TITLE PAGE

"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal

Joanne Hinds[a, *], Emma J. Williams[b], and Adam N. Joinson[a]

[a] School of Management (University of Bath, UK)

Information, Decisions and Operations Division, School of Management, University of Bath, Claverton Down, Bath, BA2 7AY, UK.

Email: A.Joinson@bath.ac.uk

[b]Department of Management (University of Bristol, UK)

Department of Management, University of Bristol, Queens Avenue, Bristol, BS8 1SD, UK.

Email: Emma.Williams@bristol.ac.uk

*Corresponding Author

Joanne Hinds, Information, Decisions and Operations Division, School of Management, East Building Room 3.1, University of Bath, Claverton Down, Bath, BA2 7AY.

Email: J.Hinds@bath.ac.uk.

Abstract

In March 2018, news of the Facebook-Cambridge Analytica scandal made headlines around the world. By inappropriately collecting data from approximately 87 million users' Facebook profiles, the data analytics company, Cambridge Analytica, created psychographically tailored advertisements that allegedly aimed to influence people's voting preferences in the 2016 US presidential election. In the aftermath of this incident, we conducted a series of semi-structured interviews with 30 participants based at a UK university, discussing their understanding of online privacy and how they manage it in the wake of the scandal. We analysed this data using an inductive (i.e. 'bottom-up') thematic analysis approach. Contrary to many opinions reported in the news, the respondents in our sample did not delete their accounts, frantically change their privacy settings, or even express that much concern. As a result, individuals often consider themselves immune to psychographically tailored advertisements, and lack understanding of how automated approaches and algorithms work in relation to their (and their networks') personal data. We discuss our findings in relation to wider related research (e.g. crisis fatigue, networked privacy, Protection Motivation Theory) and discuss directions for future research.

Keywords: Facebook, cybersecurity, targeted advertising, data breach, privacy fatigue, networked privacy.

1. Introduction

As society becomes increasingly digitized, individuals and organisations face incessant challenges when it comes to protecting data and mitigating against security threats. In the first half of 2019 for instance, 3,800 data breaches were reported to have occurred globally, compromising 4.1 billion data records (Winder, 2019). With cyberattacks and data leakages occurring across all sectors, (from health care to finance, and retail to government etc. Magee, 2018) it is unsurprising that such incidents are reported so frequently in the news. The Facebook-Cambridge Analytica scandal was amongst one of the most heavily publicised data breaches of 2018 – following the revelation that around 87 million individuals' data were illicitly harvested without their consent (Cadwalladr, 2018; Kitchgaessner, 2018). Moreover, this data was then used to create psychographically tailored advertisements that allegedly aimed to influence people's voting preferences in the 2016 US presidential election (Kitchgaessner, 2018). The scale of the data-misuse, combined with such grand claims of mass-manipulation provoked global outrage and stimulated numerous protests calling for people to delete their accounts (e.g. '#DeleteFacebook', and '#Faceblock' (Slawson, 2018; Timms & Heimans, 2018).

The scandal also sparked debates about the ethical standards of individuals' privacy online, alongside demands for artificial intelligence to be regulated (e.g. Hern, 2018). However, despite the outcry and widespread appeal for change, implementing these standards, or merely deleting accounts is not so straightforward. For instance, previous research has highlighted that individuals are reluctant to respond to (seemingly) endless data breaches (Choi, Park, & Jung, 2018), and often display behaviour that appears to conflict with their concerns (e.g. Barnes, 2006; Norberg, Horne, & Horne, 2007). Research has also shown that individuals are often unaware that the information on their newsfeeds is curated in line with their preferences and viewpoints (Eslami et al., 2015; Hern, 2017). This would also

suggest that they are unaware that fake news, filter bubbles, and targeted advertisements could supposedly influence their opinions or political preferences. To our knowledge, the link between how people perceive their privacy in relation to this particular form of targeted advertising (and the persuasive effects thereof) is not well understood, thus this research attempts to explore this area. More specifically, it seeks to understand: 1) how concerned people feel about their privacy online, 2) how they protect themselves, and 3) whether they pro-actively manage content (i.e. block, delete, report) that they disagree with, or do not wish to see.

We conducted an exploratory study that investigated people's perspectives on these issues in April/May 2018, directly after the Cambridge Analytica scandal was reported in the media. Through a series of semi-structured interviews, we asked three overarching questions with respect to Facebook: 1) What is your understanding of online privacy? 2) How do you protect yourself in this online context? and 3) How do you avoid unwanted content? In particular, we also aimed to explore whether participants highlighted the Cambridge Analytica scandal within these discussions, and if so, how this affected their outlook and use of Facebook. Figure 1. depicts a timeline of events related to the Cambridge Analytica scandal in relation to when our study was conducted. In the following sections, we provide an overview of how Cambridge Analytica collected and profiled personal data, before discussing related concepts and theoretical models that have been applied to the study of online privacy and targeted advertising.

INSERT FIGURE 1 ABOUT HERE

1.1. Privacy and Targeted Advertising

Understanding online privacy is a challenging and complex matter. Users are typically required to disclose personal information in order to use online services, and the settings that protect/restrict access to these services change frequently. This can be

particularly confusing when using social media, because individuals must continually reveal information about themselves in order to interact with others. Over the last few years, research has demonstrated that privacy is not restricted to a platform's settings or the content individuals choose to publish online (e.g. Kosinski, Stillwell, & Graepel, 2013; Youyou, Kosinski, & Stillwell, 2015). Rather, a person's patterns of behaviour (such as their language patterns, number of friends, frequency of logins) can reveal certain demographic attributes or personality traits when analysed by computer algorithms. The opportunity to study human behaviour in this way has provoked much research seeking to predict how accurately personal information can be predicted from a person's digital footprints (e.g. Hinds & Joinson, 2018; Hinds & Joinson, 2019).

If digital footprints are accurate reflections of a person's identity and behaviour, then such analytics become lucrative methods that organisations can use to create targeted advertisements that align with people's personal preferences. Indeed, research in both marketing and psychology has reported that advertisements psychologically tailored towards individuals' socio-demographics and preferences are more effective than non-tailored advertisements (Hirsh, Kang, & Bodenhausen, 2012; Matz, Kosinski, Nave, & Stillwell, 2017; Moon, 2002). It is the combination of using digital traces to subsequently influence behaviour that was the premise of Cambridge Analytica's business model (i.e. their claims to "*use data to change audience behaviour*" ("Cambridge Analytica," 2018)). Further, what made such activities possible was largely due to Facebook's privacy policies at the time Cambridge Analytica collected people's data. The personality quiz, 'This Is Your Digital Life' was an application that asked respondents to share their data in exchange for the results of the personality test. What respondents did not realise however, was that agreeing to share their data also granted the app permission to collect data from their entire network as well

(Hern, 2018b). Hence, for the 270,000 individuals who provided access to their data, there were millions who did not (Hern, 2018b).

Although the true effectiveness of Cambridge Analytica's targeted advertisements are unknown, the notion that they could influence voting preferences has been highly criticised by both social scientists and politicians (e.g. Chen & Potenza, 2018; Trump, 2018)). One such reason is that personality questionnaires are highly limited because individuals may have distorted perceptions of their characteristics, or they may misrepresent themselves when answering questions (Stone, Bachrach, Jobe, Kurtzman & Cain, 1999). This would mean that advertisements tailored towards individuals' attributes would not be particularly accurate or well matched to their traits. Another reason is that the data harvested by the app may not have been that representative of a person's attributes either. Facebook likes were said to have formed a large part of the psychological profiling, and these are also limited if people's preferences change over time, or if they are not very active from the outset (e.g. Chen & Potenza, 2018).

Nevertheless, the possibility of harvesting and analysing personal information in this way highlights some stark issues in terms of how individuals understand threats to their data, how they protect themselves online, and how (or whether) they pro-actively manage the content they are exposed to. Further, the Cambridge Analytica scandal represents a relatively unique type of data breach to be explored from a research perspective, whereby users' norms and expectations of their routine online interactions were effectively exploited for political gain. To our knowledge, no research has examined people's perspectives of such circumstances[1]. In the following section, we outline previous research and theoretical

[1] Perhaps the most closely-related research is the work bu Jia ans Xu (2016) who examined individuals' concerns about privacy to activity within their social circles. Jia and Xu (2016) found that people who were more concerned about their privacy tended to engage less with friends (through tagging and third-party application use), than those who did not. Other research of people's reactions to data breaches have focused on the financial costs and trends/characteristics of data breaches over time (e.g. Acquisto, Friedman, & Telang, 2006; Gupta & Sharman, 2012; Garrison & Ncube, 2011), public responses to specific news articles (Bachura et al., 2017; Fiesler & Hallinan, 2018), and people's intentions to use online retail stores (Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Raghav Rao, 2016).

concepts relating to people's understanding of online privacy and discuss how these may relate to the Cambridge Analytica scandal.

1.2. Theoretical Background

1.2.1. Privacy concerns and behaviours.

Is it likely that the Cambridge Analytica scandal prompted people to change their privacy settings or delete their Facebook accounts? Or were people even aware what had happened? Existing research on people's privacy concerns and behaviour is fraught with contradiction, and it seems likely that the Cambridge Analytica scandal may echo such findings. While the news reported widespread concerns over privacy online, alongside incitement to "take action", it is quite likely that people did not react whatsoever. Recent research has demonstrated that people feel exhausted from hearing about (seemingly) endless data breaches in the news, and as a result feel that attempts to do anything to protect their data are pointless (e.g. Choi et al., 2018; Keith, Lowry, Evans, & Babb, 2014; Lee, Son, & Kim, 2016; Zhang, Zhao, Lu, & Yang, 2016). This phenomenon, known as *privacy fatigue* (Choi et al., 2018) has also been found to occur when privacy controls are complex or too difficult to keep track of (Keith et al., 2014; Zhang et al., 2016) and due to the overwhelming social/psychological strains of using social networking sites (Lee et al., 2016; Zhang et al., 2016). Similarly, the varied ways in which people use social media – whether to keep in touch with family/friends, read news, or participate in civic activities (e.g. Raine, 2018) means that people may frequently see activity they may disagree with or find aggravating. In particular, research has found that political discussions on social media have caused many people to feel "worn out", and "stressed and infuriated" (Duggan & Smith, 2016). These increasing feelings of losing control, both in terms of keeping up to date with privacy settings and from "unavoidable" exposure to stressful content may therefore cause people to disengage from taking measures to protect their privacy online. This, combined with the

'black box' nature of algorithmic advertising (e.g. Eslami, Kumaran, Sandvig, & Karahalios, 2018), and people's inability to see or understand how their data is used may further strengthen such feelings.

