a user in their Tweets.

Changes to the Privacy Policy

Twitter revises the Privacy Policy as necessary. Users will be made aware of revisions only if the revision is deemed substantial enough. By continuing the use of Twitter Services, the user thereby demonstrates agreement with the revised Privacy Policy.
This page has been left blank intentionally.
Google’s Terms of Service are located at www.google.com/policies/terms. [GO-14-A] The Terms of Service inform users that services are provided by Google Inc. located in California, United States. All services provided by Google Inc. are included and hence the Terms of Service are applicable to the services provided by Google+. Because the Terms of Service encompass all services they are intentionally kept broad in scope. Additional terms may have to be consulted for other services provided by Google. The summary of these terms was made using the Terms of Service with an effective date of April 14, 2014. Archived versions may also be accessed via the site. [GO-14-A]

Three sections of the Terms of Service have been found to be of specific relevance to the privacy of Google+ users.

Section: “Privacy and Copyright Protection” - The user is referred to the Google Privacy Policy.

Section: “Your Content in our Services” - As directly stated in the Terms of Service, “When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.” [GO-14-A] Google has the right to use any content submitted by the user. This right is limited to using such data only for operating, promoting, improving or developing services. Even when the user discontinues use of Google services, Google retains the right to use previously submitted content for the purposes stated above.

It is important to note that Google analyses all content submitted by a user. This includes reviews, feedback and e-mails. Automatic analysis is done when any content is submitted, received and stored. As per the Terms of Service, the results of such analysis are used to customize search results, for advertising and for spam and malware detection. Google also reserves the right to include user profile names and profile photos in advertisements. For example, photos submitted to Google+ may be used as background on Google products. The user is advised to change their settings accordingly if they do not wish their publicly viewable information to appear in advertisements.

Section: “About these Terms” - The user is advised that the Terms of Service operate under the laws of the state of California, United States.
This page has been left blank intentionally.
APPENDIX F

Google: Privacy Policy Summary

The Google Privacy Policy governs the way information is collected, the reasons for its collection and how the information may be used. It applies to all services offered by Google Inc. and its affiliates. Affiliates include YouTube, services provided on Android devices and Google services that are used on other sites, such as their advertising services. Any services that are using their own separate privacy policy are not included. The Privacy Policy reviewed for this summary is effective as of March 25, 2016 and is available at www.google.com/policies/privacy. [GO-16-A] Older versions of the Privacy Policy are available for viewing at www.google.com/policies/privacy/archive. [GO-16-C]

What Information is used for
Information collected by Google is used to improve Google services, customise search results and advertisements, and to improve security such as spam filtering. [GO-C]

How Information is Collected
Information is collected both from information submitted by the user, as well as from user interactions with Google services. Google utilises cookies and other similar technologies in order to gather the information. Google’s best known such mechanisms are Google Analytics and the DoubleClick cookie.

Types of Information Collected
The device information collected when a user accesses Google services includes:
- Operating system information.
- Device hardware type/model.
- Unique device identifiers such as an IMEI number.
- Phone number and mobile network information.
- Types of browsers used.
- Hardware settings.
- Language preferences.

Logs are maintained by Google that include information such as the user’s search queries, ads clicked on, websites visited, videos watched and the Internet protocol address. It also includes information such as the user’s phone number, phone number of person/s interacted with, time, date and duration of calls, and text message routing information.

Location information is gathered using a variety of sources such as the IP address, GPS, Wi-Fi access points and mobile network towers. Google also uses location information that is gathered from user search queries about locations the user is showing interest in. This
includes any information that infers the user is either interested in a particular location or might be at that location. [GO-A]

It is important to note that information is collected both while users are signed in and also when not signed in. Information gathered while users are signed in may be combined with the users’ Google accounts. Such information can include contacts added, calendar events, photos, videos or documents uploaded. [GO-B] A new feature added to the current Privacy Policy is that users now can opt out of certain customisations that occur when they are not signed-in. This means that users can control whether or not they want to allow targeted advertisements and search results that are based on their past searches. [GO-16-A]

If collected information is combined with a user’s account it will be regarded as ‘personal’ information and treated as such under the policy. The policy goes on to reiterate items already mentioned in the Terms of Service such as usage of profile name and profile photos in advertisements and the fact that content analysis is automated and set to analyse all content submitted including emails sent and received.

