Psychological and Behavioural Science

Personal data protection online.

Geary Hayley
Neervoort Lara
Turkenitch Roni

London School of Economics and Political Science
PB403 Psychology of Economic Life
Summative coursework
December 2018

Course convenors: Dr. Fred Basso & Prof. Saadi Lahlou
Other teachers: Dr. Kate Laffan, Mr. Maxi Heitmayer

Table of Contents

1. Background Information

1.a.) Defining Data Privacy

To gain a full understanding of psychological mechanisms behind the use of Facebook, the distribution of personal data within the platform, and negative consequences that may arise from such behaviour, it is necessary to explicitly define 'online data privacy' as a concept. Within this essay, violations of privacy extend beyond newsworthy data leaks, privacy scandals, and identity theft, which are later discussed. Data privacy in this instance concerns the fine line between privately and publicly available personal information and how such information is used by third parties. Within this essay, ethical issues regarding the triangulation of demographic information and browser history by Facebook and advertisers will be considered concerning consumer exploitation and manipulation through targeted advertising. Individuals share data on Facebook to connect with others, rather than generating a source of revenue and supporting the platform, as Facebook sells data to third parties. Facebook currently has a protective role in the storage of sensitive personal information individuals provide the platform with, however, in exploiting and capitalising on this breaches of trust are incurred.

1.b.) Facebook and the issue of Data Privacy

Facebook as a centralized entity, potentially has a complete control over the content that its users are consuming. Therefore, Facebook can control the way their users think and even more than that, the way they act. In the way that Facebook operates, requiring data from the users as a payment to use the platform, they can manipulate user's behaviour more easily. If Facebook wants certain users to make a certain decision they can "nudge" them to do so with the previous data they have. For instance, if Facebook wants overweight users to make healthier choices they can easily manipulate them by addressing them healthier content over their profiles. Moreover, Facebook is a goldmine for identity thefts, because there are a few methods by which identities can be stolen and private data is on the stake. Although Facebook is putting in a lot of effort to prevent these privacy violations, it is still a huge threat that many users that are not aware of it, and a lot of privacy scandals have occurred in the past that will be outlined in the following section.

1.c.) Privacy scandals involving Facebook

The implementation of Facebook's multi-sided business model and thereby the commodification of personal user data has led to numerous privacy scandals for Facebook (Fiegermann, 2018). In the spring of 2018, it was revealed that Facebook allowed the data of more than 87 million users to be utilized by the British-American political data mining firm Cambridge Analytica. The company had Facebook users take personality quizzes so one could learn more about their big five personality traits, without knowing that this data would be used for political persuasion purposes (Isaak, & Hanna, 2018). What is even more worrying is that not only the data of the users that took the personality test was used but also the personal data of their Facebook friends (Isaak, & Hannah, 2018). This data was in turn utilised to build a very specific personality profile of over 87 million users, which facilitated the development of very specifically targeted advertisements for Donald Trump's 2016 Presidential Election campaign (Isaak, & Hanna, 2018). It was later revealed that Cambridge Analytica did not only implement this user data for the Trump campaign but also had ties to the Brexit Leave campaign (Cadwalladr, & Townsend, 2018).

Following the Cambridge Analytica scandal, Facebook's reputation majorly suffered. Mark Zuckerberg, Facebook's CEO, was required to testify in both the U.S. Senate and the European Parliament "to clarify the issues related to the use of personal data" (Salinas, 2018). Facebook experienced "the biggest ever one-day drop in a company's market value, falling from a record high of $619bn on Wednesday to just $501bn in early trading on Thursday" (Solon, 2018). In October 2018, Facebook was fined £500,000 by the Information Commissioner's Office in the UK as a result of the Cambridge Analytica scandal because of allowing third parties to make use of user data without sufficient consent and failing to be transparent about how data was harvested by third parties (Waterson, 2018).

This has not been the only privacy scandal that has involved Facebook within the past year (Fiegermann, 2018). In September 2017, the news that Facebook allowed Russians to meddle in the U.S. Election campaign using targeted advertising, "a foreign scheme to commit election fraud in the United States" for which 13 Russians and three companies were prosecuted, severely damaged their reputation (Frenkel, & Benner, 2018). Facebook knew of the suspicious Russian activity to disrupt the 2016 U.S. elections for a year already before the news came out, but kept it private to try and save its reputation (Frenkel, Confessore, Kang, Rosenberg, & Nicas, 2018). In November 2018, a New York Times' investigation into how Facebook handled these multiple privacy crises (Frenkel, Confessore, Kang, Rosenberg, & Nicas, 2018) led to

media uproar and demands for role changes in the board of Facebook, which forced Mark Zuckerberg to defend his company to the press (Fiegermann, 2018). This further highlights the major detriment that Facebook experienced due to these recent privacy scandals, and emphasizes the importance for the company to work with different parties on a new solution for the way they handle user data. This solution will be proposed after carefully examining the issue of data privacy on Facebook with the relevant psychological and economic theories.

2. Introduction

Throughout the last decade, social media platforms have become increasingly ingrained with in our personal lives, influencing the ways in which we communicate with others, with average users spending over two hours per day on social networking sites (Statista, 2018a). Users engage with social networks for multiple reasons, including entertainment, passing time, self-expression, and self-documentation (Alhabash, & Ma, 2017). The most used social media platform is Facebook, which currently has 2.23 billion active users and was the first platform to surpass one billion registered accounts (Statista, 2018b). This essay will review the societal issue of online data protection on social media, and will focus specifically on Facebook because this social medium has the largest number of global users (Statista, 2018b) and has currently experienced multiple privacy scandals that have influenced both their reputation and stock price (Isaak, & Hannah, 2018; Solon, 2018).

Starting off as a Harvard dorm-room initiative to rate the attractiveness of fellow students, Facebook quickly developed into a multi-billion dollar business, with main sources of revenue coming from selling user data to advertisers that create personalized advertising (Esteve, 2017). In 2017, Facebook earned 39.9 billion dollars through targeted advertising by selling the data of its users to third parties and advertisers (Statista, 2018c). The platform routinely collects vast amounts of consumer data, ranging from purchase and search history to demographic information and personality characteristics (Belu, 2017). Up until 2015, Facebook had already collected 300 petabytes (one petabyte = 1.000.000 gigabytes) of personal data, which is "a hundred times the amount the Library of Congress has collected in over 200 years" (Zyskind, & Nathan, 2015).