Attempts to understand the relationship between people's privacy-related concerns and their behaviour frequently demonstrates that the two contradict, a phenomenon known as the *privacy paradox* (Barnes, 2006; Norberg et al., 2007). People will often claim to be concerned about their privacy, to later disclose personal information for relatively little in return, such as their income or date of birth for a discount in an online shop (Beresford, Kübler, & Preibusch, 2012), or their phone number/address to use financial services (Norberg et al., 2007). Numerous researchers have sought to understand the privacy paradox, and as a result have offered a range of explanations, including a lack of understanding of risk and knowledge of privacy-protective behaviours (Hargittai & Litt, 2013; Y. J. Park, 2013; Stutzman, Gross, & Acquisti, 2012), inexperience of first-hand online privacy invasions (Dienlin & Trepte, 2015), and social influences (e.g. sharing data because their friends and family do) (Van Gool, Van Ouytsel, Ponnet, & Walrave, 2015). However, despite significant attempts to explain the privacy paradox over recent years, the evidence supporting these accounts remains contradictory and inconclusive (for a review see Kokolakis (2017) or Gerber, Gerber, and Volkamer (2018)). Current evidence also offers no insight toward users' privacy concerns and behaviours in the Cambridge Analytica context – indeed disclosing one's date of birth to make a purchase is a far cry from the prospect of illicitly harvesting profile data to influence political preferences. The unprecedented nature of the scandal means that we do not know how individuals perceive/understand privacy within this context, or indeed whether their current understanding (and subsequent behaviours) will change as a result.

Alternative explanations to the privacy paradox suggest that individuals make privacy decisions by evaluating the potential risks and benefits of disclosing information. For instance, some researchers suggest that individuals perform a *privacy calculus,* in which their behaviour is determined by the outcome of the privacy trade-off (Dinev & Hart, 2006; Jiang, Heng, & Choi, 2013; Lee & Kwon, 2015). In other words, if the perceived benefits of sharing data exceed the costs, then an individual will likely disclose information, for example sharing personal data in order to reap the benefits of loyalty programs[2]. Whilst Facebook users likely made such decisions frequently in their use of the platform, the covert nature of Cambridge Analytica's tactics rendered any privacy decisions (within this context) impossible. Thus, people had no way of knowing that their data would be used, how it would be used, and therefore had no means to evaluate the costs/benefits of their interactions. Investigating people's understanding of online privacy (and indeed whether any concerns are now influenced by the scandal) will highlight whether existing phenomena apply in this new and complex context.

If the ways in which people make privacy related decisions in these circumstances is unclear, then it seems likely that people may feel confused about how to manage their data in the future. One solution could simply be to delete social media accounts entirely (a move that was repeatedly encouraged in the scandal's aftermath (Slawson, 2018; Timms & Heimans, 2018)). However, previous research has highlighted that prior campaigns such as 'Quit Facebook Day' (Portwood-Stacer, 2013; Quitfacebookday.com, 2010) have been ineffective because people are generally reluctant to leave due to social pressures, and the technological affordances it provides (e.g. receiving event updates, maintaining connections with weak ties) (e.g. Baumer et al., 2013)).

[2] Such decisions can also be affected by cognitive biases, heuristics and *bounded rationality* (Acquisti, 2004; Gerber et al., 2018; Kokolakis, 2017), in part because people lack the ability or motivation to process all possible information correctly when making decisions (Deuker, 2010). This means that they can over or underestimate the costs and benefits of the situation (Flender & Müller, 2012).

1.2.2. Networked privacy and Communication Privacy Management theory

Another consideration is that users lack awareness and understanding of how computer algorithms work, and what they can infer from their and/or others' information. This notion is particularly challenging, given that algorithms are generally opaque, to the extent that in some cases the developers do not even know how they work (e.g. Pasquale, 2015) . Similarly, this is also complicated by the fact that a user's privacy is also interconnected with that of other people – a notion referred to as '*networked privacy'* (Marwick & Boyd, 2014). On Facebook, people can disclose others' information when publishing content, or through interaction with others. This content can then be re-posted, or shared by others within their networks, who may also continue to propagate that information (e.g. Ellison, Steinfield, & Lampe, 2011; Jia & Xu, 2016; Wisniewski, Richter Lipford, & Wilson, 2012)). In many instances sharing such data is intentional (e.g. tagging someone in a photo, or commenting in a post), and when this is the case, people can adjust their settings or take other measures in attempt to protect their privacy. In other circumstances, users may be unaware that they are revealing information about other people. For instance, research has demonstrated that an individual's private attributes such as age or location can be inferred via others' data, unbeknownst to the individual themselves. (e.g. Park, Lee, Han, & Lee, 2009; Zamal, Liu, & Ruths, 2011). Such findings are based on the principle of homophily, the notion that *birds of a feather flock together* – which implies that individuals who share commonalities tend to congregate together (as reflected in their social network connections). The role of networked privacy was particularly prominent within the Cambridge Analytica scandal because the vast majority of individuals' data was accessed via one of their network connections without their permission, and without anyone's consent. Since the news of the scandal made such activities explicit, exploring the extent to which people understand (or are even aware of) these possibilities, in addition to whether they have taken any subsequent

action (i.e. changing settings, deleting accounts) will provide insights that will be valuable in improving people's privacy-related behaviour in the future.

Communication Privacy Management (CPM) theory may also provide insight towards individuals' concerns and behaviours. CPM suggests that individuals use the perceived costs and benefits of information disclosure to establish privacy boundaries with those they communicate with (Petronio, 1991, 2002). Up until recently, people may have thought that they had more control over their privacy boundaries, and likely did not consider how privacy can be collectively determined. According to CPM theory, when boundaries are unclear, conflict can result as people feel their expectations of maintaining their privacy have not been met (i.e. their privacy has been violated). This concept, known as *'boundary turbulence'* (Petronio, 2002) often occurs unintentionally, and especially in circumstances where privacy boundaries are not fully understood. Thus, the scandal represents an extreme case of boundary turbulence, because people had no opportunity to regulate their privacy, both in terms of how their information was accessed from others within their networks, and from their historical patterns of digital traces. Therefore, how people subsequently perceive the costs and benefits of information disclosure in light of the Cambridge Analytica scandal may thus change the way people choose to interact online in order to reduce this perceived turbulence.

In sum, existing research highlights that understanding people's perceptions of their privacy online is a complex matter. Further, this is particularly challenging when considered in a landscape of continually evolving computer algorithms and targeted advertising that access and use information in ways that may be unclear to users and considered outside of their control. As we continue to leave digital patterns of our lives online, the Cambridge Analytica scandal therefore provides a unique opportunity to attempt to address this matter. To our knowledge, there is no prior work that has explored people's perspectives within this

context. For these reasons, we adopted an exploratory approach toward data collection and analysis, which comprised a set of semi-structured interviews and an inductive thematic analysis. This conceptual approach and methodology were particularly important as this topic is currently unexplored and complex, and we did not want to unduly influence respondents' answers with pre-defined questions used in more restrictive approaches such as structured interviews or surveys.

Our work seeks to extend and contribute towards existing research in two main ways. First, this work will gather empirical evidence on people's perceptions of their privacy online line, and how they manage their data in light of perceived risks. Second, the work will utilise an inductive ('bottom up') thematic analysis, following the guidelines of Braun and Clarke (2006, 2013). Such methods are seldom used in privacy research; hence this type of analysis will enable us to explore people's responses in greater detail. By reflecting on how the findings relate to existing theoretical concepts within the privacy domain, the work should help future researchers to explore people's perceptions in this new and complicated arena. We describe our methods for this process in more detail in the following section.

2. Method

2.1. Study Design

To explore people's concerns and perspectives following the Cambridge Analytica scandal, we adopted a qualitative approach (following the guidelines of Braun and Clarke (2006, 2013), where we asked participants about their understanding of online privacy, their protective strategies, and how they manage unwanted content (see Procedure below). The study was conducted in May 2018, directly after the scandal was reported in the news. Our goal was to examine participants' thoughts and understanding in an open-ended manner, therefore, we conducted semi-structured interviews where our initial questions were designed

to be quite general regarding online privacy. This flexibility enabled us to explore participants' answers in detail, without prompting any pre-determined concepts. Further, we also wanted to investigate whether the scandal was affecting people's responses and was at the forefront of their minds when thinking about online privacy. Thus, to avoid priming participants, the scandal was not mentioned in any of the study information (recruitment advertisement, information sheet, consent forms, interview questions). Given the limited research focused on networked privacy and the use of data for targeted persuasion efforts, we believe that this design provided the most appropriate basis to explore the concepts outlined in the introduction. The study was approved by both university and project ethics committees.