**Data Storage and Processing**

Google advises the user that their personal information may be processed on any server located in any of the countries where Google holds such servers. Because locations are not provided, the user will not know exactly in which country the information is stored and processed.

In the “Compliance and cooperation with regulatory authorities” section of the Privacy Policy, a link is provided that redirects the user to a webpage regarding “Self Regulatory Frameworks”. [GO-14-B] The information on this webpage was last revised on November 21, 2014 and explains that Google complies with the U.S.-EU Safe Harbour agreement for the “collection, use and retention of personal information from European Union member countries”. [GO-14-B] It fails to inform readers that this agreement has been invalidated in October 2015 and what other measures Google is using in the interim.

**User Awareness**

A variety of options are presented so that the user may make adjustments to their settings. Direct links to relevant information are provided. Users are also made aware that information shared publicly may be indexed by various search engines and are given examples of options such as deleting web history. Users are furthermore informed that when the user deletes information from Google services, such information will not immediately be deleted from all active servers containing copies of the information and that it may not be deleted at all from Google’s backup servers.

**Information shared by Google**

**With Parties within Google**

Within Google, access to personal information is restricted and only available to relevant entities on a need-to-know basis.
With Parties outside of Google
Non-Personally Identifiable Information:
Google reserves the right to share information that does not personally identify an individual with any of their partners such as advertisers and publishers.

Personal Information:
Google does not share what is deemed 'personal' information with anyone outside of Google unless it is for any of four stated reasons:

- With the explicit consent of the user.
- When a domain administrator is used to maintain the user’s account.
- For processing provided by Google’s affiliates and other trusted parties. This processing must be done in compliance with the Google Privacy Policy and only when instructed to do so by Google.
- For legal reasons such as legal process, governmental requests, investigations into Terms of Service violations, or fraud, security or technical investigations. A Transparency Report is available and provides information about governmental requests received by Google. The information can be accessed at www.google.com/transparencyreport/userdatarequests. [GO-15-A]
This page has been left blank intentionally.
The LinkedIn User Agreement can be located at linkedin.com/legal/user-agreement. Anyone wishing to review this agreement does not need to be signed into LinkedIn or have a LinkedIn account. [LI-14-A]

The summary of the agreement is based on the User Agreement that was last revised on October 23, 2014. LinkedIn reserves the right to make changes to these terms. LinkedIn states that it will notify users of such changes. When a user continues using the services, it is implied that the user is agreeing with the new User Agreement terms.

At the beginning of the document, the User Agreement states that the terms apply to LinkedIn.com, SlideShare.net, LinkedIn Pulse and other LinkedIn services and apps. It does not go into detail about what the ‘other LinkedIn services and apps’ include. The user is notified that by agreeing to the terms set out in the User Agreement they also agree to the LinkedIn Privacy Policy. The agreement applies to both registered and un-registered users utilising LinkedIn Services. As soon as an individual joins or uses LinkedIn or other LinkedIn services such action will imply that they have agreed to the terms of the User Agreement. For United States residents the agreement is made with LinkedIn Corporation. For users residing outside of the United States it is made with LinkedIn Ireland, located in Dublin.

**Summary by Sections**

**Under Section 2, Obligations, Subsection 2.4, Notices and Service Messages**, the user agrees that LinkedIn may send notices using various means, such as the user’s email address or mobile number. Account settings should be adjusted accordingly if users wish to control or limit such messages.

**Under Section 2, Obligations, Subsection 2.5, Messages and Sharing**, users are further advised that they may use account settings to control who sees posted information. By default only applying for jobs and using InMail are set to be private.

**Under Section 3, Rights and Limits, Subsection 3.1, Your License to LinkedIn**, LinkedIn states that even though the user owns their content, LinkedIn is granted permission to “a worldwide, transferable and sublicensable right to use, copy, modify, distribute, publish, and process, information and content that you provide through our Services, without any further consent, notice and/or compensation to you or others”. [LI-14-A] This includes any suggestions or feedback the user sends to LinkedIn. However, certain limitation to the license exist:

- Content can be deleted. Deletion does not affect content shared with other users who may have saved such content. It also may take some time until LinkedIn deletes such content from all of their systems and as such deletion will not be immediate.
- A user’s content will not be used in advertisements without the user’s specific consent.
- LinkedIn will obtain user consent before giving third parties, who are beyond LinkedIn Services, the right to publish the user’s content.
- LinkedIn may change the format of content but will not change the meaning of the content.