One issue that quickly becomes apparent with this mass collection of personal data is the lack of transparency as Facebook does not disclose specifically what data is collected, how this is used and who has access to it. We do know that with the petabytes of data, a very specific profile is built of every user that can predict purchasing and consumption behaviour, which can then be used by advertisers to tailor their advertisements very specifically at certain users (Isaak, & Hannah, 2018). Facebook even collects data of people that do not have a Facebook account by creating shadow profiles using their browsing history and their friends' information (Wagner, 2018).

"Create an account - It's free and always will be." is stated on Facebook's homepage. Consumers are made aware that Facebook requires no monetary input, but are unaware that

they are actually paying for the use of the social media through a different type of currency - their personal data (Srnicek, 2017). The lack of transparency is further illustrated as users are commonly unaware of the uses of their personal data by third parties. For instance, "most users, who are focused on their social experiences in the online environment, are likely to remain largely uninformed about the nature and extent of commercial surveillance on social networking platforms" (Montgomery, 2015, p. 779). Not only is this lack of transparency problematic, the routine collection of consumer data poses additional ethical issues, including the potential manipulation of behavior online, and threats to personal security and privacy (Srnicek, 2017).

3. Multi-sided platforms

In gaining a comprehensive understanding of the issues that arise from data privacy on Facebook or the lack thereof, the business model in which the buying and selling of personal data occurs will be discussed. Facebook implements a 'multi-sided business model', which capitalises on interactions and transactions between the users, the platform and the advertisers by coordinating the needs and wants of various parties within one framework (Evans, 2003).

Multi-sided platforms (MSPs) allow for the conversion of currencies between various stakeholders, altering the ways in which individuals consume information and communicate with others compared to real-life interactions offline (Evans, 2003). The interdependence between multiple groups of customers within MSPs facilitates the transformation of currencies and enables the monetisation of such currencies dependent on the goals of the groups (Boudreau, & Hagiu, 2009).

Despite the benefits for multiple parties, consequences often arise that are particularly salient for individual users based on their activity within MSPs. To participate in various digital activities, assumptions regarding the rationality in which individuals managed and distributed their personal data were made in the past (Posner, 1981). Prior to the development of Facebook, behaviour regarding information protection and privacy was assumed to be similar on- and offline. However, such failures to account for the irrationality of consumer behaviour are now widely accepted on and offline, providing explanations for the vast amount of personal data individuals distribute online (Simonson, & Tversky, 1992). As Lilley, Gordzinsky, & Gumbus (2012) report investigating opinions of Facebook's targeted advertising and data collection practices: 'many respondents were found to be relatively uneducated and passive prosumers, and those expressing a high concern for privacy were no exception.' Subsequently, Facebook

operates profitably as a multi-sided platform, leveraging personal user data while doing so with a lack of transparency towards its users.

As we have seen in the background section regarding privacy scandals, the issue of data protection is not only important for individual users, but also very important for the organization of Facebook. As was outlined, past privacy scandals have lead to a hurt in reputation, enormous drops in stock and even fines for the company (Isaak, & Hanna, 2018; Solon, 2018). This emphasizes the importance for the company to work with different parties on a new solution for the way they handle user data. Therefore, in the next section, we will examine the different stakeholders involved in this issue in order to be able to come up with a sustainable solution.

4. Stakeholder analysis

It is important to analyze the different stakeholders with the perspective of how they relate to the personal data protection problem on Facebook. We will refer back to the different stakeholders throughout the analysis of the problem as well as in our solutions.

Stakeholders		**Role**	**Motivation**
Facebook		Attracting and retaining users while selling their data to third parties	Gaining users and making profit from their personal data by selling it to third parties
Users	Citizens - Shadow Profiles	Individuals that do not have a Facebook profile are (passively) involved, as Facebook builds shadow profiles using their browsing information and their Facebook friends' information (Wagner, 2018)	Limiting Facebook's invasion of their privacy as there was no explicit agreement to terms and conditions of data collection
	Passive Users	Generating capital for Facebook by providing personal data through creating an account and engaging in passive activity on Facebook E.g. Scrolling through feed, liking pictures of their friends etc. (Gerson, Plagnol & Corr, 2017)	Using Facebook for entertainment and passing time (Alhabash & Ma, 2017)
	Active Users	Generating the same source of capital for Facebook as passive users. They are more valuable for Facebook because they additionally actively share posts and pictures online (Gerson, Plagnol & Corr, 2017)	Using Facebook for entertainment and passing time, but also for self-expression and self-documentation (Alhabash & Ma, 2017)
Advertisers		Mass purchasing of personal data from Facebook and implementing highly personalized ads based on this data	Increasing sales by enhancing the specificity of targeted advertising

Government	Creating legislation to hold organisations responsible for personal data collection and possession (General Data Protection Regulation)	Protecting the citizens Protecting the right for privacy
Browsers	Supporting the structure of Facebook, search engines and their data traffic	Making profit and creating brand awareness
Designers	Designing interfaces, material, content and the user experience and influencing how users act on the platform	Making online content and platforms attractive and user-friendly for multiple parties

5. Application of Theory to Data Protection Problem

Installation Theory

Installation Theory (Lahlou, 2017) provides a general framework to analyse and alter current data usage and protection practices on Facebook. Installations are mechanisms through which behaviour is enabled and scaffolded. They can be managed and redefined to facilitate and promote behaviours that the installation directs. Within this, three layers place constraints on behaviour, including The Objective Material Environment, The Embodied Interpretive System, and Social Regulation. This three-fold combination further constraints behaviour, creating a channelling system, which reliably alters behaviour. Within the following discussion, this multilevel model will be used to analyse problems surrounding data protection and usage on Facebook and applied to a discussion of a short-term solution to encourage users to protect individual data. Additionally, various behavioural, social and psychological theories shown to reliably predict and explain behaviour are discussed within the framework of the layers of Installation Theory.