2.2. Participants and Recruitment

We conducted semi-structured interviews with 30 Facebook users. Participants were recruited through advertisements placed around campus/on the university website, and through snowball sampling during April-May 2018. We chose to recruit participants from the university population because it provided us with access to a reasonably broad range of demographics in terms of age, education (i.e. subject/level of study – undergraduate/postgraduate, as well as staff members who did not have higher education qualifications) and job role (i.e. we recruited people who were employed in non-academic positions, such as administration, sales, and finance). Further, the university population of both staff and students enabled us to obtain a sample of people who were old enough to have detailed histories on Facebook - younger users may not have had accounts or built up substantial histories during the period that data was collected by Cambridge Analytica. A recent survey also highlighted that 74% of Facebook users are aged between 18-54 (Statista, 2018) and in our sample, ages ranged from 18-46 years old ($M = 26.53$, $SD = 7.51$); 10 were male, and 20 were female. Our, sample was reasonably diverse in terms of in terms of level

of education and occupation; 5 participants were mature students (i.e. they were undertaking studies following/alongside employment), and 9 participants were employed (in a variety of roles including administration, sales consultancy, and web design). Table 1 displays the full breakdown of the demographics per participant. Note, in order to preserve participants' anonymity, ID numbers are not reported in Table 1. Thus, the order in which participants' details appear does not correspond to the ID numbers reported in the results section.

INSERT TABLE 1 ABOUT HERE

2.3. Procedure

To take part in the study, participants had to meet the following criteria: 1) log in to Facebook at least once daily, and 2) be willing to discuss their activities and opinions with a researcher. Interview sessions were conducted in a private laboratory on campus and lasted between 20 minutes and 1 hour. Upon arrival to the lab, participants were asked to complete a series of forms, which asked for their: 1) demographic information, 2) Facebook usage (using the questionnaire adapted from Ross et al. (2009)), and 3) informed consent.

At the start of the interview, participants were informed that the purpose of the study was to investigate people's understanding of online privacy, and to establish whether there are common trends in the way that people choose to interact and view content on Facebook. The researcher asked the participant a series of warm-up questions about their general Facebook usage and behaviour – e.g., how they interact with others, and the type of content they tend to like and share amongst their networks. Then, the researcher proceeded to ask questions regarding their thoughts on privacy and potential risks to their data, specifically: 1) What is your understanding of online privacy, 2) How do you protect yourself in online contexts, and 3) How do you avoid unwanted content? As mentioned previously, these questions were purposely designed to be broad in order to gauge whether participants' responses had been influenced by the scandal. For each question, the researcher listened to

the participants and asked them to expand on their answers, and followed up with further questions accordingly. If participants did not mention the scandal, the researcher asked them if they were aware of Cambridge Analytica towards the end of the interview, and asked whether it was something they were concerned about. Table 1 outlines whether each participant was aware of the scandal. At the end of the interview, participants were fully debriefed – the researcher explained what would happen to their data, and participants were given the opportunity to withdraw their consent (none did). They then completed another consent form, confirming they were happy for their data to be analysed and written-up. Participants were compensated £10 for their time.

2.4. Data Analysis

Interviews were audio recorded and transcribed. All personally identifying information was removed or anonymised. We analysed the transcripts by conducting a thematic analysis in line with the approach outlined by Braun and Clark (2013, 2006). A thematic analysis is a qualitative method that focuses on extracting themes and patterns within data through interpretation (Berg, 2004). Our thematic analysis was inductive (i.e. data driven) so that themes could be directly formed from the original data. This also allowed us to explore the data without any pre-conceived ideas. Our analysis consisted of four stages, comprising open coding, axial coding, and selective coding. First, a preliminary set of codes were identified through open coding. Here, two researchers (first and second authors) independently read through the transcripts and generated a set of codes. The researchers then collated and discussed their codes in order to develop/refine a series of concepts. Second, codes were further developed through axial coding. A researcher extracted data from the codes by combining and/or splitting them into a series of overarching themes and subthemes. Third, themes were further refined through a final iteration of selective coding, where transcripts were re-read and data relating to the core themes

identified were coded. Lastly, definitions and names for each theme identified were finalised.

3. Results

Our analysis highlighted a rich and diverse set of opinions and perspectives. Overall, 11 participants mentioned Cambridge Analytica without prompting throughout their interview, and 23 participants were aware of the scandal (when subsequently asked by the interviewer). While we do not know the extent to which the scandal influenced the responses from those who had knowledge but did not reference it directly, their insights (as well as those who had no knowledge whatsoever) provide insight into people's current thoughts on this landscape. To that end, we include a code next to each quotation, which includes the participant number (P) followed by whether they were aware (A) or unaware (U) of the scandal. We organise our findings across three main categories, specifically 1) Contradictory concerns and beliefs, 2) Coping strategies, and 3) Staying versus leaving Facebook. These categories broadly align with each of our main questions (i.e. what is your understanding of online privacy, how do you protect yourself in online contexts, and how do you avoid unwanted content?) Within each category we discuss two related sub-themes that capture participants' most prominent thoughts, feelings and attitudes that were generated from the interviews (see Figure 2 for a taxonomy of these themes/sub-themes). We describe these themes and discuss their relation to existing research in the remainder of this section.

INSERT FIGURE 2 ABOUT HERE

3.1. Contradictory Concerns and Beliefs

When asked about their understanding of privacy, one of the themes most prominent in individuals' answers was the extent to which they feel concerned about their data. In particular, these concerns appeared to be provoked by the notion of feeling "threatened"

when organisations might be monitoring them, or using their data in unknown ways. However, these feelings were also fraught with contradictory perspectives regarding the future of their privacy. In some cases, participants felt like the situation was hopeless, whereas others believed that they could actively improve and manage how their information spreads online. Such patterns of contradictory perspectives reflect similar work on privacy attitudes and behaviours more broadly. These findings are elucidated in more detail below.

3.1.1. I feel safe, but that's creepy

Overall, participants conveyed mixed sentiments towards their privacy on Facebook, which ranged from *"I'm not bothered",* to *"I'm extremely concerned".* It seemed that these polarised views were, to some degree, reflected in participants' awareness of the scandal. For instance, those who described feeling comfortable with their privacy settings frequently expressed a "*nothing to hide*" mentality, where they had no concern sharing information amongst their networks. However, such expressions were made by those who had no awareness of Cambridge Analytica. As such, they attributed their lack of concern to the fact that their privacy settings were "private" (which would be sufficient in preventing strangers or unauthorised organisations from accessing their data), and that they were cautious in what they posted, both in terms of personal data (e.g. they did not share credit card or address details) or in their opinions and thoughts:

"… I can't think of anything I post that I wouldn't… like I don't really care if other people would see it… it's not like I'm posting my credit card details or anything, and if someone really wanted to they could share one of my posts… So, it doesn't make much of a difference to me like, you know, I've got nothing to hide on Facebook. (P20-U).

In contrast, participants who referenced the scandal expressed more concern, although many acknowledged that this would depend on the context in which their data was being

used. For instance, one person explained how they were happy for others to see their posts, but not if their data was used for other purposes:

> *"… I don't mind people seeing I like this post, but that is involving, like privacy issues recently, like the Cambridge thing… If I like the post and they use the information for other purposes, like commercials and that, then this is something quite scary… It's like someone's looking behind whatever you're doing. I really don't like that."* (P24-A)

Further, irrespective of whether participants felt concerned about their privacy, everyone who mentioned Cambridge Analytica considered themselves to be "*immune*" or unlikely to be influenced by psychological targeting. They stated that this was because they were "*well-educated*" about their political beliefs (P8-A, "*privileged"* (i.e. not from a minority or disadvantaged background) (P29-A), "*not vulnerable*" (i.e. they considered themselves to be technologically savvy and aware of possible risks) (P1-A), or generally *"not a target"* (P18-A). Despite this, participants frequently described targeted advertising as "*freaky*" or "*creepy*" (P19-A, P24-A). This was particularly the case when targeted advertisements appeared after looking at something once, or immediately after browsing another website. For example:

> *"…When I search for items on eBay, and then all of a sudden, I get Facebook ads drawing my attention to exactly what I've searched on eBay. I thought, 'How on earth does Facebook know what I've searched for on eBay?' I mean, I'm still not clear about it, but then I do worry… My goodness, how does this work? How is it connected? I just can't figure out what the connection is…"* (P8-A).

Alternatively, participants also reflected on times where they found targeted advertising useful. For instance, one participant explained how targeted advertisements from the accommodation website Zoopla helped them to find a home:

"So, I see quite a few ads from Zoopla and I was like, 'Well, fair enough, I did spend three days looking for accommodation on there', but that stuff is actually quite useful." (P12-A)

Overall these findings suggest that participants tend to view online privacy simplistically (e.g. if they refrain from disclosing their bank details, then their data is safe). They were also unaware that personal information could be inferred through their interactions or via their friends'/followers' interactions within their networks. Thus, the belief that one has "nothing to hide" is naïve to this possibility, as well as to the concept of networked privacy. This naivety also appeared to extend to individuals' perceptions of targeted advertisements. When targeted advertisements "make sense" and reflect a person's behaviour or interests (i.e. they feel like they understand why they are seeing it, they experience no concern. Alternatively, advertisements are perceived as creepy or unnerving when individuals have no recollection of viewing the associated content online. In these instances, individuals' worries appeared to be focused on the contextual intricacies of *how* organisations obtained and targeted data accurately, rather than on the consequences that such communications may have. As a result, individuals seemed to be in denial about their susceptibility to the persuasive effects of communications such as those made by Cambridge Analytica.

Further, these findings reflect typical sentiments expressed in privacy research more broadly. For instance, previous research has described instances where individuals perceive privacy intrusions as "creepy" to later say they are unbothered (e.g. Phelan, Arbor, & Resnick, 2016). Similarly, Shklovski, Mainwaring, Skúladóttir, and Borgthorsson (2014) found that while people often disliked tracking and third party data collection, they could also see valid and legitimate reasons for collecting data (e.g. personalised services). However, it is not just privacy perspectives that contradict here, it is people's views on the effectiveness

of targeted advertising to influence political preferences. The overwhelming perception that they are resistant to any persuasive communications stands in stark contrast to the supposed success of Cambridge Analytica's attempts to influence.