**Under Section 6, Dispute Resolution**, it is stated that any dispute resolution will take place under the legal jurisdiction of Santa Clara County, California, United States. If a dispute should arise from users located outside of the United States, the first point of contact should be LinkedIn Ireland in Dublin.
APPENDIX H

LinkedIn: Privacy Policy Summary

Any user of LinkedIn Services automatically agrees with LinkedIn’s Privacy Policy when agreeing to the terms in the LinkedIn User Agreement. The Privacy Policy governs the collection, use, sharing and storing of users’ personal information. The Privacy Policy reviewed was last revised on October 23, 2014 and is available at linkedin.com/legal/privacy-policy. [LI-14-B] An archive of previous policies is not available on-line. To read the current version users do not have to be logged in or have a LinkedIn account.

LinkedIn will only share a user’s personal information with third parties with the user’s consent, to carry out instruction given by the user, as is “reasonably necessary” to provide LinkedIn services, as required by law, to enforce the User Agreement or to protect LinkedIn or its members and visitors. [LI-14-B]

Data Controllers
As already stated in the User Agreement, the Privacy Policy reiterates that information from users within the United States is controlled by LinkedIn Corporation in the state of California, while information from users located outside of the United States is controlled by LinkedIn Ireland in Dublin. The Privacy Policy advises LinkedIn users that their information may be processed outside of the country in which they reside, in locations where LinkedIn, its affiliates or service providers operate.

User Provided Information
LinkedIn stores any information provided by the user, such as name, e-mail address, mobile number, the user’s location, previous jobs, education and any other information the user chooses to add to their LinkedIn profile. Such information is used by LinkedIn to serve relevant advertisements and content, both while using their services and when on other websites that have a connection to LinkedIn via, for example, cookies or social plugins.

Synced Information
LinkedIn will also collect information when a user chooses to sync outside content with their LinkedIn account. This includes syncing their address book, mobile device contacts or mobile calendar. LinkedIn will store all the information obtained via such syncing action, including all information in the address book such as e-mail addresses and phone numbers. As stated by LinkedIn, such information is used to provide “a template to send invitations on your behalf to your contacts that are not Members”. [LI-14-B] This means that LinkedIn may send invitations on the user’s behalf to anyone within the user’s address book who is not yet a member.

Users should be aware that communications initiated via LinkedIn services, such as sending connection invitations to other LinkedIn users, may expose the user’s e-mail address or mobile number as the name and primary email address will be visible in the header of the
message. However, a request for an introduction will only list the user’s name but will not include the e-mail address. Users are also advised that communications made using emails, instant messaging and other similar means with other LinkedIn users are not encrypted and it is thus advised not to communicate any sensitive information using such communication methods. [LI-14-B]

Information collected by LinkedIn
LinkedIn collects information any time a user interacts with any of the LinkedIn Services or visits a site that uses LinkedIn cookies or social plugins. This is the case whether they are a LinkedIn member or just a visitor. Information shared with websites that use LinkedIn cookies and plugins consists of general reports to allow such sites to measure traffic to their website. Personal information will not be shared with such sites. LinkedIn provides a separate Cookie Policy in which the reasons for using cookies and similar technologies are stated. [LI-14-C] Reasons given include:

- Identifying the device used.
- Keeping the user logged in when they return to the site.
- Serving customised advertisements both on the LinkedIn sites and on third-party sites that use LinkedIn plugins. (Further technologies are utilised for this purpose, such as web beacons, pixels and anonymous ad network tags.)
- Detecting violations of the User Agreement and other malicious activity.
- Saving user preferences.
- For analytics and research purposes.