6. Problem Analysis

6.a.) Layer 1 – The Objective Material Environment

The first layer within Installation Theory is the Objective Material Environment, which encompasses physical objects within an individual's immediate surroundings. Such objects are 'constructed artefacts…made with a deliberate intention' (Lahlou, 2017), supporting and constraining certain behaviours. Facebook's physical structure facilitates personal data sharing in exchange for unrestricted access and use of the platform (Burke, Marlow, & Lento, 2009). When initially creating a profile, contact details, birthday, gender and name are required for a basic account. This immediately limits choice regarding the disclosure of personal information. Through this affordance, Facebook has prompted millions of users to adopt data sharing behaviours when using the platform (Fogg, & Iizawa, 2008). Additionally, Facebook generates visible reminders of missing information, encouraging user completion. Furthermore, default options on Facebook promote data sharing (Acquisti, & Gross, 2006), which are subject to little change as people rarely alter set options (Thaler, & Sunstein, 2003). For instance, privacy settings automatically allow Facebook 'friends' and their 'mutual friends' to view information on your timeline.

Through additional physical affordances, Facebook's interface creates barriers discouraging personal privacy updates. Facebook has 'the incentive to keep security and access controls weak by design in order to encourage information exchange and increase their company's value to advertisers' (Wilson, Gosling, & Graham, 2012). For instance, immediate access to privacy settings is not salient to the user, requiring additional action to change security preferences. Subsequently, little action is taken by users, with research indicating that 36% remain on default privacy settings, and 37% expose more information than they report intending to (Liu, Gummadi, Krishnamurthy, & Mislove, 2011). Furthermore, research indicates that users on social media are both unable and unwilling to successfully manage their data sharing settings (Madejski, Johnson, & Bellovin, 2012).

The lack of transparency of data protection within the objective material layer may lead to the alienation of personal data online. Alienation describes the processes by which individuals no longer regard a possession as their own (Marx, 1844), creating feelings of powerlessness in relation to the object (Seeman, 1959). Consequently, users are less inclined to take action monitoring and protecting their Facebook data. Alienation from personal data may be amplified through close relationships between third parties and Facebook. Commonly, 'Single Sign-On' schemes require individuals to provide Facebook data to access other applications and websites

(Wang, Chen, & Wang, 2012), enabling data sharing across organisations. Access is fully restricted if individuals fail to provide information, further limiting control. Additionally, recent mergers with Whatsapp and Instagram has allowed Facebook to gain a more complete profile of users to sell onto third parties (Porter, 2018).

6.b.) Layer 2 – The Embodied Interpretive System

Beyond Facebook's physical affordances that promote personal data sharing, additional determinants of individuals' behaviour exist within the online platform. The embodied interpretive system is the second layer within Installation Theory. This encompasses all mechanisms internal to the body that direct behaviour, including; reflexes, knowledge, representations etc. (Lahlou, 2017). Such mechanisms are biologically present, culturally acquired, or the product of life experiences. Embodied interpretive systems connect perceptions of the situation with appropriate actions. For instance, many Facebook users do not often consider the consequences of putting large amounts of personal information online (Thatcher, 2014; Marwick, 2016). One way this can be understood is through the recent commodification and commoditisation of online data (Lupton, 2014), a concept linked to alienation. Inherently, online data has no value and is not shared online for the purpose of being sold to third parties. Economic value is generated through MSP's that involve numerous stakeholders, including Facebook, advertisers, and users (Boudreau, & Hagiu, 2009). The process of consuming content from Facebook is disconnected from the production of economic value from data, leading users to neglect risks of sharing information in public spheres.

Each layer within Installation Theory provides feedback and feedforward for particular behaviours, which either inhibits or promotes future action. Within the embodied interpretive layer much behaviour is automatic (Lahlou, 2017). For instance, much Facebook use is habitual (Vishwanath, 2014). Sharing personal information by posting a picture provides immediate positive reinforcement through attention from other users, encouraging the repetition of this behaviour (Quan-Haase, & Young, 2010), which over time becomes habitual. Habits are additionally seen in passive users on Facebook, who are reinforced through notifications of others' activity, promoting habitual checking of the site. Consequently, individuals continue sharing data and using Facebook without considering risks involved. In contrast, data distribution may additionally be a product of hyperbolic discounting in which the consequences of privacy breaches are not immediate. This is seen for behaviours including unhealthy eating (Barlow, Reeves, McKee, Galea, & Stuckler, 2016), smoking (Odum, Madden, & Bickel,

2002), and a lack of exercise (Scharff, 2009), suggesting that hyperbolic discounting can be generalised to data sharing behaviours on Facebook.

A combination of additional cognitive biases may provide explanations as to why individuals frequently share personal information on Facebook. One such bias is information avoidance, where individuals persistently share information on Facebook despite having privacy concerns (Lahlou, 2008). Research suggests that this behaviour is motivated by a need to reduce cognitive dissonance arising from this behaviour-intention inconsistency (Akerlof, & Dickens, 1982; Golman, Hagmann, & Loewenstein, 2017). Less effort is required to modify views of data sharing risks compared to altering behaviour towards changing privacy settings on Facebook. This phenomenon can additionally be explained through the 'privacy paradox.' Despite reported privacy concerns, individuals share vast amounts of personal information, creating a 'paradoxical dichotomy between attitudes and behaviour' (Kokolakis, 2017).

6.c.) Layer 3 – Social Regulation

Embodied knowledge and physical affordances of Facebook are not enough to regulate and promote most user behaviour on Facebook- both active and passive. The final layer within Installation Theory is social regulation (Lahlou, 2017) - the main explanation for Facebook use. The network effect is arguably the primary factor contributing to the current and continued use of Facebook despite growing privacy concerns and scandals (Shapiro, Varian, & Becker, 1999). This demonstrates the cyclical nature of online social media networks guided by social regulation factors, including the formation and maintenance of human capital (Ellison, Steinfield, & Lampe, 2007). On Facebook, each citizen that joins and regularly uses Facebook creates increasing value to other users (Shapiro, Varian, & Becker, 1999). Within MSPs, indirect network effects are present. The growth in one user group enhances the value of the platform for another group. For instance, the growth in Facebook users increases the value of the platform for advertisers (Johnson, 2018). As the platform becomes more valuable for advertisers and users, a 'lock-in' effect is generated, making complete abstinence or transference to another system more difficult (Barnes, Gartland, & Stack, 2004). This facilitates the growth and maintenance of Facebook, creating larger incentives for sustained use and reducing the number of individuals leaving the platform (Johnson, 2018).