3.1.2. There's nothing I can do, but I'll help.

The ramifications of the Cambridge Analytica scandal provoked further mixed sentiments surrounding whether participants could effectively do anything to stop their data being used in similar ways in the future. Many participants expressed thoughts of feeling "*helpless"*, and that the "*damage is done"*, where third parties have already taken their data, expressing they have "*given up"* and will continue using Facebook without changing anything. For instance, one participant explained:

> *"…with stuff like the recent Facebook scandal, it's like you don't realise how open your data is. I feel like a lot of companies probably do have my data now and I've just kind of got to the point where I've accepted, the basic data, I don't care about sharing that with third parties anymore because I know most of them probably have it by this point."* (P28-A)

In a similar vein, some participants reported feeling "*trapped*", describing that they are concerned about how their data is being used, yet they *need* to keep their account because Facebook enables them to stay in touch with friends and family. For example:

> *"After that [scandal] happened, I went back to my Facebook account and started to raise the privacy of my account… So I started to be more conscious of my rights as a user of social media, and I tried to do things, but the problem is, I don't do everything I want because this means that that would limit my use of Facebook… the other alternative would be to deactivate my account… But then, this is what keeps me in touch with friends and family, so I decided to stay with Facebook and just keep an eye on what I'm doing."* (P25-A)

Despite some participants' sense of losing control, others described more active efforts to inhibit the spreading of controversial or negative content by reporting them to Facebook. Although such actions do not affect an individual's own account/data directly, these types of perspectives demonstrate an attitude of serving the "*greater good*", by attempting to prevent "*bad*" content from spreading through others' networks. For example, one participant described how they regularly reported Britain First (a far-right political party in the UK, whose Facebook page has since been deactivated after repeatedly violating community guidelines):

> *"… I reported them [Britain First] almost constantly… the response I got was always rubbish like… 'We have reviewed it and it has not broken our terms'. I'm like, it has, but sometimes it's not the post that necessarily has, but the comments that have led off it."* (P18-A)

Finally, others reported an element of hypocrisy in other people's behaviour or rationality generally. Specifically, one participant explained that while many people seemed worried, they often readily gave away their data without checking the organisation's terms and conditions:

> *"We all are very exposed aren't we, in so many ways. Everything we do is exposed and we sell it to ourselves because most of the time they say, 'Oh if you like us and comment here and give us your Facebook, you will get a free cappuccino from Starbucks'… so everyone's going to give you all the data you want… Most people don't care about their privacy… and they don't even read the terms and conditions, they just click 'accept.'"* (P4-A)

The sense of powerlessness experienced following the scandal reflects previous work on learned helplessness (e.g. Seligman, 1972; Shklovski et al., 2014). Learned helplessness (i.e. the belief that a situation is unchangeable, even if solutions subsequently become available)

has been associated with other instances where individuals have learned how their data is used and distributed, such as in mobile applications (Shklovski et al., 2014), or after experiencing a data breach (Bott & Renaud, 2018; Choi et al., 2018). However, the sense of stopping "bad" information from spreading (by actively reporting persuasive content) suggests that individuals are not completely resigned to such loss of control. The distinction between these findings is that individuals must give up their data (to a certain degree) in order to use Facebook and they have little (or no) control over what organisations do with that information. Yet when organisations' intentions are visible (e.g. influencing political preferences), and it is possible to act on these activities (e.g. reporting Britain First), then they are perceived as a means by which people can help others at a broader collectivistic level. These discrepancies also relate back to our previous finding that people believe they are immune to persuasive communications, whereas other more vulnerable or "less savvy" people are not. Thus, the cost-benefit analysis they perform in giving-up/accepting their data is taken may not seem so drastic when they believe they are resilient to persuasive communications. Yet by attempting to intervene or prevent (what are perceived as) politically harmful communications from spreading, they can help to protect those who are more "susceptible".

3.2. Coping Strategies

In order to manage some of the concerns discussed above, participants described numerous strategies they use to manage how their accounts are displayed to others, and how others' posts are displayed to them. In some instances, this was to maintain privacy, in other cases it was to manage people that they found "annoying". Many participants also acknowledged that they *should* "pay more attention" or update their privacy settings, but found doing so tiresome and tedious.

3.2.1. Managing me, managing you.

Participants frequently described being aware of how they appear on Facebook. Primarily, this related to how others perceive them, and what they are willing to share (rather than what third parties may do with their data). Overall, participants displayed relatively open attitudes towards their self-disclosure, with some expressing "nothing to hide" mentalities, e.g. *"… I don't see the point in like, putting on a façade."* (P29-A). Others were more conservative in their approaches and described how they monitor and maintain who sees their profile. These included holding regular "*friendship culls*" (P6-A, P11-U, P12-A, P15-A, P26-U), or "*checks*" to see what their profile looks like to others (P11-U, P18-A, P23-U). The main reasons participants had for performing culls were to maintain "close" friends within their networks, and to weed-out friends they found annoying or that had conflicting opinions to their own. For example, one participant described:

> *"I have a Facebook cull every year where I get rid of anyone whose name I didn't recognise… I'll get rid of anyone who I've not talked to all year, or who I don't enjoy seeing their posts from. So, someone I was friends with but they posted a lot of stuff to do with the British National Party and UKIP and a lot of things which I just really disagreed with and really angered me, so I was just like, 'I'm sorry, I'm going to have to unfriend you because it's not good.'"* (P12-A)

Alternatively, inspecting their own profile, and viewing how it appears to others (by using the "View As" button) was a common approach that participants used to check their profile was displayed as they intended. This provided participants with a sense of "*security*" (P23-A) or reassurance in their privacy settings. For example:

> *"… I always have a little look and double-check everything… I'll just go through and check that all my photo albums are set to, like, friends, maybe friends of friends, and yeah, any information I don't want visible to everyone, just make sure that's all just*

set to what I want. I like the fact that it's got the 'View As' thing, so that you can view as a stranger and get to see exactly what they can see." (P11-U)

Similarly, another participant described adjusting their privacy settings depending on the type of content they were posting. Specifically, they would filter out different posts to different people in their network, especially when posting or sharing something that may conflict with others' values or beliefs:

"… you can filter out what you don't want to see before you post, so I use that quite often, actually, especially when it comes to some posts that might be a bit too sensitive for my parents, like gay marriage support, or something." (P1-A)

These findings highlight that people are generally aware of how others perceive them and take steps to mitigate how they present themselves to others, by controlling "who sees what". However, this awareness appears to be limited to their own posts/disclosures to their friends/followers. Beyond that, individuals do not seem to consider the broader implications of their interactions and how these may inform the design of targeted advertisements. Instead, participants decisions to manage what others see was driven by the desire to manage annoyances – to stop themselves from seeing content they find aggravating, rather than to prevent organisations from inferring information about them. Again, perhaps this is also linked to participants' perceptions that they are immune to such operations. It also suggests that people are naïve to networked privacy. Thus, while having "nothing to hide" may be a liberating thought when sharing opinions and aspects of their lives, the participants did not realise the subtle and more nuanced ways that such interactions can "leak" their personal information.

3.2.2. I must update my privacy settings… maybe later.

Although participants did not consider Cambridge Analytica when describing how they manage who sees their information, Cambridge Analytica seemed to be at the forefront

of most participants' minds when asked about their privacy directly. For instance, many participants mentioned "*recent events in the news*" when asked how worried they were. That said, no one described feeling more concerned as a result of the scandal. Many participants mentioned that they *"probably should check"* (P10-A, P13-U) their privacy settings, and read Facebook's terms and conditions (as well as those on other websites/platforms), but described finding the time or the inclination to do so difficult. For example:

> "*I did do the other day [read Facebook's terms and conditions]. It was after work and I was on my laptop and I was like, 'This is really boring this', and it was page after page, and it was next, next, next…"* (P13-U)

Further, one participant described a desire to stay "*in denial"*, despite being warned about potential privacy threats:

> *"Sometimes things get shared on Facebook, where someone says, 'Did you know that if you haven't done this, then people can see this,' and I'll think, 'Oh! Is that true? I better have a look at that'. But otherwise, I'll just live in denial. I think that everything is fine and private, and probably it isn't."* (P10-A)

These contradictory thoughts could possibly be explained by a lack of trust and general confusion that participants described in terms of how privacy settings work, especially when they are "*constantly changing"*. For instance, one participant explained:

> "*I think Facebook's made it very difficult for you to remain very private. Like, maybe I don't know, maybe they've changed it now, but I remember like maybe two years ago when I was trying to… push down my privacy, I found it really difficult to be able to tick all the boxes that meant I was completely private because it just felt like I was just getting through some hoops… Friends of friends, they were still finding my profile… Because it almost seems like they don't want you to be private… Well, obviously they don't because I don't think that's come up, they want your profile to be*

as private but also as public as it possibly can, so I think they make it very difficult for you to just like really limit yourself to just your friends." (P7-A)

Alternatively, one aspect that many participants seemed particularly concerned by was Facebook's facial recognition feature. At the time of our interviews, Facebook's new facial recognition software had been launched in the UK (Tamblyn, 2018; Welch, 2018), and many participants had received an update asking for their permission to turn it on. Many participants who mentioned facial recognition, described that they did not want to enable it, because they did not trust it was safe:

"Now there's an update thing asking me whether you wanted it [Facebook] to use facial recognition. I think I said no for the time being. I wasn't sure. And they said it was a good thing so that people couldn't use your photographs without your consent, but I don't know, maybe I'm being too naïve, but I can't imagine people particularly doing that anyway." (P17-A)

Overall, participants' thoughts reflect other recent findings that indicate people's lethargy over constantly changing security policies and data breaches (Bachura, Valecha, Chen, & Rao, 2017; Choi et al., 2018; Fiesler & Hallinan, 2018). Thus, not only is keeping up-to-date tiresome, when people do make the effort to update their settings/read policies etc., they are quickly deterred or confused by the overwhelming amount of information they are confronted with. Remaining in a state of denial about potential risks and threats to personal data relieves individuals of having to worry about organisations taking/using their data and enables them to continue using Facebook unhindered. Likewise, the risks posed by organisations such as Cambridge Analytica are much more subtle than other types of threats. That is, receiving targeted communications intended to influence political preferences does not pose the same consequences as having one's bank or address details stolen. The individuals in our study generally did not know whether their data had been used or not – therefore it may be easier to

remain in denial (in cases like these) because such threats pose no direct personal impact. Alternatively, previous research of individuals who have experienced a data breach suggests that people experience denial in a similar way to the denial experienced in the grieving process, where individuals experience disbelief over their own privacy loss and instead assume it is something that happens to other people (Bott & Renaud, 2018).