LinkedIn uses persistent and short-term session cookies, as well as locally stored objects used by Adobe Flash. Companies used by LinkedIn for such purposes include DoubleClick, BlueKai, Lotame, Google Analytics, Quantcast, Nielsen, ComScore and Eloqua. [LI-14-C] Various methods to control cookies are provided to users including opting-out of cookie usage, in which case LinkedIn will place an opt-out cookie onto the user’s device. Users are cautioned that the LinkedIn site will not work as it should without the use of cookies. [LI-14-C]

When a member is logged in or identified by one of the LinkedIn cookies, any information collected will be associated with the member’s account and used to customise advertisements and content. This occurs even when the member is not logged in, but when a cookie can positively identify the member based on device or other information that is collected and logged. Device information includes IP Address, computer or mobile operating system, web browser used, mobile device identifier and name of the Internet service provider or mobile carrier. Location information may be collected if such setting is enabled on the device. Information is also collected when users choose to use their LinkedIn account to log into a third-party website or application. LinkedIn will receive information from such third-party websites and applications.

Advertising Mechanisms
Personal information is not shared with any parties outside of the LinkedIn affiliates unless permission is sought and granted by the user. In the LinkedIn Ads Agreement, referred to in
Section 2.11 of the Privacy Policy, entities wishing to make use of LinkedIn Ads are advised that advertisements shown to users are to be based on “non-personally identifiable profile data”. [LI-10] Profile data will not be supplied to entities wishing to advertise and such entities should not attempt to collect profile data. LinkedIn users who view any of the ads presented are to remain anonymous to advertising companies. Users have the option of opting-out of the use of customised advertisements. [LI-10]

LinkedIn Communications
Users can control communications sent by LinkedIn by adjusting their account settings. Otherwise, they may continue to receive emails, mobile text messages, push notifications or posts on the LinkedIn site or app.

Sharing Information with Affiliates
LinkedIn may share user information, including personal information, with LinkedIn affiliates as deemed necessary to provide services. Information is shared and combined across LinkedIn Services, such as between SlideShare and LinkedIn, to provide customised content to the user.

Sharing Information with Third Parties
LinkedIn does not share personal information without user consent, unless it is required to do so by law or to enforce the User Agreement. Public profile information is available for indexing by search engines. Users who do not wish to have their information indexed can change the appropriate account settings. Changing these settings will also control what information will be exported when recruiters export a member’s public profile information. Furthermore, the user can control the degree of connection to other LinkedIn members. This will control whether other members will be able to see the user’s full profile and contact information or only partial information. Recruiters and similar subscribers will however be able to see the full profile.

Service Providers
Third-party service providers used by LinkedIn may have access to user information. However, this is only to the extent necessary for required services.

Right to Access Information
Members have the right to request personal information that is held by LinkedIn, including information such as IP address logs. Such a request can be submitted to the LinkedIn Help Center.

Account Closure and Data Retention
According to Section 3.1, once an account has been closed, information will typically be removed within 24 hours and LinkedIn will “generally delete closed account information and will de-personalize any logs or other backup information through the deletion process within 30 days of account closure, except as noted below”. [LI-14-B] At the end of Section 3.1, LinkedIn explains that information shared with other LinkedIn users may have been copied
and saved and therefore may still be accessible after the account has been closed. Content submitted to a group will also remain visible, but the user’s name will not be shown. It also advises users that information indexed by search engines will remain available until the search engine’s cache is refreshed.

The exceptions referred to in Section 3.1 are listed in Section 3.2. Here it states that LinkedIn will “keep your information for as long as your account is active or as needed”. [LI-14-B] Reasons provided include instances when it is “reasonably necessary to comply with our legal obligations, meet regulatory requirements, resolve disputes between Members, prevent fraud and abuse, or enforce this Privacy Policy and our User Agreement”. [LI-14-B] Information is also kept for reporting and trend analysis and for plugin impression data. LinkedIn’s plugin impression data will be de-personalised within 7 days but will be retained for a period of 30 days for security, debugging, and site stability purposes. [LI-14-B]

**Data Transfer**

In Section 4.2 of the Privacy Policy users are informed of LinkedIn’s compliance with the U.S.-EU Safe Harbour framework for data transfers from the European Union to the United States. After explaining its compliance with the Safe Harbour program the LinkedIn Privacy Policy continues with the addition of the following text:

“No: The U.S.-EU Safe Harbor Framework is no longer recognized as a legal mechanism to transfer personal data from the EU to the US. LinkedIn Ireland uses other legal mechanisms, including standard contractual clauses.” [LI-14-B]