Much research considering social media engagement examines the 'fear of missing out' (Beyens, Frison, & Eggermont, 2016; Przybylski, Murayama, DeHaan, & Gladwell, 2013). This indicates that the consistent use of Facebook is promoted by a fear of loss rather than the

anticipation of reward, suggesting that loss aversion may play a role in the maintenance of Facebook behaviours through social regulation (Tversky, & Kahneman, 1991). The pervasiveness of Facebook use extends beyond online behaviours to missing face-to-face interactions as much event planning is facilitated through Facebook. Research suggests that this demand to be present on and offline influences protection online. Information is not deleted from personal profiles when individuals develop concerns over privacy, only particular privacy settings on Facebook are altered (Tufekci, 2008).

7. Short-term solution: Pro-TECH-t

A comprehensive and targeted solution is necessary to reduce harmful data collection practices and increase proactive privacy behaviours on Facebook. Our primary recommendation is aimed at users. Returning to the stakeholder analysis, both passive and active users facilitate exchanges between Facebook, advertisers, browsers, designers and subsequently citizens. In adopting a bottom-up approach, cumulative changes in data sharing behaviours will subsequently alter interactions between other stakeholders. Third parties would then have to alter data collection, commodification and distribution practices to remain competitive in the market, reducing many current privacy issues. Additionally, a user-based recommendation fits cost-effectively within the threefold structure of Installation Theory compared to large-scale government initiatives or interventions aimed at Facebook. An effective installation 'closely supports and monitors the desired activity at every step' (Lahlou, 2017). Such 'steps' are implemented within all three layers simultaneously to successfully guide behaviour to reach the desired result. The following discussion will describe this recommendation within each layer and discuss how various features will result in behavioural changes in data protection on Facebook.

This recommendation will be introduced via web browsers as an add-on application called 'pro-TECH-t'. Pro-TECH-t will utilise an algorithm for analysing browsing patterns, which determines users' activity on Facebook. A notification will appear prompting immediate response when individuals are using Facebook for 'passing time' (Alhabash, & Ma, 2017). This prevents frustration if users are on Facebook for a particular reason as the notification may disrupt their sequence of actions. Additionally, the irregularity of the notification will reduce overexposure to information, which overwhelms individuals and often produces less reliable behaviour changes (Lam, DeRue, Karam, & Hollenbeck, 2011). Displayed within this notification is a summary of what personal information Facebook possesses, which organisations external to Facebook are using it, what they are using it for, and examples of

what this information may be used for in the future (*See Figure 1)*. Based on the volume of personal data individuals have on Facebook, pro-TECH-*t* will value the data and give estimates of the profit Facebook is earning from selling this data, and the possible profit advertisers and retails may make through targeted advertising. Succeeding this summary and data valuation, a choice between three tiers, ranging from 'Restricted Access' to 'Unrestricted Access', will appear within the pro-TECH-t notification window (*See Figure 2 and 3*). This system will provide individuals with a trade-off between, 1) granting Facebook access to varying amounts of their personal data, and 2) having some features within the platform restricted. For instance, the restricted access tier allows Facebook access to basic demographic information, but in turn, the user can only perform limited functions within the platform. This will provide an incentive for both Facebook to cooperate and users to participate as trade-offs promote Facebook use and privacy considerations. Additionally, users can choose to opt out of targeted advertising for organisations that possess their data. Individuals will still receive advertisements, but they will not be targeted. This technology, which is currently implemented within many browsers provides individuals with privacy options and does not prevent organisations from marketing products.