3.3. Staying Versus Leaving Facebook

Finally, many participants expressed mixed emotions and general confusion over whether they should keep using Facebook or delete their accounts altogether. Despite many reporting increasing frustrations with Facebook, and also with many of their 'friends', it appeared that the need to keep their connections with others prevented them from leaving. Further, many of the features provided by Facebook in terms of blocking, unfollowing, or hiding others' posts appeared to help mitigate most of these annoyances. In all cases, declarations of wanting to leave did not appear to be motivated by the scandal explicitly, indicating that such sentiments are complex and multifaceted.

3.3.1. I've had enough… but I can't leave.

Almost all participants expressed some form of anger or feeling of being "*fed-up"* with Facebook. These feelings stemmed from other people's behaviour (e.g. annoying posts), rather than content displayed in advertisements, fake news, or (perceived) threats to their data. Specifically, frustrations of others' (supposed) narcissistic tendencies in the form of "*posting selfies"*, (P1-A, P10-A), "*attention seeking*" (P18-A, P29-A), and generally "*showing off*" (P9-A), were participants' main annoyances. As a result, some participants explained that they had distanced themselves, and tried to reduce the amount of time that they spent using Facebook:

> *"So, if someone just keeps on doing something that's really annoying because, you know, when you're looking at something you can feel it, you can feel yourself getting*

annoyed and I think it's more… I'm like, you are absolutely entitled to your opinion but also I don't want to feel this way when I look at my phone." (P18-A)

However, despite many participants' increasing frustrations, some commented that they could not deactivate their accounts. This was because they had some form of reliance on Facebook. These sentiments were also expressed earlier, where participants provided accounts of feeling *"trapped"*. For example:

"*I was like, 'What if I just delete the network or my account from here? But then I wouldn't be contactable for gigs and I thought, 'Okay, I'd better not'."* (P13-U)

Other participants explained that they now consider Facebook to be a part of their history, and that they like keeping a digital record of their life. One participant even described deactivating their account because they found other people annoying, but then returned a few weeks later because they felt Facebook was a part of their identity:

"I have a history on Facebook… I did deactivate the account for quite some time because I felt like it was a bit distracting to me, like I'd go to Facebook every single half hour, which is too often to me and it's distracting. So, I deactivated for a while, maybe two or three weeks, and then I went back to it because, as I said, you feel like Facebook is part of you. If you've been on Facebook for ten years now, you have all... your posts, even your comments as part of your history… So, when you put it on Facebook, it's like, people before… they used to write diaries…" (P25-A)

Similar to our previous findings, participants tended to express anger over other people's posts rather than over third parties targeting them with 'persuasive' advertisements. Such annoyances were enough to make people consider closing their accounts, yet ultimately people felt a need to stay in order to maintain connections with others, or for some other practical reason. This reflects previous findings which have also demonstrated that people are often reluctant to leave social media due to the social cost and inconvenience involved in

doing so (e.g. Fiesler & Hallinan, 2018; Schreiner & Hess, 2015). The Cambridge Analytica scandal was not at the forefront of participants' explanations when describing their thought processes surrounding leaving Facebook. This could also be due to the lack of perceived threat of persuasive communications, as other research has found privacy concerns to be a sufficient catalyst to incite leaving (e.g. Baumer et al., 2013; Shklovski et al., 2014). For instance Stieger, Burger, Bohn, & Voracek (2013) found that Facebook "quitters" frequently cited concerns over the treatment of personal data by organisations as a main reason for leaving. This therefore suggests that absence of this perceived risk, combined with the cost of leaving explains why the scandal did not provoke participants to close their accounts.

3.3.2. To block, or not to block?

In relation to participants' considerations about leaving Facebook, many described their approaches toward handling unwanted or annoying communications. Interestingly, all participants reported having some form of unwanted communication or behaviour from people within and outside of their networks. These included suspicious (or "unusual") contact from strangers (P10-A, P15-A, P25-A), communications from ex-partners (P11-A, P20-U, P27-A), or some form of harassment (P18-A, P20-U). In some cases, unwanted communications were considered to be easy to deal with, such as blocking strangers who sent "friend requests" or messages (P10-A, P21-U). For example:

> *"… I had someone who sent me a message… I wasn't friends with him on Facebook, we had like one mutual friend. I must have appeared in the timeline when it's got suggested friends there. He just sent me a message, 'Oh you're really pretty… I want to know if you're single.' Oh, for god's sake! It just came out of nowhere, so I blocked him in case he sent anything else."* (P21-U)

In other cases, participants described how they handled more complicated situations, where simply blocking or "unfriending" would be inappropriate. These were circumstances where

participants felt they had to deal with a kind of "*social politics*", where they needed to maintain a relationship/connection with someone, yet they did not want to maintain their Facebook friendship with them. Examples of these types of relationships included close family members (e.g. their sister-in-law) and friends. In these instances, participants explained that they found the "unfollow" or "hide" functions useful for managing this. For example:

> *"I did that [unfollowed] with some of my family members. I kept that as a secret of course… When I felt they went too far on criticising whatever I put on Facebook and saying that I come from a different world… because I live somewhere else…"* (P25-A)

Another described that they unfollowed one of their friends because they liked them, but disagreed with their political opinions:

> *"One guy was talking about Brexit a lot and wanted to leave, so I was like… I didn't want to unfriend him because I actually really like him, but I also just didn't want to hear his misinformed comments. So, I was like, I know he's going to say something probably quite rude, and that's not the way forward."* (P18-A)

Not only did the *hide* or *unfollow* functions enable participants to preserve social obligations, they helped participants to protect the feelings of people they did not particularly like, or found offensive or annoying, since some participants considered outright blocking or unfriending to be "*mean*". (P10-A)

In line with our earlier findings, many participants described receiving unwanted or frustrating communications, yet the focus of such annoyance primarily related to content posted by their friends, rather than from external organisations. The intricate strategies that people develop to manage such communications – striking a balance between reducing their personal distaste and preserving their relationships appear to mitigate these issues. The idea

that such information could come in the form of targeted advertisements did not appear to resonate in participants' rationales, or if they did such troubles were overridden by the more aggravating actions of those within their networks.

4. Discussion

4.1. Theoretical Implications

Our findings highlight two main trends across participants' perspectives: 1) individuals lack understanding of their networked privacy - they lack knowledge/awareness of how information can be derived through others' interactions, and that this information can be used to inform the design of targeted advertisements, and 2) individuals think that they are immune to targeted advertisements/persuasive communications (as used in the efforts of Cambridge Analytica). A lack of understanding in both of these areas illustrates the complex nature of how information is communicated and shared by individuals (both knowingly and unknowingly), and subsequently used by organisations. Therefore, without such awareness it seems unlikely that individuals will be able to make truly informed decisions about the privacy of their personal data online.

A number of participants reported increased concern about their privacy as a result of the scandal, whereas those who had not heard of Cambridge Analytica described feeling unbothered. Individuals with "nothing to hide" mentalities viewed privacy more literally (i.e. they are happy to share aspects of their lives with others), and logically (i.e. refraining from posting bank details meaning they are not "at risk") rather than as something that could be violated through more subtle or covert means. Similar reasoning was expressed by participants who described concerns about how organisations obtain and use their data, where they reported worries about data misuse without any knowledge or understanding as to how this occurs. This lack of understanding could be explained by related research that has found that people feel overwhelmed and fatigued by opaque practices of organisations as well as

frequent data breaches reported in the news (Choi et al., 2018; Hargittai & Marwick, 2016; Keith et al., 2014), meaning they stop trying to stay up-to-date with such developments. Although no-one claimed to feel exhausted by the news of the scandal explicitly, this could be inherent in participants' lack of outrage/shock about the story.

These insights also suggest that individuals have no understanding of the role of their networks in contributing towards how advertisements may be crafted and psychologically tailored toward them. This exposes their potential naivety towards privacy risks and lack of understanding of how their information can be inferred from others within their networks (rather than solely from their own accounts). However, whether this makes them more "vulnerable" than knowledgeable individuals is unclear. For instance, other research has found that knowledge of security does not necessarily predict whether individuals will behave more securely (Arianezhad, Camp, Kelley, & Stebila, 2013; Kelley & Bertenthal, 2015; Tambini, 2018) and this is further complicated when a person's vulnerability is also dependent on the knowledge and actions of others within their networks. Despite this, some participants were vocal about "taking action" by reporting controversial or negative content to Facebook. This demonstrates that people were mindful of harmful content spreading through their networks and were motivated in helping to protect others. The willingness to actively try and disrupt these types of activities contrasts with the aforementioned perceptions of cynicism, helplessness, or that such endeavors are now pointless (Choi et al., 2018; Keith et al., 2014). Perhaps the difference here is that certain efforts to influence are more transparent and provide a means by which they can be challenged/disrupted, and where consequences for these interventions are also visible. For instance, it was often political content that provoked these reactions – but content that was posted in various groups (not via advertisements specifically), that people could report to Facebook for violating certain guidelines (or if it conflicted with their values and they deemed it harmful). Increasing

aggravation regarding political content has been reported in numerous studies and reports over the last few years (Duggan & Smith, 2016; Vraga, Thorson, Kligler-Vilenchik, & Gee, 2015). Thus, actions where people report or attempt to diffuse, counter, or block such content could act as a strong incentive to hinder those types of messages pervading on Facebook.