A link is provided for users to obtain more information in regard to the added note. When clicking on this link, the user is redirected to a different webpage. The information contained within this webpage was dated on October 27, 2015 and has since been revised in February 2016. It briefly explains that as of October 6, 2015 the Safe Harbour Agreement has been invalidated and that because of this, LinkedIn will be utilising standard contractual clauses for data transfers between the European Union and the United States. [LI-16-B] As per a statement made by the Article 29 Working Party on October 16, 2015, the use of standard contractual clauses for such transfers is acceptable in the interim. [EC-15-A]

Because of this note, the information contained within the Privacy Policy must have been revised at some point in or after October 2015, when the Safe Harbour agreement was declared invalid. However, the date of the Privacy Policy’s last revision remained October 23, 2014. As the change is rather significant in nature from a legal perspective, it is peculiar why the revision date was not updated at the time the note was added to the policy.

In Section 4.3, following the Safe Harbour information, LinkedIn states that it will notify users when changes are made to the Privacy Policy, if such changes are deemed significant. However, an addition of text about the Safe Harbour Agreement neither triggered a new revision date, nor a user notification. LinkedIn methods of handling revisions appear to be inconsistent.
APPENDIX I

Comparison of GDPR (EU) 2016/679 and Directive 95/46/EC

Table 3 depicts a brief comparison of the General Data Protection Regulation (EU) 2016/679 and the Directive 95/46/EC in areas most relevant to user privacy in social networks. In the interest of keeping length to a minimum, only areas of notable change have been included, as a full summary and comparison would result in a more extensive table. The majority of information contained within the table is verbatim, however some wording, for the purpose of condensing the information, has been edited. Quotation marks were not used for verbatim text to produce a table that is easier to read. Some wording has been bolded to highlight specific areas of change. [EL-95] [EL-16]

Table 3 Comparison of the General Data Protection Regulation and Directive 95/46/EC

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject-matter and objectives</strong> (Article 1)</td>
<td><strong>Object of the Directive</strong> (Article 1)</td>
</tr>
<tr>
<td>This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.</td>
<td>Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.</td>
</tr>
<tr>
<td><strong>Territorial scope</strong> (Article 3)</td>
<td><strong>National law applicable</strong> (Article 4)</td>
</tr>
<tr>
<td>1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.</td>
<td>1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:</td>
</tr>
<tr>
<td>2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:</td>
<td>(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;</td>
</tr>
<tr>
<td></td>
<td>(c) the controller is not established on community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the community.</td>
</tr>
<tr>
<td></td>
<td><strong>Definitions</strong> (Article 4) <strong>Definitions</strong> (Article 2)</td>
</tr>
<tr>
<td><strong>‘Personal data’</strong></td>
<td>‘Personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;</td>
</tr>
<tr>
<td>Recital (26) Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly.</td>
<td>‘Personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;</td>
</tr>
</tbody>
</table>
'Processing'

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Processing of personal data' ('processing') shall mean 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;

'Profiling'

'Profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

No definition for 'profiling'.

'Pseudonymisation'

'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

No definition for 'pseudonymisation'.

'Consent'

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

'Biometric data'

'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

No definition for 'biometric data'.

Principles relating to processing of personal data (Article 5)

(a) Processed lawfully, fairly and in transparent manner;
(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
(d) Accurate and, where necessary, kept up to date;
(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, ('storage limitation');
(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality');

Principles relating to data quality (Article 6)

(a) Processed fairly and lawfully;
(b) Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
(c) Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
(d) Accurate and, where necessary, kept up to date;
(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
<table>
<thead>
<tr>
<th>Lawfulness of processing (Article 6)</th>
<th>Criteria for making data processing legitimate (Article 7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing shall be lawful only if:</td>
<td>(a) the data subject has unambiguously given his consent; or</td>
</tr>
<tr>
<td>(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</td>
<td></td>
</tr>
<tr>
<td>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</td>
<td>(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</td>
</tr>
<tr>
<td>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</td>
<td>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</td>
</tr>
<tr>
<td>(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;</td>
<td>(d) processing is necessary in order to protect the vital interests of the data subject; or</td>
</tr>
<tr>
<td>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</td>
<td>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or</td>
</tr>
<tr>
<td>(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.</td>
<td>(f) 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, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).</td>
</tr>
</tbody>
</table>

### Processing of special categories of personal data (Article 9)

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

### The processing of special categories of data (Article 8)

1. Member States shall prohibit the processing of 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.

### Paragraph 1 shall not apply if:

- a) the data subject has given explicit consent to the processing of those personal data

Note: The GDPR provides further detail in terms of when such data can be processed for public interest reasons.

