# School of Electronics and Computer Science

Faculty of Physical Sciences and Engineering

University of Southampton

**Palak Prakash Jain**


11/01/2018

**Topic 3: Anonymity, Privacy and Security**

I am aware of the requirements of good academic practice, and the potential penalties for any breaches.

**Personal tutor: Federica Paci**

A report submitted for the award of

**MEng Computer Science**

## Table of Contents

## Topic Brief

3. Anonymity, Privacy and Security- Meaningful consent. Social media platforms such as Facebook are widely used by individuals as a convenient and effective way of keeping in contact and sharing information. However, Facebook's terms and conditions run to many thousand words, and few people have read them in full when agreeing to terms and conditions. Due to the convenience of clicking "Accept" to Terms and Conditions without reading them, some individuals inadvertently make accessible large amounts of sensitive or personal data, or share their contact list with others, without fully understanding what they have done, e.g. who has access to that information of how it is or might be used. Create a short report on meaningful consent on social media platforms, which covers: (1) the key ways in which individuals inadvertently compromise their security or unwillingly share personal information on social media. (2) The possible implications of sharing sensitive or personal information on social media. (3) Given that so few people read the full Terms and Conditions of programs and apps they download, your report must also outline how computer systems might be designed to better elicit meaningful consent from users when downloading apps or using social media.

## Abstract

Since the arrival of social networking sites in the early 21st century, the use of social media has grown multiple fold. Unsurprisingly, today it has become the forefront of communication for most of the world. However, with the influx in social media users, there has also been a surge in the amount personal data available online, leaving a large proportion of us worried. With a sharp rise in cyber crimes, personal data misuse has become a great concern.This report analyses the ways in which we, users, unwillingly and inadvertently sacrifice our personal data, and discusses its implications. Legislations like the General Data Protection Regulation aim to prevent the misuse of personal data but often fail.  After all, it is our fault as users that we give in personal information about ourselves in the first place. This paper presents key measures we can take to ensure the protection of our personal information and puts light on the possible implementation of specific computer systems to better elicit meaningful consent from users.

## Introduction

Social media platforms are widely used by individuals around the world as a convenient and effective way of keeping in contact and sharing information*(Sileo, 2018)*. Today, Facebook is by far the most used social media platform, worldwide. As of September 2018, the social media giant had 2.27 billion monthly active users *(Statista, 2018)*. One would think, almost a quarter of the world population uses Facebook, what risks could I possibly face if I use it ?  In early 2018, the news that a political consulting company 'Cambridge Analytica' harvested the personal data of approximately 80 million facebook users, reached headlines. The company had misguided facebook users to fill in surveys, stating that the information provided will be used for academic purposes*(Hern and Pegg, 2018)*, but, instead used it for political purposes.This is a cyber-crime, and a violation of the General Data Protection Act (which had not yet been implemented) as companies are not allowed to use users' personal data for purposes not known to them. In fact, it is often the case that legislations are put in place after the cyber crimes are committed, as a method to prevent them in the future. However, the result is that they are ultimately a step behind the crimes. This, therefore, raises an important discussion on how we end up giving information about ourselves.

## How do we compromise our personal information and security ?

Individuals allow their privacy to be eroded, usually unknowingly and unwillingly, simply by using smartphones. Research shows that 70 % of the British population now carries around devices which record and report their location, their friends and interests all the time (*The Guardian, 2018)*. The ease in which data sets collected from their social media pages makes it subtly easy for social networking sites or third parties to identify people from a set of anonymized data or even bring out their secrets. The following sections of the report highlight how users' behaviour on social media, especially Facebook, could lead to the misuse of their personal information and points out what can be done to prevent such from occurring.