Another explanation for participants' apparent indifference toward the scandal is that none reported that their data was used by Cambridge Analytica, or that they had personally experienced a data breach. Previous research has indicated that attitudes toward privacy and data breaches tend to be based on heuristics or secondhand experiences, which are not enough to influence more secure or cautious behaviour (Dienlin & Trepte, 2015; Gerber et al., 2018). Similarly, people are often believed to suffer from an "illusion of control" when dealing with the privacy of their data. Brandimarte, Acquisti, & Loewenstein (2013) found that individuals appear to confuse the control they have when publishing their information with the control that third parties have when assessing that information. As a result, individuals are more likely to allow their personal information to be published, and even share more personal information if they are given explicit control of this process. Yet, when a third party is responsible for the publication of such data, they may perceive this as a loss of control and express concerns about it (Brandimarte et al., 2013). It seems plausible that similar effects were occurring here – participants did not experience a loss of control, by not experiencing the data breach first hand, and by not realising what their data may surreptitiously reveal (i.e. it would be impossible to know which of their posts, likes, information etc. obtained via their networks contributed to psychologically tailored advertisements). This may therefore make it difficult or unrealistic for a person to experience outrage or panic in response to the scandal.

Previous research on people's reactions to data breaches may also help to justify our findings, as studies have found similar effects where participants have reported feeling that they have "nothing to hide" or that "rich people will be targeted" rather than themselves (Solove, 2007; Zou, Mhaidli, Mccall, & Schaub, 2018). However, such research has largely focused on the economic costs (Acquisti & Grossklags, 2007; Layton & Watters, 2014), the characteristics and trends (Gupta & Sharman, 2012; Garrison & Ncube, 2011), and public reactions made via social media channels and news article comments (Bachura et al., 2017; Bott & Renaud, 2018; Fiesler & Hallinan, 2018) to data breaches, not on people's personal reactions to this new type of activity. A common finding amongst these studies (where actual victims or data breaches were studied) is that people exhibit emotions that resemble reactions to other losses or grieving processes (Bachura et al., 2017; Bott & Renaud, 2018). As such, individuals are believed to experience denial, anxiety, and anger (akin to Kübler-Ross' five-stages of grief (Kübler-Ross & Kessler, 2005)) before reaching a level of acceptance of the intrusion. Although we were unable to study these aspects (as no participants reported experiencing a data breach here), the finding that individuals' sentiments reflected other attitudes broadly found in privacy research suggests that similar emotions may be associated with these types of breaches. Further, it highlights that people cannot differentiate between the two disparate contexts. Losing personal data is markedly distinct from the psychological inferences made by Cambridge Analytica, as privacy could be violated without any explicit breach of their information (i.e. it is inferred through patterns in theirs' and others' data). Thus, participants view privacy as something that is more tangible and within their control than this new reality where it can be violated more coercively.

Participants inability to distinguish between the different characteristics of the scandal and more "typical" data breaches also raises questions about their belief of being "immune" to psychological targeting. Hence, if persuasive advertisements are ineffective (in the context

of political communications), then does it really matter what organisations do with their information? Or, if these individuals are immune, do they need to consider how their online activity may therefore impact others who are more susceptible? Such considerations did not appear to be prevalent in participants' mindsets. Further, the notion that participants found some advertisements creepy highlighted that their lack of understanding of how accurately information had been obtained and crafted, not on worries about their susceptibility to that information. Protection Motivation Theory (PMT) (Rogers, 1975) may help to explain this, as it suggests that people assess whether something is threatening, and then whether they feel able to cope with that threat (e.g. change their behaviour). Thus, finding targeted advertisements creepy indicates that people do not know how their online behaviour has caused the ad to be targeted toward them in the first place. Consequently, this means that they cannot necessarily change their behaviour in order to protect themselves from this happening again. Alternatively, when individuals perceive targeted advertisements to be more logical to their activities/preferences, they may feel more confident in taking measures to protect themselves (should they want to). Our findings highlighted that targeted advertisements such as these were often viewed positively as they acted as reminders or helped people to locate what they wanted.

Studies that have examined perceptions of targeted advertising have displayed similar results. For instance, algorithms used in targeted advertising are typically opaque (i.e. users generally do not know how they work). The feeling of "being watched" and making accurate (or "creepy") inferences from people's data can decrease trust in behavioural advertising. In an attempt to mitigate this, some advertisers have made their algorithmic processes transparent to alleviate users' concerns (e.g. Facebook, 2019; Google, 2019). Eslami, Kumaran, Sandvig, & Karahalios (2018) examined how revealing parts of algorithmic processes to users affected their perceptions towards advertisements and their own privacy.

They found that users preferred interpretable explanations about why advertisements were presented, however users found vague or oversimplified language to be untrustworthy. Problematically, it seemed that participants found interpretability and simplicity "creepy", and as such did not want to be exposed to information they felt uncomfortable with.

It may also be the case that participants' beliefs that they were resistant to influence related to *cognitive dissonance* processes, where people feel uncomfortable holding contradictory beliefs or values. In order to reduce the perceived dissonance between conflicting thoughts and behaviours, people may change either their beliefs or their behaviours (Festinger, 1957). For instance, users may enjoy using Facebook, since it enables them to maintain relationships and enjoy the other benefits that the platform has to offer. If they become aware of potential privacy risks or threats relating to their use of the platform, then they may either choose to change their behaviour to reduce the perceived risk or adapt their cognitions with regards to the likely personal risks. It was evident from the interviews that participants did not show high levels of awareness regarding the wider privacy implications of their online interactions – whether this stemmed from denial of the issue, active avoidance of materials that aim to raise awareness of these risks, or simply not previously being exposed to such information, remains unclear.

Finally, participants conveyed mixed emotions when discussing whether to keep or close their Facebook accounts. Many explained that they had considered this, or had closed their accounts at some point (no one had done so in response to the Cambridge Analytica scandal, however), only to return later on. This pattern of behaviour, known as *social media reversion* (Baumer, Guha, Quan, Mimno, & Gay, 2015) has been suggested to occur due to reasons including perceived addiction, social boundary negotiation (i.e. privacy, surveillance and impression management), usage of other platforms, and their friends' reactions to non-use (Baumer, Sun & Schaedler, 2018; Baumer et al., 2015; Guha, Baumer & Gay, 2018).

Our findings appeared to reinforce elements of these findings, as participants who described returning to Facebook felt that they needed to keep their accounts in order to stay connected to their friends. Similarly, those expressing desires to leave were motivated by social surveillance and annoyance (such as attention seeking, narcissistic tendencies etc.). Threats to privacy, or surveillance from organisations/institutions did not seem to factor into our participants' reasoning (which was also similar to Baumer et al's findings). Notably, our findings were limited to anecdotal accounts of people leaving and returning and so did not explore the full range of potential reasons participants may have had in doing so.

Another prominent reason for keeping Facebook was that many participants considered their account to be part of their identity or 'digital history'. So, aside from a mechanism that enables them to keep in touch with their friends, Facebook provides a place to reminisce about past events and to keep digital records of their memories. Again, participants holding these perspectives seemed oblivious to the privacy risks associated with keeping data in this way. For instance, recent research in *digital hoarding* (i.e. the over-accumulation of emails, photographs and so forth) has highlighted that many people feel attached to their digital data, feeling that its value may be realised sometime in the future (Sweeten, Sillence, & Neave, 2018). The sentimental value of digital data has been widely reported (Brewer & Jones, 2015; Thomas & Briggs, 2014) as well as the notion that virtual possessions become a part of a person's identity (Belk, 2016). As such, this can create reluctance to delete personal information, especially if people also perceive the task to be unnecessary and unrewarding (Dabbish, Kraut, Fussell, & Kiesler, 2005). Further, this can also affect a person's network, for instance research on *shadow profiling* has demonstrated how personal attributes (such as sexuality and political orientation) can be inferred through others' data (Bagrow, Liu & Mitchell, 2019; Garcia, 2017). If people are reluctant to delete

their information, then not only does this put themselves at risk, but also others within their networks too.

4.2. Limitations

Our study has numerous limitations. Whist our sample had a degree of diversity in relation to age, level of education and occupation, it is likely that our sample is non-representative of the general population. Therefore, we do not know the extent to which our findings generalise across different backgrounds and cultures. Although participants reported mixed concerns regarding their privacy on Facebook and in general, none appeared to have experienced any data theft or misuse first hand, our findings may have been different if we interviewed people who had experienced some kind of privacy intrusion, or indeed had seen the kind of behavioural targeting that was employed by Cambridge Analytica. Further, as our interviews were limited to participants' experiences and self-reports of using Facebook we had no measure of their *actual* behaviour. Therefore, it could be the case that some of the behaviours that they described were different in reality (e.g. they may have claimed to have reported abusive behaviour towards others, but instead they did nothing), but unfortunately, we had no way of truly assessing this in our interviews.

