Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Self-censorship in Social Networking Sites (SNSs) – Privacy concerns, privacy awareness, perceived vulnerability and information management

Mark Warner[1] and Victoria Wang[2]

[1] UCL Interaction Centre, University College London, UK
[2] Institute of Criminal Justice Studies, University of Portsmouth, UK

E-mail: mark.warner@ucl.ac.uk

Received: 03 July 2018
Accepted for publication: 10 February 2019
Published: In Press

Abstract

Purpose - This paper aims to investigate behavioural changes related to self-censorship (SC) in Social Networking Sites (SNSs) as new methods of online surveillance are growing increasingly. In particular, it examines the relationships between self-censorship (SC) and its four related factors: privacy concerns (PC), privacy awareness (PA), perceived vulnerability (PV), and information management (IM).

Methodology - A national wide survey was conducted in the United King-dom (N = 519). The data were analysed to present both descriptive and inferential statistical findings.

Findings - The level of online self-censorship increases as the level of privacy concern increases. The level of privacy concern increases as the levels of privacy awareness and perceived vulnerability increase, and the level of information management decreases.

Contribution - This study extends the literature on online self-censorship, showing that privacy concerns increase the level of self-censorship in SNSs. It provides support for three antecedent factors to privacy concerns which impact upon the level of self-censorship when communicating in SNSs.

Keywords - Self-censorship, privacy concerns, privacy awareness, perceived vulnerability, information management, Social Networking Sites (SNSs)

DOI: 10.1108/JICES-07-2018-0060

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

1. Introduction

The growth of Social Networking Sites (SNSs) has led to an increasing amount of rich personal data being shared and stored online, which challenge the management of personal information and the notion of privacy (Xu, 2012). These personal data could be used for different purposes and by different parties. Individuals are able to conduct surveillance and collect data on one another, especially members of the same networking site (Krasnova et al., 2009). Businesses have developed new methods to exploit data for their own commercial ends (Sun et al., 2016). Governments have also developed a wide range of bulk-surveillance technologies to scrutinise these data (Lyon, 2015). Moreover, since the terrorist attacks of 9/11, governments' electronic surveillance has grown exponentially. Twelve years later, Snowden revealed the extent of this electronic surveillance in a public release of a large cache of sensitive documents detailing previously unknown surveillance capabilities of governments, including those of the United Kingdom (UK) (MacAskill et al., 2013). Post-Snowden, the general perception of threats to personal information online has openly shifted from a predominant focus on commercial intelligence to government intelligence activities related to the prevention and detection of security threats (Wilton, 2017).

This shift has brought about a series of public debates in the UK concerning the balance between privacy and security. These debates have resulted in three independent surveillance reviews (Anderson, 2015; House of Commons, 2015; Royal United Services Institute, 2015) and the introduction of the Investigatory Powers Bill, outlining new laws governing surveillance powers (gov.uk, 2016). In order to better balance security and privacy, it is important to evaluate the social costs that increased security and surveillance could generate. One proposed social cost is the perceived need for individuals to self-censor their online communication as a result of privacy concerns (Richards, 2012). Whilst previous researchers have explored self-censorship in social networks, these have focused on self-censorship around controversial events of high significance to authorities such as US airstrikes in Iraq and Syria (Stoycheff, 2016), and discussions related to NSA surveillance (Hampton et al., 2014). Other research has explored self-censorship around less sensitive information such as political views (Liu et al., 2017) but tested its relationship with self-presentation behaviours rather than privacy concerns and its antecedent factors.

This study looks to address this gap by exploring the possible impact privacy concerns and its antecedent factors have on social media self-censorship in a heightened surveillance climate. We focus our research on SNSs as a significant portion of the population in the UK (and worldwide) now use these services to communicate. By way of a nation-wide survey in the UK (N = 519) in 2016, our study examined the relationships between *self-censorship* (SC) and its four related factors: *privacy concerns* (PC), *privacy awareness* (PA), *perceived vulnerability* (PV), and *information management* (IM). Particularly, it i) evaluates the level of self-censorship of UK residents in relation to privacy concerns in SNSs; and ii) measures possible impacts of privacy awareness, perceived vulnerability, and information management on individuals' behaviour in SNSs, and how these relate to their privacy concerns, and in turn, their self-censorship. The research findings present a general picture of self-censorship in SNSs of UK residents as various forms of surveillance technologies are increasingly penetrating every arena of the online world. In particular, these findings indicate that the level of

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

online self-censorship increases as the level of privacy concern increases. The level of privacy concerns increases as the levels of privacy awareness and perceived vulnerability increase, and the level of information management decreases. When evaluating new types of electronic surveillance, or when reviewing existing surveillance policy (as occurred in the UK post-Snowden), the benefits to security that these systems provide should be weighed against their costs. Yet, a lack of academic research on social costs such as self-censorship, make this challenging. Our research on self-censorship in SNSs as a social cost of surveillance add to the body of knowledge in this area and can be used to help in future cost/benefit evaluations.