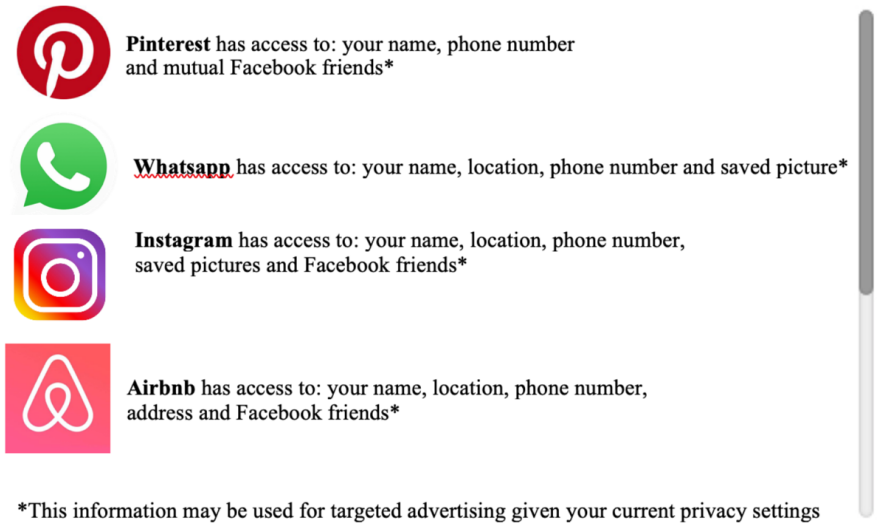

Figure 1: Third parties with access to what personal data through Facebook

Figure 2: Three-tier system interface of pro-TECH-t

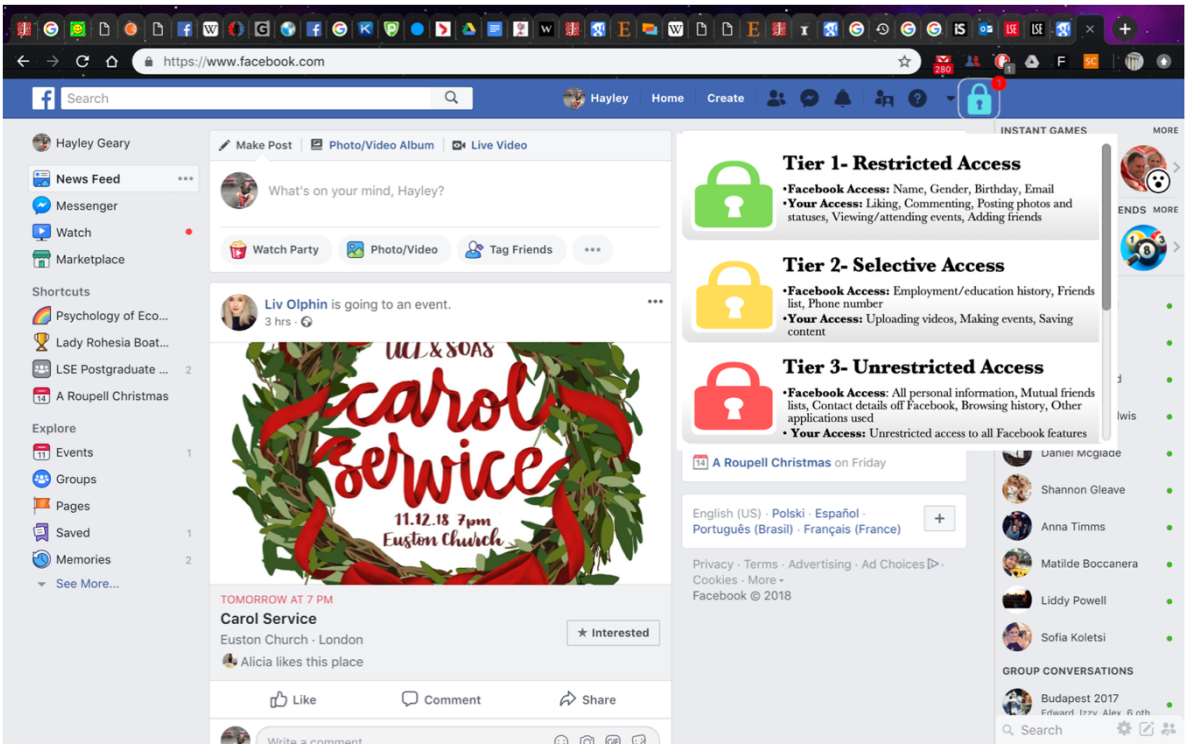

Figure 3: Example of tier system pop-up on Facebook

7.a.) Layer 1 - The Objective Material Environment

As discussed, the physical design of Facebook facilitates data sharing practices. The implementation of pro-TECH-t within browsers will alter the objective material layer in which Facebook operates, promoting data protection behaviours. This 'app' generates frequent visual reminders to update privacy settings, which enhances the salience of the issue. Increasing the salience of required action has shown to reduce the intention-behaviour gap, in which many intentions are not acted upon (Hagger, & Luszczynska, 2014; Dolan et al., 2012). As discussed, information about the harms personal data distribution may cause is largely avoided leading to cognitive dissonance through a lack of protective action. Pro-TECH-t involves fewer steps in altering privacy preferences compared to the cognitively complex sequence of actions Facebook currently requires, suggesting people will be more likely to act (Gigerenzer, & Hoffrage, 1995). This may additionally reduce feelings of cognitive dissonance as more individuals actively engage in changing privacy settings compared to passively changing their attitudes towards protection (Festinger, 1962). Furthermore, the transparency of data treatment by Facebook and other organisations is enhanced through pro-TECH-t, as alternative uses by third parties are explicitly reported. This provides incentives for organisations as transparency is linked to consumer trust within many industries (Bhaduri, & Ha-Brookshire, 2011). A similar attempt has recently been made by the Digital Advertising Alliance of Canada, with predictions to significantly enhance consumer trust (Synqrinus, 2017).

7.b.) Layer 2 - The Embodied Interpretive System

Behaviour change interventions that are implemented through altering physical installations in the objective material layer will be enhanced through simultaneous intervention in the embodied interpretive layer. Pro-TECH-t will additionally change embodied competences regarding the appropriate actions to take when using Facebook can be altered. Within the three-tier system, the second tier 'Selective Access' will be the default option automatically selected for participants. A wealth of research suggests that few individuals choose an alternative choice given the additional effort required (Thaler, & Sunstein, 2003; Halpern, Ubel, & Asch, 2007; Kahneman, Knetsch, & Thaler, 1991). The default option will provide users with enhanced data protection compared to current default privacy settings on Facebook, whilst not significantly limiting Facebook's access to user data, remaining profitable if sold. Additionally, the pop-up restricts choice between three tiers to reduce the impacts of bounded rationality. Research has shown that given limited cognitive processes, users may struggle to choose between many options with varying different trade-offs, often leading to no option chosen at all (Iyengar, & Lepper, 2000).

7.c.) Layer 3 - Social Regulation

The impact social regulation has on promoting particular behaviours on Facebook is well-established (Moore, & McElroy, 2012). In considering such factors, pro-TECH-t can generate and capitalise on collective action by establishing behavioural norms. When selecting access tiers, users will be confronted with how many of their Facebook friends are both using pro-TECH-t and the number of individuals who have selected each tier. Many behavioural change interventions have made comparisons between personal behaviour and average group behaviour to promote change (Midden, Meter, Weenig, & Zieverink, 1983). The influence of group social regulation has larger impacts over appeals made to individuals due to the influence of descriptive norms (Cialdini, 2007; Gerber, & Rogers, 2009). Furthermore, cumulative group effects to change behaviour can be altered by establishing perceptions of the risk of data protection issues in groups (Van Der Pligt, 1998). Research indicates amplification of risk in group settings, whereby perceptions of danger are heightened in group situations compared to individual perceptions of risk (Kasperson et al., 1988). In creating a sense of urgency regarding personal data on Facebook, a cumulative response may be effective in promoting behaviour change.