### "Likes" on social media

Each time one clicks the 'like' button on a website, they broadcast themselves not only to friends on social media but also to social services providers and advertising/ data harvesting companies that work with them. For example, liking posts with one type of political viewpoint repeatedly could suggest to third parties one's political viewpoints. If such data is collected in masses, it can also determine how different groups in a population vote *(The Guardian, 2018)*. However, avoiding to 'like' posts still does not prevent personal information being spent. Facebook still records its users' visited pages or videos viewed. Now, in its terms and conditions, the company highlights that users' web browsing habits will be kept confidential, but once the information is collected there is no guarantee that it will not be released to third parties.

There are a few ways in which we can prevent such privacy invasions. First of all, we can choose to block cookies on the web browsers altogether, or delete all cookies before even visiting websites. Alternatively, we can raise our privacy levels in the web browser directly by selecting the 'Private Browsing' mode (or equivalent, in different search engines). Plug-ins such as Facebook Blocker are also available to prevent sites like Facebook from tracking our surfing behaviour.

### Posting pictures online

As part of being an active social media user, we often post pictures or posts and get tagged in pictures that may be embarrassing. Posts on the internet can also remain permanent, depending on the terms and conditions, and privacy policies offered online. The concept of 'timeline' in facebook, introduced in late 2011, makes it much simpler for others to view your posts from the past *(Sileo, 2018)*. This function could expose private

matters and embarrassing situations. Employers often examine their candidates' behaviour on social media to judge their candidacy in the circumstances that they are lacking or are unsure of their behaviour. This can possibly negatively affect the outcome of the candidate's application. In order to prevent this, they can untag themselves by clicking on the remove option on posts, or in general, choose to review posts before they appear on their 'timeline'.

**Associations with third parties**

Third party applications available through social media include online quizzes and games but also communication apps like Skype *(Sileo, 2018)*. These applications are made available through social media, however, they are created by other companies. Usually, these applications are free of cost and as a result, very tempting to social media users. However, we often fail to realise that these companies generate revenue by harvesting and processing our personal information from their respective social media pages and then selling that information to advertisers. As a result, the price we pay for enjoying these services is our personal data. Many apps collect simple information that we have available public anyway, however some apps can dive deep into our profiles to indulge on information that we had even declared private. In addition, there have been cases where personal information has been dug up from users' friends' profiles.This was in fact the case in the Facebook Cambridge Analytica Scandal. Social webpages are social by nature, as a result, thus we cannot stop them from sharing information with each other, however, what information they share is in our hands.

**Confidential details**

Some types of information should be kept as confidential as possible, and if possible, should not be shared at all. Information such as health and financial data are prime examples. Often times, instead of filling up confidential personal information such as credit card details and entering passwords, users click the "remember me" button, which allows the website cookies to store this highly personal information. We should also prevent or even limit the use of numbers like social security or passport numbers, confidential student or health data, avoid spam emails and manage accounts through strong passwords *(Cohen, 2016*). Even posting our own location or others' location can invite harassment, stalking and burglary. Details that may seem unimportant such as birthday, job and names or friends and family could potentially be used to send phishing emails. This is more specifically known as spear phishing; the e-mail appears to be from a known individual or a company, making it seem legitimate, however, it invites the user to click on links/ attachment that contain malware or to enter in more confidential details

*(Almanac.upenn.edu., 2018)*. Thus, it is important that we can differentiate between the day-to-day emails and phishing emails.

## Terms And Conditions

Before downloading any applications or using any social media networks, we are required to accept the terms and conditions. However, these terms are usually a few pages long, and less than 1% of us really end up reading all of it. People, on average, only spend approximately 29 seconds before they end up ticking the terms and conditions box *(Luger, Moran and Rodden, 2013)*. While this is a concern, it is definitely not a surprise as these conditions are not only awfully long but also highly complex.

### Meaningful Informed Consent

The requirement for informed consent cannot be disregarded for four main reasons: firstly, it allows people to express approval or disapproval of the purpose of gathering personal information. Secondly, it should be used by people so that they can effectively protect themselves from all the possible ways their data can be misused and cause them further harm. It allows the users to be the judge of what information they make available and lastly, it establishes trust between the user and the provider, by involving them in making decisions about the use of their data.