4.3. Practical Implications and Recommendations for Future Work

Our findings highlight numerous insights that could be useful to system designers, online communities, cybersecurity practitioners and researchers generally. Overall, our findings showed that people believe that they are resistant to persuasive communications, they lack understanding of how targeted advertising works, and do not realise that their privacy can be violated through subtle, indirect ways (via their own and others' data). Participants did not consider privacy or targeted advertisements beyond themselves, rather, their thinking was limited to their own settings and information disclosure. This was evident in people's perceptions of targeted advertising, as people described their confusion about how

algorithms work and struggled to comprehend how their digital traces may be a factor in this. There is a clear need for improving awareness of networked privacy risks and educating people on how to protect themselves. However, researchers and practitioners must be careful in order to avoiding contributing to further fatigue/disengagement by overloading people with more information they may struggle to understand or keep up with. Future research could therefore explore ways to make this more effective.

Researchers could also consider how certain features could be designed or improved to support people's abilities to manage how information spreads throughout their networks. Our findings conveyed a variety of intricate strategies that individuals use to regulate their privacy boundaries with others. The 'View As' and 'Hide' buttons appeared to be popular mechanisms people use to curate their content in terms of controlling how they appear to others. Similar features could therefore be developed to inform people what organisations or institutions can "see" from their digital traces, as a way to inform people to better manage their collective privacy. Further, future research may want to further disentangle people's complex feelings and behaviours related to leaving Facebook. It seems that for many, the need to maintain connections, or the desire to keep memories overrides people's decisions to close their accounts and delete their data. Further work of the ramifications of digital hoarding within the context of networked privacy would therefore help us to understand the potential security implications of these behaviours.

The notion of feeling fatigued seemed to underpin many of the concepts present in our findings, from updating settings, to paying attention to expert advice, feeling drained by others' behaviour etc. Further work could seek to establish ways to attempt to motivate people to become more engaged and motivated towards understanding their privacy and actively managing it. Similarly, the finding that users will not close their accounts has also been present amongst numerous debates about regulating Facebook in terms of imposing

laws and rules for how data is used and protected (Casanovas, De Koker, Mendelson, & Watts, 2017; Tambini, 2018). Future research could explore users' thoughts and behaviours surrounding the potential impact of such regulatory regimes.

Finally, another challenge concerns responsibility - in terms of what a user is responsible for, and what organisations/platforms are responsible for. Existing research has displayed mixed perspectives regarding responsibility for privacy in terms of whether it is the individual's or the organisation with whom they are transacting (Vitak, Shilton, & Ashktorab, 2016). For instance, Fiesler and Hallinan (2018) found that some people felt victims were to blame for their own privacy violations, because they "should have known" or used common sense when disclosing or protecting their information, whereas others felt that organisations or platforms should be responsible. Irrespectively, both perspectives are problematic - placing responsibility in hands of users creates more pressure to read policies, accept terms and conditions, stay up-to-date with changes etc. in a climate in which we know that they are already tired and frustrated of these demands (Barnes & Van Dyne, 2009; Choi et al., 2018; Keith, Maynes, Lowry, & Babb, 2014). Likewise, placing responsibility entirely on organisations can arouse suspicion of their motives, and decrease individuals' trust, making them feel like they lack control over their data (e.g. Brandimarte et al., 2013; Kokolakis, 2017). This is also further complicated when considering aspects such as shadow profiling, or how data is shared with third parties beyond the original platform. Future research could therefore explore how to best address and balance these issues.

5. Conclusion

In sum, our study examined how people understand online privacy, its relationship to targeted advertising, and how they manage/avoid different types of such content online. Our aim was to explore whether Cambridge Analytica was at the forefront of people's minds

during this time. By conducting an inductive thematic analysis, our findings highlighted a number of key insights regarding how people feel about psychologically tailored advertisements, and their understanding of how algorithms may use their online data. Overall, most people were aware of the Cambridge Analytica scandal and its supposed attempts to influence people's political preferences. However, they lacked understanding of how people's data were collected and used in such settings, and that their personal information could be inferred from others within their networks. Despite expressing concern over how organisations may use their data in future, all participants believed they would be immune to any attempts to persuade/influence their behaviour. Future research could further examine these concepts and attempt to establish new ways to encourage users to more actively protect themselves online.

6. Acknowledgments

This work was part funded by the Centre for Research and Evidence on Security Threats (Economic & Social Research Council Award No. ES/N009614/1).

8. References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM Conference on Electronic Commerce*.

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy? In *Digital Privacy: Theory, Technologies, and Practices*.

Acquisto, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. In *ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems*.

Arianezhad, M., Camp, L. J., Kelley, T., & Stebila, D. (2013). Comparative eye tracking of experts and novices in web single sign-on. In *Proceedings of the third ACM conference on Data and application security and privacy - CODASPY '13*. https://doi.org/10.1145/2435349.2435362

Bachura, E., Valecha, R., Chen, R., & Rao, R. R. (2017). Modeling Public Response to Data Breaches. In *Twenty-third Americas Conference on Information Systems* (pp. 1–10). Boston.

Bagrow, J. P., Liu, X., Mitchell, L. (2019). Information flow reveals prediction limits in online social activity. *Nature Human Behaviour*, (1).

Barnes, C. M., & Van Dyne, L. (2009). "I'm tired": Differential effects of physical and emotional fatigue on workload management strategies. *Human Relations*. https://doi.org/10.1177/0018726708099518

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*. https://doi.org/10.5210/fm.v11i9.1394

Baumer, E. P., Sun, R., Schaedler, P. (2018). Departing and Returning: Sense of Agency as an Organizing Concept for Understanding Social Media Non/use Transitions. *Proceedings of the ACM on Human-Computer Interaction-CSCW*, *2*(23).

Baumer, E. P. S., Adams, P., Khovanskaya, V. D., Liao, T. C., Smith, M. E., Sosik, V. S., & Williams, K. (2013). Limiting, leaving, and (re) lapsing: an exploration of facebook non-use practices and experiences. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. https://doi.org/10.1145/2470654.2466446

Baumer, E. P. S., Guha, S., Quan, E., Mimno, D., & Gay, G. K. (2015). Missing Photos, Suffering Withdrawal, or Finding Freedom? How Experiences of Social Media Non-Use Influence the Likelihood of Reversion. *Social Media and Society*. https://doi.org/10.1177/2056305115614851

Belk, R. (2016). Extended self and the digital world. *Current Opinion in Psychology*. https://doi.org/10.1016/j.copsyc.2015.11.003

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters*. https://doi.org/10.1016/j.econlet.2012.04.077

Berg, B. L. (2004). *Qualitative Research Methods for the Social Sciences*. *Pearson Education*. https://doi.org/10.1161/01.CIR.0000015506.36371.0D

Bott, G. J., & Renaud, K. (2018). Are 21-st Century Citizens Grieving for the Loss of Privacy? In *In 2018 Dewald Roode Workshop on Information Systems Security Research.* IFIP Working Group 8.11/11.13.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*. https://doi.org/10.1177/1948550612455931

Braun, & Clarke. (2013). Successful Qualitative Research: A Practical Guide For Beginners. *Successful Qualitative Research A Practical Guide for Beginners*.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*. https://doi.org/10.1191/1478088706qp063oa

Brewer, R. N., & Jones, J. (2015). Pinteresce: Exploring Reminiscence for Implicit Digital

Reciprocity of Older Adults. *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing (CSCW'15)*. https://doi.org/10.1145/2685553.2699017

Cadwalladr, C. (2018). Facebook suspends data firm hired by Vote Leave over alleged Cambridge Analytica ties. *The Guardian*. Retrieved from https://www.theguardian.com/us- news/2018/apr/06/facebook-suspends-aggregate-iq-cambridge-analytica-vote-leave- brexit

Cambridge Analytica. (2018). Retrieved from https://cambridgeanalytica.org

Casanovas, P., De Koker, L., Mendelson, D., & Watts, D. (2017). Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology*. https://doi.org/10.1007/s12553-017-0190-6

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems*. https://doi.org/10.1016/j.dss.2015.12.007

Chen, A., & Potenza, A. (2018). Cambridge Analytica's Facebook Data Abuse Shouldn't Get Credit For TRUMP. Retrieved January 19, 2019, from https://www.theverge.com/2018/3/20/17138854/cambridge-analytica-facebook-data-trump-campaign-psychographic-microtargeting

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2017.12.001

Dabbish, L., Kraut, R., Fussell, S., & Kiesler, S. (2005). Understanding email use: predicting action on a message. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems SE - CHI '05*. https://doi.org/http://doi.acm.org/10.1145/1054972.1055068

Deuker, A. (2010). Addressing the privacy paradox by expanded privacy awareness – the example of context-aware services. In *IFIP Advances in Information and Communication Technology*. https://doi.org/10.1007/978-3-642-14282-6_23

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*. https://doi.org/10.1287/isre.1060.0080

Duggan, M., & Smith, A. (2016). The Political Environment on Social Media.

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media and Society*. https://doi.org/10.1177/1461444810385389

Eslami, M., Kumaran, S. R. K., Sandvig, C., & Karahalios, K. (2018). Communicating Algorithmic Process in Online Behavioral Advertising. *Communicating Algorithmic Process in Online Behavioral Advertising*. https://doi.org/https://doi.org/10.1145/3173574.3174006

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., … Sandvig, C. (2015). I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in news feeds. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/2702123.2702556

Facebook. (2019). What are my ad preferences and how can I adjust them? Retrieved January 19, 2019, from https://www.facebook.com/help/247395082112892?helpref=uf_permalink

Festinger, L. (1957). A theory of cognitive dissonance. *Scientific American*. https://doi.org/10.1037/10318-001

Fiesler, C., & Hallinan, B. (2018). “We are the product”: Public reactions to online data sharing and privacy Controversies in the media. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3173574.3173627

Flender, C., & Müller, G. (2012). Type indeterminacy in privacy decisions: The privacy paradox revisited. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-35659-9_14

Garcia, D. (2017). Leaking privacy and shadow profiles in online social networks. *Science Advances*. https://doi.org/10.1126/sciadv.1701172

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*. https://doi.org/10.1016/j.cose.2018.04.002

Google. (2019). About ad settings. Retrieved January 19, 2019, from https://support.google.com/ads/answer/2662856?hl=en-GB

Guha, S., Baumer, E. P., Gay, G. K. (2018). Regrets, I’ve Had a Few: When Regretful Experiences Do (and Don’t) Compel Users to Leave Facebook. In *In Proceedings of the 2018 ACM Conferene on Supporting Groupwork* (pp. 166–177). ACM.