7.d.) Short-Term Limitations

A limitation to our short-term solution might be that permission from Facebook is necessary to construct add-on applications on Facebook's Application Programming Interface (API's). API's allow efficient coordination between multiple applications, in this instance pro-TECH-t and Facebook. Incentivising Facebook is dependent on their concerns for reputation by implementing extra data protection. Considering recent declines in stock prices and news coverage of privacy scandals, Facebook recognises that self-regulation of data protection is limited, creating a new type of stakeholder - data protectors such as pro-TECH-t. Existing 'protectors' operate externally to Facebook whereas pro-TECH-t will operate in conjunction with the platform, suggesting higher success. Facebook may recognise potentially monetary and social advantages of employing external organisations for data protection, gaining user trust.

8. Long-term solution

Despite the comprehensive application of Installation Theory in an attempt to alter data sharing behaviours on Facebook, pro-TECH-t only offers a short-term solution that ultimately does not prevent personal data from becoming publicly available. A short-term solution is however

essential as the development of and moving to a longer, more sustainable solution may take time. Without immediate action, the problem may become much larger. Currently, the multi-sided platform in which Facebook operates encourages the commoditisation and commodification of user data between numerous stakeholders. Facebook and third parties routinely over-collect and under protect individuals' data, creating unsafe, online environments and ethical dilemmas. Large-scale interventions including the EU General Data Protection Regulation (GDPR), information campaigns and the above solution encourage self-protection. However, data privacy is still a pervasive issue because Facebook's main source of income is based on collecting petabytes of personal data (Zyskind, & Nathan, 2015). A solution to reduce this impact requires a globalised switch to decentralised social media networks, which will be discussed below as a long-term solution to data protection.

An emerging technology that may provide an alternative social network platform without the aforementioned data privacy issues is Blockchain, as this operates external to MSPs. This decentralised data management technology, with recent uses including Bitcoin in 2008. Bitcoin is a peer-to-peer electronic payment system, used as a global currency without institutional involvement (Nakamoto, 2008). Considering various ethical limitations of currency transactions within the MSP, this model will be replaced by a decentralised social network, eliminating the middleman, in this instance Facebook. This new model will enable the same features and services as the multi-sided business model in a less intrusive way, with enhanced security. Blockchain has a unique method of data storage, in which user data is kept in an encrypted and transparent way on every node on the network (Zyskind, & Nathan 2015). In turn, it is mathematically impossible to compromise data within the network, in contrast with centralized networks, which employ few storage entities exposed to a single point of failure attack (Zyskind, & Nathan 2015).

Central features of Blockchain technology make the transfer of digital property, including personal data, transparent and secure (Puthal, Malik, Mohanty, Kougianos, & Yang, 2018), where users can follow and manage all personal data obtained them (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). Furthermore, through such networks, users have complete control over their data, meaning they can manage the degree to which their data is publicly available, avoiding breaches of personal security. The adoption of a social network utilising Blockchain technology would promote safer data management practices compared to Facebook and pro-TECH-t, which operate within MSPs involving multiple parties. The adoption of a new platform and reduction of the influence Facebook currently has is a slow process with much

investment needed. However, the long-term benefits may outweigh the high initial costs if particular stakeholders are appropriately involved. Browsers, for instance, bridge the gap between the raw infrastructure of the internet and the users, suggesting a need to adapt to the implementation of decentralised social networks as data transformation and storage is different.

8.a.) Long-Term limitations

When evaluating the utility of Blockchain in creating decentralised social networks, it is necessary to consider limitations as this solutions will replace one of the most powerful organisations in the world. The relationship between advertisers and users is important within this model. Without advertisers, no investment in the decentralised network will be present suggesting incentives need to remain high for the switch to occur. Rather than purchasing user data from Facebook, organisations obtain data directly from users. However, data commoditisation remains present as advertisers are still purchasing data to gain insights about consumers and creating proxy 'profiles' about them to mimic and predict purchasing behaviour. A 'reverse search engine' is suggested to combat this. For instance, a way to facilitate users actively approaching organisations, wanting certain products to be advertised to them should be considered. This prevents alternative data uses from social media platforms, in that consumer data will not be mined to later manipulate purchasing through targeted advertising. Additionally, the accumulation of personal data by third parties will be reduced as advertisers would have no use for it, eliminating the volume in which data leaks currently happen.

Secondly, similar to most new technologies, Blockchain is experiencing some issues which are surrounded by a level of controversy. Concepts such as Bitcoin, built on Blockchain has gained a negative reputation as they have been used within controversial context, including money laundering, and use on the black markets (Camber, Greenwood, 2018). However, Bitcoin is only one use of this new technology, applicable to other domains. Moreover, as the technology is new, the scalability of how many users it can support is up for debate (Zheng, Xie, Dai, Chen, & Wang, 2017). For instance, comparisons between Bitcoin and MasterCard have been made, suggesting that Blockchain technology is only able to hold 1% of the capacity that centralized networks such as MasterCard can (Lo, & Wang, 2014). Although some voices in the Blockchain industry claim it will replace the foundations of the internet as we know today (Rosenberg, 2015), evidence yet has to be supplied.

Furthermore, the network effect and resistance of Facebook to competitors needs to be considered as the MSP is Facebook's most valuable asset. The 'lock-in' effect may be a large obstacle in the adoption of the new Blockchain platform. However, again with the correct involvement of stakeholders on which Facebook depends, a switch may be possible. Additionally, Facebook currently has numerous privacy concerns and public relations issues. If Facebook, for instance, was the lead the change to decentralised networks, a global impact would be quick. Designers additionally have a crucial role in this transition. Designing the interface is essential to facilitate easy use and reduced resistance to the adoption of the new platform, with particular emphasis on the improved data safety features encompassed within the platform.

The popularity and use of decentralized social networks are growing. However, they occupy a small niche, and only decentralized substitutions for particular types of social networks including Twitter and Instagram exist, with nothing similar to Facebook as numerous features are included within this platform. Moreover, social networks are rapidly changing, meaning predictions for future use is uncertain. Additionally, data indicate that younger generations are interacting on alternative platforms to Facebook (Statista, 2018d).