### Information to be provided where personal data are collected from the data subject (Article 13)

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

   a) and b) contact details of Controller, controller's representative and/or data protection officer.

   c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

   d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (i.e. if based on 'legitimate interests', information on these must be provided.)

   e) the recipients or categories of recipients of the personal data, if any;

   f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

### Information in cases of collection of data from the data subject (Article 10)

1. Article 10 - Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

   a) the identity of the controller and of his representative, if any;

   b) the purposes of the processing for which the data are intended;
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the **period** for which the **personal data will be stored**, or if that is not possible, the **criteria used to determine that period**.

(b) the existence of the right to request from the controller access to and rectification or **erasure** of personal data or **restriction of processing** concerning the data subject or to **object to processing** as well as the **right to data portability**;

(c) 3 - the existence of the right of access to and the right to rectify the data concerning him.

(d) the **right to lodge a complaint** with a supervisory authority;

(e) whether the provision of personal data is a **statutory or contractual requirement**, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the **possible consequences of failure to provide such data**;

(f) the existence of automated decision-making, **including profiling**, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

<table>
<thead>
<tr>
<th>Right of access by the data subject (Article 15)</th>
<th>Right of access (Article 12)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 15 - 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:</td>
<td>Member States shall guarantee every data subject the right to obtain from the controller: (a) 1 - Confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.</td>
</tr>
<tr>
<td>(a) the purposes of the processing;</td>
<td>(a) 2 - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source;</td>
</tr>
<tr>
<td>(b) the categories of personal data concerned;</td>
<td>(b) as appropriate the rectification, erasure or <strong>blocking</strong> of data, the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data;</td>
</tr>
<tr>
<td>(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular <strong>recipients in third countries or international organisations</strong>;</td>
<td></td>
</tr>
<tr>
<td>(d) where possible, the envisaged <strong>period for which the personal data will be stored</strong>, or, if not possible, the criteria used to determine that period;</td>
<td></td>
</tr>
<tr>
<td>(e) the existence of the right to request from the controller rectification or erasure of personal data or <strong>restriction of processing</strong> concerning the data subject or to object to such processing;</td>
<td></td>
</tr>
<tr>
<td>(f) the <strong>right to lodge a complaint</strong> with a supervisory authority;</td>
<td></td>
</tr>
<tr>
<td>(g) where the personal data are not collected from the data subject, any available information as to their source;</td>
<td></td>
</tr>
<tr>
<td>(h) the existence of automated decision-making, <strong>including profiling</strong>, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.</td>
<td>(a) 3 - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);</td>
</tr>
</tbody>
</table>
| (i) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort. | (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.
<table>
<thead>
<tr>
<th>Right to erasure (‘right to be forgotten’) (Article 17)</th>
<th>No such right.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:</td>
<td></td>
</tr>
<tr>
<td>(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;</td>
<td></td>
</tr>
<tr>
<td>(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;</td>
<td></td>
</tr>
<tr>
<td>(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);</td>
<td></td>
</tr>
<tr>
<td>(d) the personal data have been unlawfully processed.</td>
<td></td>
</tr>
<tr>
<td>Recital (65) However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.</td>
<td></td>
</tr>
<tr>
<td>Notification of a personal data breach to the supervisory authority (Article 33)</td>
<td>No notification</td>
</tr>
<tr>
<td>In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.</td>
<td></td>
</tr>
<tr>
<td>Communication of a personal data breach to the data subject (Article 34)</td>
<td>No notification</td>
</tr>
<tr>
<td>1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.</td>
<td></td>
</tr>
<tr>
<td>3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:</td>
<td></td>
</tr>
<tr>
<td>(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;</td>
<td></td>
</tr>
<tr>
<td>(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;</td>
<td></td>
</tr>
<tr>
<td>(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.</td>
<td></td>
</tr>
<tr>
<td>Transfers of personal data to third countries or international organisations (Chapter 5)</td>
<td>Transfer of personal data to third countries (Chapter 4)</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Transfers on the basis of an adequacy decision (Article 45)</td>
<td>Principles (Article 25)</td>
</tr>
<tr>
<td>1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.</td>
<td>1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transfers subject to appropriate safeguards (Article 46)</th>
<th>Derogations (Article 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.</td>
<td>2. A Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.</td>
</tr>
<tr>
<td>2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a) a legally binding, enforceable instrument; b) binding corporate rules; c)/d) standard data protection clauses adopted by the Commission or by a supervisory authority; e) an approved code of conduct; f) an approved certification mechanism;</td>
<td></td>
</tr>
<tr>
<td>3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: a) contractual clauses; or b) provisions to be inserted into administrative arrangements between public authorities;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Derogations for specific situations (Article 49)</th>
<th>Derogations (Article 26)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer of a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:</td>
<td>1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:</td>
</tr>
<tr>
<td>(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers.</td>
<td>(a) the data subject has given his consent unambiguously to the proposed transfer; or</td>
</tr>
<tr>
<td>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;</td>
<td>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or</td>
</tr>
<tr>
<td>(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;</td>
<td>(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or</td>
</tr>
</tbody>
</table>