Gupta, M., & Sharman, R. (2012). Determinants of Data Breaches: A Categorization-Based Empirical Investigation. *Journal of Applied Security Research*. https://doi.org/10.1080/19361610.2012.686098

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people’s job search. *IEEE Security and Privacy*. https://doi.org/10.1109/MSP.2013.64

Hargittai, E., & Marwick, A. (2016). " What Can I Really Do? " Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*.

https://doi.org/10.1016/j.cub.2004.01.035

Hern, A. (2017). How social media filter bubbles and algorithms influence the election. Retrieved April 3, 2020, from https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles

Hern, A. (2018a). Cambridge Analytica scandal "highlights need for AI regulation." Retrieved January 19, 2019, from https://www.theguardian.com/technology/2018/apr/16/cambridge-analytica-scandal-highlights-need-for-ai-regulation

Hern, A. (2018b). How to check whether Facebook shared your data with Cambridge Analytica. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica

Hinds, J., Joinson, A. (n.d.). Human and computer personality prediction from digital footprints. *Current Directions in Psychological Science*.

Hinds, J., Joinson, A. (2018). What demographic attributes do our digital footprints reveal? A systematic review. *PLoS ONE*, *13*(11).

Hirsh, J. B., Kang, S. K., & Bodenhausen, G. V. (2012). Personalized Persuasion: Tailoring Persuasive Appeals to Recipients' Personality Traits. *Psychological Science*. https://doi.org/10.1177/0956797611436349

Jia, H., & Xu, H. (2016). Measuring individuals' concerns over collective privacy on social networking sites. *Cyberpsychology*. https://doi.org/10.5817/CP2016-1-4

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*. https://doi.org/10.1287/isre.1120.0441

Keith, M.J., Maynes, C., Lowry, P. B., & Babb, J. (2014). Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In *ICIS*. https://doi.org/10.13140/2.1.3164.6403

Keith, Mark J, Lowry, P. B., Evans, C. M., & Babb, J. S. (2014). Privacy fatigue : The effect of privacy control complexity on consumer electronic information disclosure Privacy fatigue : The effect of privacy control complexity on consumer electronic information disclosure. In *ICIS2014*. https://doi.org/10.13140/2.1.3164.6403

Kelley, T., & Bertenthal, B. I. (2015). Tracking Risky Behavior On The Web: Distinguishing Between What Users 'Say'' And "Do''."' *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)*.

Kitchgaessner, S. (2018). Cambridge Analytica used data from Facebook and Politico to help Trump. *The Guardian*.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*. https://doi.org/10.1016/j.cose.2015.07.002

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Kübler-Ross, E., & Kessler, D. (2005). *On grief and grieving: Finding the meaning of grief through the five stages of loss*. Simon and Schuster.

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa.2014.10.012

Lee, A. R., Son, S. M., & Kim, K. K. (2016). Information and communication technology overload and social networking service fatigue: A stress perspective. *Computers in*

Human Behavior. https://doi.org/10.1016/j.chb.2015.08.011

Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization-privacy paradox in mobile wellness healthcare services. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2014.11.031

Magee, T. (2018). The most significant UK data breaches. Retrieved December 3, 2018, from https://www.computerworlduk.com/galleries/data/most-significant-uk-data-breaches-3662915/

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media and Society*. https://doi.org/10.1177/1461444814543995

Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*. https://doi.org/10.1073/pnas.1710966114

Moon, Y. (2002). Personalization and personality: Some effects of customizing message style based on consumer personality. *Journal of Consumer Psychology*. https://doi.org/10.1207/15327660260382351

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Park, S. H., Lee, H. J., Han, S. P., & Lee, D. H. (2009). User age profile assessment using SMS network neighbors' age profiles. In *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*. https://doi.org/10.1109/WAINA.2009.136

Park, Y. J. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*. https://doi.org/10.1177/0093650211418338

Pasquale, F. (2015). *The Black Box Society*. *The Black Box Society*.

https://doi.org/10.4159/harvard.9780674736061

Petronio, S. (1991). Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. *Communication Theory*. https://doi.org/10.1111/j.1468-2885.1991.tb00023.x

Petronio, S. (2002). Communication Privacy Management Theory. *Boundaries of Privacy: Dialectics of Disclosure*. https://doi.org/10.1080/15267431.2013.743426

Phelan, C., Arbor, A., & Resnick, P. (2016). It's Creepy, But It Doesn't Bother Me. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2858036.2858388

Portwood-Stacer, L. (2013). Media refusal and conspicuous non-consumption: The performative and political dimensions of Facebook abstention. *New Media and Society*. https://doi.org/10.1177/1461444812465139

Posey Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*. https://doi.org/10.1108/09685221111173049

Quitfacebookday.com. (2010). We're Quitting Facebook. Retrieved January 19, 2019, from http://www.quitfacebookday.com/

Raine, L. (2018). Americans' complicated feelings about social media in an era of privacy concerns. Retrieved January 19, 2019, from http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*. https://doi.org/10.1080/00223980.1975.9915803

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in Human*

Behavior. https://doi.org/10.1016/j.chb.2008.12.024

Schreiner, M., & Hess, T. (2015). Examining the Role of Privacy in Virtual Migration: The Case of WhatsApp and Threema. In *Proceedings of Americas Conference on Information Systems*.

Seligman, M. E. (1972). Learned Helplessness. *Annual Review of Medicine*, *23*(1), 407–412.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/2556288.2557421

Slawson, N. (2018, April 7). Faceblock campaign urges users to boycott Facebook for a day. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/07/faceblock-campaign-urges-users-boycott-facebook-for-one-day-protest-cambridge-analytica-scandal

Solove, D. (2007). "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*.

Statista. (2018). Distribution of Facebook users worldwide as of October 2018, by age and gender. Retrieved January 19, 2019, from https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/

Stieger, S., Burger, C., Bohn, M., & Voracek, M. (2013). Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking*. https://doi.org/10.1089/cyber.2012.0323

Stone, A. A., Bachrach, C. A., Jobe, J. B., Kurtzman, H. S., Cain, V. S. (1999). *The science of self-report: Implications for research and practice*. *Contemporary Psychology-Apa Review of Books*.

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*. https://doi.org/10.1145/1958824.1958880

Sweeten, G., Sillence, E., & Neave, N. (2018). Digital hoarding behaviours: Underlying motivations and potential negative consequences. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2018.03.031

Tambini, D. (2018, April 27). What should be done with Facebook - break it up, or regulate it? *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2018/apr/27/facebook-regulate-tech-platforms

Tamblyn, T. (2018, April 18). Facebook's Facial Recognition Software Is Now In The UK. Here's How It Works. *Huffington Post*. Retrieved from https://www.huffingtonpost.co.uk/entry/facebooks-facial-recognition-software-is-now-in-the-uk-heres-how-it-works_uk_5ad73798e4b03c426daa08a9

Thomas, L., & Briggs, P. (2014). An older adult perspective on digital legacy. In *Proceedings of the 8th Nordic Conference on Human-Computer Interaction Fun, Fast, Foundational - NordiCHI '14*. https://doi.org/10.1145/2639189.2639485

Timms, H., & Heimans, J. (2018, April 16). Commentary: #DeleteFacebook is just the beginning. Here's the movement we could see next. *Fortune*. Retrieved from http://fortune.com/2018/04/16/delete-facebook-data-privacy-movement/

Trump, K. (2018, March 23). Four and a half reasons not to worry that Cambridge Analytica skewed the 2016 election. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/monkey-cage/wp/2018/03/23/four-and-a-half-reasons-not-to-worry-that-cambridge-analytica-skewed-the-2016-election/?noredirect=on&utm_term=.2c05b7e715ec

Van Gool, E., Van Ouytsel, J., Ponnet, K., & Walrave, M. (2015). To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2014.11.036

Vitak, J., Shilton, K., & Ashktorab, Z. (2016). Beyond the Belmont principles: Ethical challenges, practices, and beliefs in the online data research community. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW*. https://doi.org/10.1145/2818048.2820078

Vraga, E. K., Thorson, K., Kligler-Vilenchik, N., & Gee, E. (2015). How individual sensitivities to disagreement shape youth political expression on Facebook. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2014.12.025

Welch, C. (2018, March 27). How to stop Facebook from looking for you with face recognition. *The Verge*.

Winder, D. (2019). Data Breaches Expose 4.1 Billion Records In First Six Months of 2019.

Wisniewski, P. J., Richter Lipford, H., & Wilson, D. (2012). Fighting for My Space: Coping Mechanisms for SNS Boundary Regulation. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*. https://doi.org/10.1145/2207676.2207761

Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*. https://doi.org/10.1073/pnas.1418680112

Zamal, F. Al, Liu, W., & Ruths, D. (2011). Homophily and Latent Attribute Inference : Inferring Latent Attributes of Twitter Users from Neighbors. *Science*.

Zhang, S., Zhao, L., Lu, Y., & Yang, J. (2016). Do you get tired of socializing? An empirical explanation of discontinuous usage behaviour in social network services. *Information*

and Management. https://doi.org/10.1016/j.im.2016.03.006

Zou, Y., Mhaidli, A. H., Mccall, A., & Schaub, F. (2018). "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. *USENIX Association*.