2. Self-censorship and its related factors – privacy concerns, privacy awareness, perceived vulnerability and information management

Self-censorship – often understood as a behaviour which presents or modified self-disclosures due to fear of negative social consequences – has been examined from organisational, political, interpersonal perspectives (Byeon et al., 2017; Woo et al., 2008; Postmes et al., 2002). Self-censorship could occur from fear of political authorities and influential organisations (Byeon and Chung, 2012; Sidhu, 2007; Solomon and Samp, 1998; Schauer, 1978). It can also occur from fear of being perceived negatively in certain social circles (Stoycheff, 2016). In Noelle-Neumann's (1993; 1974) theory, the Spiral of Silence, she suggested that through a fear of being isolated, individuals self-monitor their environments to assess the correlation between perceived general societal beliefs and their own beliefs. Stoycheff (2016) further indicates that individuals are more likely to censor themselves when they believe that i) they are being watched through surveillance, and ii) at the same time, the surveillance is justified. An example is this was identified in a study into post-Snowden internet search behaviours which found self-censorship of keywords that users felt may get them into trouble with the US authorities (Mathews & Tucker, 2015).

In terms of self-censorship online, previous research on e-commence has explored factors affecting the extent of online disclosure in order to conduct an e-commerce transaction effectively (e.g., Dinev et al., 2008; Dinev and Hart, 2006; Culnan and Armstrong, 1999). Previous research has also modelled the extent of information sharing while using a specific online technology (Das and Kramer, 2013; Krasnova et al., 2009; Xu, 2007; Adams and Sasse, 2001), or within a specific social context (Bansal, et al., 2010). In particular, previous research on SNSs has discussed self-censorship as a boundary regulation strategy on these sites (e.g., Das and Kramer, 2013; Sleeper et al., 2013; Stutzman and Hartzog, 2012). In a study of 3.9 million Facebook users, Das and Kramer (2013) identified 71% of those users as having performed some forms of self-censorship. More recently, Sangho et al.'s (2017) research has indicated that the degree of self-censorship in SNSs regarding large corporations is mediated by the amount of knowledge about, and the perceived power of, these corporations.

In selecting the antecedent privacy concern factors, we draw from previously developed models. Firstly, we explored Dinev and Hart's (2005) model which found (privacy) awareness and Internet literacy as factors affecting privacy. As this research

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

was carried out in 2005 when social penetration of the Internet was much less than it is now - with the Internet now pervasive through western society - we have excluded Internet literacy as a factor. Dinev and Hart (2006) and Xu et al.'s (2008) studies both found support for privacy risk as an antecedent factor to privacy concerns, whilst Dinev & Hart, 2004 found perceived vulnerability as an antecedent factor. As risk is difficult for individuals to ascertain, especially in online environments where there is a high degree of uncertainty around surveillance capabilities, we have included end users' perceptions of their own vulnerabilities. Finally, although previous research found support for control as a privacy related factor (e.g. Xu et al., 2008), we acknowledge Nissenbaum's (2009) Privacy as a Contextual Integrity (PCI) which argues that appropriate flow of information, rather than absolute control, is a more realistic expectation when communicating in today's online social networks.

To develop our research hypotheses and formulate the questions in our survey, we reviewed existing literature on factors related to self-censorship, privacy concern (PC), and our selected antecedent factors: privacy awareness (PA), perceived vulnerability (PV), and information management (IM).

2.1. Privacy Concerns

Privacy is defined differently by different individuals from varying perspectives. A comprehensive critical analysis of existing literature on theoretical foundations and definitions of privacy could be found in Allmer (2011). Generally, there is a tendency to view the notion of privacy in dichotomies of 'private' and 'public', or 'sensitive' and 'non-sensitive' (Froomkin, 2000; Posner, 1978). More recently, Nissenbaum's (2009) seminal concept of PCI suggests that this dichotomised view of privacy fails to consider the different social contexts in which we live our lives, and also the changes in our willingness to disclose varying levels of 'selves' within these differing contexts. Thus, data about a person from one sphere must be treated quite differently from data about the same person from another sphere, which asks for particular scrutiny when combining information. The concept of PCI is empirically tested on mobile device users, which identifies the influences particular contextual factors and information uses have on privacy expectancy (Martin and Shilton, 2016). However, current technologies, such as various data mining techniques that are able to analyse the continuous stream of data following from ubiquitous computing devices, could give rise to situations in which the concept becomes insufficient (Matzner, 2014).

Nevertheless, the types of information that we are willing to reveal to our family members differ from that which we are willing to share with our work colleagues. Schau and Gilly (2003) view privacy as instrumental in providing control over how information about the self is distributed to others. Perhaps, privacy could be perceived as an instrument of autonomy that enables self-determination over who we are and how we are perceived in society (Solove, 2007; Froomkin, 2000). In a society without privacy, self-censorship of personal information would become irrelevant.