Amongst several studies done by researchers to examine the complexity of terms and conditions, is a study done by University of Nottingham, in which researchers observed numerous supplier terms and conditions, to reach to the conclusion that they are far beyond the literacy level of an average adult. The complexity of the privacy statements was relative to a ‘SMOG grade’, a measure of the mean years of schooling required to understand a piece of text. These grades were calculated for terms and conditions of some Energy Services and were found to be equivalent to that of the works of Shakespeare *(Luger, Moran and Rodden, 2013)*.

According to the Information Commissioner's office, a number of techniques can be implemented to ensure the terms and conditions are clear, concise and comprehensible: layering, dashboards, just-in-time notices, and icons *(Ico.org.uk, 2019)*. The layered approach is providing people with a short notice containing key information about the organization and how it uses personal data. It may contain links to expand on each section, which may contain even more links for further details.This is very helpful in the way that it allows focus on the most relevant information that alerts the reader right away, while more complex and specific information can be accessed

through further links. A dashboard is a tool that allows individuals to manage what is happening to their personal data. It allows them to change settings and agree to the particular processing or sharing of their data. It directly complies with the GDPR rule that terms and conditions must be just as easy to withdraw from than they are to accept. The just-in-time notice appears when individuals provide companies with a particular piece of information; it provides a brief explanation of how the information will be used. Icons can be used in such a way that when one enters his/her personal information, and hovers over the icon, it reveals what the data will be used for.

## Conclusion

We use social media to share moments with our closed ones, our opinions, interests and hobbies but often fail to realise the harsh consequences of sharing excessive, sensitive or even simple information *(Almanac.upenn.edu., 2018)*. The underlying factor for these problems is human psychology. We are not forced to press the ‘like’ button or post our views. We give our consent to the use of our data, enthusiastically but ill-informed. Legislations like the GDPR have developed to force terms and conditions to be simplified and made clear to use. Yet, studies that analyse these terms and conditions statements come to a conclusion that they are quite complex and most users lack sufficient understanding of the privacy statements.Terms and conditions should be standardized altogether for all companies, which should individually install techniques, as suggested by the ICO, to better elicit meaningful consent from users.

# References


Almanac.upenn.edu. (2018). *12/08/15, One Step Ahead: TMI: The Risks of Sharing Too Much Information on Social Media - Almanac, Vol. 62, No. 16*. [online] Available at: https://almanac.upenn.edu/archive/volumes/v62/n16/osa.html (Accessed 13 Dec. 2018).

Cohen, S. (2016). *Privacy Risk with Social Media*. [online] HuffPost. Available at: https://www.huffingtonpost.com/sam-cohen/privacy-risk-with-social-_b_13006700.html (Accessed 4 Jan. 2019).

Hern, A. and Pegg, D. (2018). *Facebook fined for data breaches in Cambridge Analytica scandal*. [online] the Guardian. Available at: https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal (Accessed 4 Jan. 2019).

Ico.org.uk. (2019). *How should we provide privacy information to individuals?* [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/how-should-we-provide-privacy-information-to-individuals/ (Accessed 4 Jan. 2019).

Luger, E., Moran, S. and Rodden, T. (2013). *Consent for All: Revealing the Hidden Complexity of Terms and Conditions*. [online] ACM Digital Library. Available at: https://www.researchgate.net/publication/258403459_Consent_for_All_Revealing_the_Hidden_Complexity_of_Terms_and_Conditions (Accessed 13 Dec. 2018)

Sileo, J. (2018). *6 Ways Your Facebook Privacy Is Compromised | Sileo Group*. [online] Sileo.com.

https://www.sileo.com/six-ways-your-facebook-privacy-is-being-compromised/ (Accessed 13 Dec. 2018).

Statista. (2018). *Facebook users worldwide 2018* | *Statista*. [online] Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Accessed 6 Jan. 2019).