9. Conclusion

In considering the problem analysis, two solutions for reducing privacy issues through Facebook were suggested. The short-term solution, pro-TECH-t, provides an immediate, easy and straightforward way in which users can proactively manage their data privacy settings on Facebook, whilst drawing attention to the less explicit uses of such data by third parties. This, however, does not fully diminish problems associated with data privacy. Therefore, we propose a long-term solution that moves away from the multi-sided platform in which Facebook currently operates to a decentralized solution that ensures security and transparency of data, making users proactive owners of their own data. However, due to the "lock-in" effect of Facebook, this is a long-term solution, and the correct implementation of various stakeholders is needed to facilitate this switch, which is not immediate. Future research on user experience is needed to investigate how the design of online environments within the two solutions is most effective to reliably discern ways in which data privacy and protection can be successfully encouraged.

10. References:

- Alhabash, S., & Ma, M. (2017). A tale of four platforms: Motivations and uses of Facebook, Twitter, Instagram, and Snapchat among college students?. *Social Media+ Society, 3*(1)
- Akerlof, G. A., & Dickens, W. T. (1982). The economic consequences of cognitive dissonance. *The American economic review, 72*(3), 307-319.

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *In International workshop on privacy enhancing technologies,* (pp. 36-58). Springer, Berlin, Heidelberg.

- Barlow, P., Reeves, A., McKee, M., Galea, G., & Stuckler, D. (2016). Unhealthy diets, obesity and time discounting: a systematic literature review and network analysis. *Obesity Reviews, 17*(9), 810-819.

- Barnes, W., Gartland, M., & Stack, M. (2004). Old habits die hard: path dependency and behavioral lock-in. *Journal of Economic Issues, 38*(2), 371-377.

- Belu, A.M. (2017). The Massive Data Collection by Facebook – Visualized. *Data Ethics*. Retrieved from: https://dataethics.eu/en/facebooks-data-collection-sharelab/

- Beyens, I., Frison, E., & Eggermont, S. (2016). "I don't want to miss a thing": Adolescents' fear of missing out and its relationship to adolescents' social needs, Facebook use, and Facebook related stress. *Computers in Human Behavior, 64*, 1-8.

- Bhaduri, G., & Ha-Brookshire, J. E. (2011). Do transparent business practices pay? Exploration of transparency and consumer purchase intention. *Clothing and Textiles Research Journal, 29*(2), 135-149.

- Boudreau, K. J., & Hagiu, A. (2009). Platform rules: Multi-sided platforms as regulators. *Platforms, markets and innovation, 1*, 163-191.
- Burke, M., Marlow, C., & Lento, T. (2009). Feed me: motivating newcomer contribution in social network sites. *In Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 945-954). ACM.

- Cadwalladr, C. & Townsend, M. (2018). Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica. *The Guardian*. Retrieved from: https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions

- Camber, R., & Greenwood. (2017) Drug dealers using bitcoin cashpoints to launder money: Police warn of explosion in use of digital currency by criminals to offload ill-gotten gains. *Daily Mail.* Retrieved: https://www.dailymail.co.uk/news/article-5142033/Drug-dealers-using-bitcoin-cashpoints-launder-money.html

- Cialdini, R. B. (2007). Descriptive social norms as underappreciated sources of social control. *Psychometrika, 72*(2), 263.

- Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology, 33*(1), 264-277.

- Hagger, M. S., & Luszczynska, A. (2014). Implementation intention and action planning interventions in health contexts: State of the research and proposals for the way forward. Applied Psychology: Health and Well-Being, 6(1), 1-47.

- Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

- Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law, 7*(1), 36-47.

- Evans, D. S. (2003). Some empirical aspects of multi-sided platform industries. *Review of Network Economics, 2*(3).

- Festinger, L. (1962). Cognitive dissonance. *Scientific American, 207*(4), 93-106.

- Fiegermann, S. (2018). As problems pile up, Mark Zuckerberg stands his ground in exclusive CNN Business interview. *CNN Business*. Retrieved from: https://edition.cnn.com/2018/11/20/tech/mark-zuckerberg-interview/index.html

- Frenkel, S., & Benner, K. (2018). *To stir discord in 2016, Russians turned most often to Facebook. New York Times.* Retrieved from: https://www.nytimes.com/2018/02/17/technology/indictment-russian-tech-facebook.html?module=inline

- Frenkel, S., Confessore, N., Kang, C., Rosenberg, M. & Nicas, J. (2018). *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*. The New York Times. Retrieved from: https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html?action=click&module=Top%20Stories&pgtype=Homepage

- Fogg, B. J., & Iizawa, D. (2008). Online persuasion in Facebook and Mixi: A cross-cultural comparison. *In International Conference on Persuasive Technology* (pp. 35-46). Springer, Berlin, Heidelberg.

- Gerber, A. S., & Rogers, T. (2009). Descriptive social norms and motivation to vote: Everybody's voting and so should you. *The Journal of Politics, 71*(1), 178-191.

- Gerson, J., Plagnol, A. C., & Corr, P. J. (2017). Passive and Active Facebook Use Measure (PAUM): Validation and relationship to the Reinforcement Sensitivity Theory. *Personality and Individual Differences*, 117, 81-90.

- Gigerenzer, G., & Hoffrage, U. (1995). How to improve Bayesian reasoning without instruction: frequency formats. *Psychological review, 102*(4), 684.

- Golman, R., Hagmann, D., & Loewenstein, G. (2017). Information avoidance. *Journal of Economic Literature, 55*(1), 96-135.

- Halpern, S. D., Ubel, P. A., & Asch, D. A. (2007). Harnessing the power of default options to improve health care. *The New England Journal of Medicine, 357*, 1340-1344

- Iyengar, S. S., & Lepper, M. R. (2000). When choice is demotivating: Can one desire too much of a good thing?. Journal of personality and social psychology, 79(6), 995.

- Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), 56-59.

- Johnson, N. L. (2018). What are Network Effects? *Applico.* Retrieved from: https://www.applicoinc.com/blog/network-effects/

- Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic perspectives, 5*(1), 193-206.

- Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., ... & Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk analysis, 8*(2), 177-187.

- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security, 64*, 122-134.

- Lahlou, S. (2008). Identity, social status, privacy and face-keeping in digital society. Social science information, 47(3), 299-330.