Where a transfer could not be based on a provision in Article 45 or 46, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.
<table>
<thead>
<tr>
<th>Anonymisation of data</th>
<th>No information on anonymisation of data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recital (26) The principles of data protection should therefore <strong>not apply to anonymous information</strong>, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.</td>
<td></td>
</tr>
<tr>
<td>Recital (29) The controller has taken technical and organisational measures necessary to ensure that additional information for attributing the personal data to a specific data subject is kept separately.</td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td>Does not further define consent.</td>
</tr>
<tr>
<td>Further to the definition given in Article 4, Recital (32) defines that consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.</td>
<td></td>
</tr>
<tr>
<td>Recital (42) For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.</td>
<td></td>
</tr>
<tr>
<td>Data Retention</td>
<td>Data Retention</td>
</tr>
<tr>
<td>Recital (39) Ensuring that the <strong>period for which the personal data are stored is limited to a strict minimum.</strong> In order to ensure that the personal data are not kept longer than necessary, <strong>time limits</strong> should be established by the controller for erasure or for a periodic review.</td>
<td></td>
</tr>
<tr>
<td>Article 13 - The controller shall, at the time when personal data are obtained, <strong>provide the data subject with:</strong> (a) the <strong>period for which the personal data will be stored,</strong> or if that is not possible, the criteria used to determine that period;</td>
<td></td>
</tr>
<tr>
<td>Only information provided is in Article 6(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.</td>
<td></td>
</tr>
<tr>
<td>No obligation to notify data subjects.</td>
<td></td>
</tr>
<tr>
<td>Direct Marketing</td>
<td>Direct Marketing</td>
</tr>
<tr>
<td>Recital (70) Where personal data are processed for the purposes of direct marketing, the data subject should have the <strong>right to object to such processing, including profiling to the extent that it is related to such direct marketing.</strong> That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.</td>
<td></td>
</tr>
<tr>
<td>Article 14 - Right to Object: (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.</td>
<td></td>
</tr>
<tr>
<td>European Data Protection Board (Article 68)</td>
<td>Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29)</td>
</tr>
<tr>
<td>The Board shall be composed of the <strong>head of one supervisory authority of each Member State</strong> and of the European Data Protection Supervisor or their respective representatives.</td>
<td></td>
</tr>
<tr>
<td>The Working Party shall be composed of a <strong>representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.</strong></td>
<td></td>
</tr>
<tr>
<td>5. The <strong>Commission shall have the right to participate in the activities and meetings of the Board without voting right.</strong> The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.</td>
<td></td>
</tr>
<tr>
<td>Identifiers</td>
<td>No information on identifiers.</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Recital (30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Profiling</th>
<th>No information on profiling.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recital (24) In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the Internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.</td>
<td></td>
</tr>
<tr>
<td>Recital (60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and the consequences of such profiling.</td>
<td></td>
</tr>
<tr>
<td>Recital (70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing.</td>
<td></td>
</tr>
<tr>
<td>Recital (71) Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transparency</th>
<th>No information on such transparency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recital (39) It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing.</td>
<td></td>
</tr>
</tbody>
</table>