The Guardian. (2018). *Internet privacy: At every turn, our privacy is compromised by technology* | *Observer editorial*. [online] https://www.theguardian.com/commentisfree/2011/may/01/observer-editorial-internet-privacy (Accessed 6 Jan. 2018).

# Bibliography

Gleibs, I. (2015). *The importance of informed consent in social media research*. [online] Impact of Social Sciences. Available at: http://blogs.lse.ac.uk/impactofsocialsciences/2015/03/27/the-importance-of-informed-consent-in-social-media-research/ (Accessed 13 Dec. 2018).

Houghton, D. and Joinson, A. (2010). *Privacy, Social Network Sites, and Social Relations*. [online] Tandfonline.com. Available at: https://www.tandfonline.com/doi/full/10.1080/15228831003770775 (Accessed Jan. 2019).

Lanterman, M. (2017). *Personal Information and Social Media: What Not To Post | Expert Commentary | IRMI.com*. [online] Irmi.com. Available at: https://www.irmi.com/articles/expert-commentary/personal-info-and-social-media (Accessed 6 Jan. 2019).

The Guardian. (2018). *The Guardian view on internet privacy: it's the psychology, stupid | Editorial*. [online] https://www.theguardian.com/global/commentisfree/2018/feb/08/the-guardian-view-on-internet-privacy-its-the-psychology-stupid (Accessed 13 Dec. 2018).

The Interaction Design Foundation. (2018). *What is Human-Computer Interaction (HCI)?*. [online] https://www.interaction-design.org/literature/topics/human-computer-interaction (Accessed 13 Dec. 2018).

**Statement of Originality**

- I have read and understood the ECS Academic Integrity information and the University's Academic Integrity Guidance for Students.
- I am aware that failure to act in accordance with the Regulations Governing Academic Integrity may lead to the imposition of penalties which, for the most serious cases, may include termination of programme.
- I consent to the University copying and distributing any or all of my work in any form and using third parties (who may be based outside the EU/EEA) to verify whether my work contains plagiarised material, and for quality assurance purposes.

***You must change the statements in the boxes if you do not agree with them.***

We expect you to acknowledge all sources of information (e.g. ideas, algorithms, data) using citations. You must also put quotation marks around any sections of text that you have copied without paraphrasing. If any figures or tables have been taken or modified from another source, you must explain this in the caption and cite the original source.

**I have acknowledged all sources, and identified any content taken from elsewhere.**

If you have used any code (e.g. open-source code), reference designs, or similar resources that have been produced by anyone else, you must list them in the box below. In the report, you must explain what was used and how it relates to the work you have done.

**I have used a resource produced by someone else. It is the technical report template, as we were meant to adhere to it.**

You can consult with module teaching staff/demonstrators, but you should not show anyone else your work (this includes uploading your work to publicly-accessible repositories e.g. Github, unless expressly permitted by the module leader), or help them to do theirs. For individual assignments, we expect you to work on your own. For group assignments, we expect that you work only with your allocated group. You must get permission in writing from the module teaching staff before you seek outside assistance, e.g. a proofreading service, and declare it here.

**I did all the work myself, or with my allocated group, and have not helped anyone else.**

We expect that you have not fabricated, modified or distorted any data, evidence, references, experimental results, or other material used or presented in the report. You must clearly describe your experiments and how the results were obtained, and include all data, source code and/or designs (either in the report, or submitted as a separate file) so that your results could be reproduced.

**The material in the report is genuine, and I have included all my data/code/designs.**

We expect that you have not previously submitted any part of this work for another assessment. You must get permission in writing from the module teaching staff before re-using any of your previously submitted work for this assessment.

**I have not submitted any part of this work for another assessment.**

If your work involved research/studies (including surveys) on human participants, their cells or data, or on animals, you must have been granted ethical approval before the work was carried out, and any experiments must have followed these requirements. You must give details of this in the report, and list the ethical approval reference number(s) in the box below.

**My work did not involve human participants, their cells or data, or animals.**