- Lahlou, S. (2017) Installation Theory. The societal construction and regulation of individual behaviour. *Cambridge: Cambridge University Press*

- Lam, C. F., DeRue, D. S., Karam, E. P., & Hollenbeck, J. R. (2011). The impact of feedback frequency on learning and task performance: Challenging the "more is better" assumption. *Organizational Behavior and Human Decision Processes, 116*(2), 217-228.

- Lilley, S., Grodzinsky, F. S., & Gumbus, A. (2012). Revealing the commercialized and compliant Facebook user. *Journal of information, communication and ethics in society, 10*(2), 82-92.

- Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. *In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 61-70). ACM.

- Lo, S., & Wang, J. C. (2014). Bitcoin as money? *Current Policy Perspectives, 14*(4)

- Lupton, D. (2014). The commodification of patient opinion: the digital patient experience economy in the age of big data. *Sociology of health & illness, 36*(6), 856-869.

- Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. *In Pervasive Computing and Communications Workshops* (PERCOM Workshops), 2012 IEEE International Conference on (pp. 340-345). IEEE.

- Marwick, A. (2016). *Online Consumers and Big Data, Workshop on Big Data Surveillance, Queens University.* Fordham University, Data & Society.

- Marx, K. (1844*).* Introduction to A Contribution to the Critique of Hegel's Philosophy of Right. *Deutsch-Französische Jahrbücher*, 7.

- Midden, C. J., Meter, J. F., Weenig, M. H., & Zieverink, H. J. (1983). Using feedback, reinforcement and information to reduce energy consumption in households: A field-experiment. *Journal of Economic Psychology, 3*(1), 65-86.

- Montgomery, K. C. (2015). Youth and surveillance in the Facebook era: Policy interventions and social implications. *Telecommunications Policy, 39*(9), 771-786.

- Moore, K., & McElroy, J. C. (2012). The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior, 28*(1), 267-274.

- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

- Odum, A. L., Madden, G. J., & Bickel, W. K. (2002). Discounting of delayed health gains and losses by current, never-and ex-smokers of cigarettes. *Nicotine & Tobacco Research, 4*(3), 295-303.

- Posner, R. A. (1981). The economics of privacy. *The American economic review, 71*(2), 405-409.

- Porter, J. (2018). Instagram is testing the ability to share your precise location history with Facebook. *Retrieved from https://www.theverge.com/2018/10/5/17940364/instagram-location-sharing-data-sharing-facebook-test*

- Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior, 29*(4), 1841-1848.

- Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The blockchain as a decentralized security framework. IEEE Consum. *Electron. Mag., 7*(2), 18-21.

- Quan-Haase, A., & Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology & Society, 30*(5), 350-361.

- Rosenberg, S,. (2015, January, 13) How Bitcoin Blockchain could Power Alternate Internet. *Wired*. Retrieved from https://www.wired.com/2015/01/how-bitcoins-blockchain-could-power-an-alternate-internet/

- Salinas, S. (2018). Four of the EU's harshest hits against Facebook CEO Mark Zuckerberg. *CNBC*. Retrieved from: https://www.cnbc.com/2018/05/23/facebook-ceo-mark-zuckerberg-the-eu-parliaments-harshest-hits.html

- Scharff, R. L. (2009). Obesity and hyperbolic discounting: Evidence and implications. *Journal of Consumer Policy, 32*(1), 3-21.

- Seeman, M. (1959). On the meaning of alienation. *American Sociological Review*, 783-791.

- Shapiro, C., Varian, H. R., & Becker, W. E. (1999). Information rules: a strategic guide to the network economy. *Journal of Economic Education, 30*, 189-190.

- Simonson, I., & Tversky, A. (1992). Choice in context: Tradeoff contrast and extremeness aversion. *JMR, Journal of Marketing Research, 29*(3), 281.

- Solon, O. (2018). *Does Facebook's plummeting stock spell disaster for the social network?* The Guardian. Retrieved from: https://www.theguardian.com/technology/2018/jul/26/facebook-stock-price-falling-what-does-it-mean-analysis

- Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture, 23*(4), 254-257

- Statista, (2018a). *Daily time spent on social networking by internet users worldwide from 2012 to 2017 (in minutes).* Retrieved from: https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/.

- Statista, (2018b). *Most famous social network sites worldwide as of October 2018, ranked by number of active users (in millions)*. Retrieved from: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-*users/*

- Statista, (2018c). *Facebook's advertising revenue worldwide from 2009 to 2017 (in million U.S. dollars).* Retrieved from: https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

- Statista, (2018d). *Distribution of Facebook users worldwide as of October 2018, by age and gender.* Retrieved from: https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/

- Synqrinus. (2017). *AdChoices Consumer Awareness*. Retrieved from https://www.the-cma.org/Media/Default/Downloads/Library/2017/DAAC-AdChoicesResearchSummary2017-full.jpg

- Thaler, R. H., & Sunstein, C. R. (2003). Libertarian paternalism. *American economic review, 93*(2), 175-179.

- Thatcher, J. (2014). Big data, big questions: Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. *International Journal of Communication, 8*, 19.

- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.

- Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. *The Quarterly Journal of Economics, 106*(4), 1039-1061.

- Van Der Pligt, J. (1998). Perceived risk and vulnerability as predictors of precautionary behaviour. *British journal of health psychology, 3*(1), 1-14.

- Vishwanath, A. (2014). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83-98.

- Wang, R., Chen, S., & Wang, X. (2012). Signing me onto your accounts through Facebook and Google: A traffic-guided security study of commercially deployed single-sign-on web services. *In Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 365-379). IEEE.

- Wagner, K. (2018). This is how Facebook collects data on you even if you don't have an account. *Recode*. Retrieved from: https://www.recode.net/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg

- Waterson, J. (2018). UK fines Facebook £500,000 for failing to protect user data. *The Guardian*. Retrieved from: https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica

- Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A review of Facebook research in the social sciences. *Perspectives on Psychological Science, 7*(3), 203-220.

- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one, 11*(10), e0163477.

- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), *2017 IEEE International Congress* on (pp. 557-564). IEEE.

- Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *In Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.