Privacy concerns (PC) have been shown to negatively impact upon an individual's willingness to reveal personal information when carrying out transactions online (Dinev et al., 2008). These concerns form a part of the Privacy Calculus Model (PCM), which proposes an individualistic, context specific, and cost-benefit analysis of behaviours

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

when carrying out online economic transactions (Culnan and Armstrong, 1999). While, in the most part, general online communications differ from economic transactions, the concept of privacy as a cost weighed against a benefit has much broader contextual applicability. The ComRes 2015 Internet Privacy Survey (ComRes, 2015) found that 79% of UK respondents (n=1000) were concerned about their online privacy – an increase of 11% from 2013 when the survey was previously conducted (ComRes, 2013). A study carried out in 2016, by the National Telecommunications & Information Administration (NTIA) in the United States, found that 84% of Internet connected households had concerns over their online privacy (NTIA, 2016) – an even greater percentage compared to that of the UK. The high number of respondents reporting concerns over online privacy in these studies suggests the need to fully understand some key factors involved in the formation of privacy concerns. Based on these discussions, this research hypothesises that:

Hypothesis 1. As the level of privacy concerns increases, the level of self-censorship will increase.

2.2. Privacy Awareness

Privacy awareness (PA) can be interpreted as the extent to which an individual is informed about privacy related factors. This would include privacy practices, privacy policies, and the use of disclosed information, as well as the individual's varying levels of consciousness about some possible impacts that each of these factors could have on his/her ability to preserve his/her private space (Phelps et al., 2000; Dunfee et al., 1999). Dinev and Hart (2006) suggested that social (privacy) awareness is a predictor of privacy concerns (PC) – individuals with high social (privacy) awareness will closely follow issues related to privacy, including practices, policies and consequences of any potential privacy violations.

An earlier study of Internet users identified that 69% of those users chose not to disclose data on a website due to being unsure of how their data may be used (Hoffman et al., 1999). Barnes (2006) suggested that teenagers are more likely to disclose personal information online than adults, owing to a significantly lower awareness of the public nature of the Internet. Adults, with a higher level of awareness, were less likely to disclose and were more concerned about any potential invasions to privacy (ibid.). While awareness may be a factor; adults, having lived longer than teenagers and having built up a strong identity and public reputation, may feel that they have more social-capital to lose. Buitelaar (2014) describes this as a narrative identity, which, in the context of online identity management, involves people spending considerable time authoring their own online identity, creating the story of their lives to reflect a credible personality. For Xu et al. (2008), in the context of e-commerce, at least, an individual's privacy awareness (PA) positively influences their disposition to value privacy. More recently, Zhong et al.'s (2016) research identified a causal relationship between the Chinese government's internet censorship system and ordinary Chinese people's reactions – perceived internet censorship significantly decreases the willingness to talk about sensitive issues.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Snowden (2015) when discussing in an online question and answer session on the topic of Internet surveillance, stated that "The biggest change (caused by his leaking of sensitive government surveillance information) has been in *awareness*". It could be argued that this increase in awareness of surveillance being carried out by UK intelligence services has the potential to increase individuals' perception of their own lack of privacy online, and thus, negatively impacting self-censorship. Using these discussions above as a springboard, and focused on the context of SNSs, this research hypothesises that:

Hypothesis 2. As the level of privacy awareness increases, the level of privacy concerns when posting and communicating online will increase.

2.3. Perceived Vulnerability

In Margulis (1977)'s formal definition of privacy, vulnerability was included as a factor – "Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (p. 10). This definition clearly identifies vulnerability as a factor that is increased when control over information is at stake.

The notion of perceived vulnerability (PV) discusses how an individual might feel exposed in some way, due to a lack of knowledge or expertise (Corritore et al., 2003). Individuals could be more vulnerable when they interact and disclose themselves online than offline. This is because online data can be easily misinterpreted, misused, disclosed and even sold to third parties by data receivers (Riegelsberger et al., 2009). It is, moreover, often difficult for individuals to evaluate any potential risks to their personal data online, and to estimate the value of these data.

Internet users are regularly exposed to risks of abuse to the information they disclose online, which may increase their perception of vulnerability (Dinev & Hart, 2004). Petronio and Altman's (2002) Communication Privacy Management (CPM) theory suggests that individuals make decisions on how to manage their private information using a set of rules. Those decisions change according to the risk reward levels that are adjusted either through an increase in vulnerability, or a reduction in the perceived benefits of disclosure. The factor of vulnerability has been previously tested as an antecedent to privacy concerns (PC) – Internet users' perceptions of vulnerability may increase when they are exposed to privacy violations (Dinev and Hart, 2004). Based on these previous findings, this research hypothesises that:

Hypothesis 3. As the level of perceived vulnerability increases, the level of privacy concerns when posting and communicating online will increase.

2.4. Information Management

The notion of privacy is associated with the extent of control over the management of information (Margulis, 2003; Altman, 1976; Fried, 1968;). The notion of information management (IM) discusses individuals' perceptions of the extents of control that they have over how others could use their personal information (Nissenbaum, 2009).

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Xu et al. (2008) examined the factor of perceived privacy control and found a statistically significant correlation between perceived control and privacy concerns in the context of social networking. An earlier study on privacy control found that individuals' choices of methods of privacy control differed depending on their self-constructed values (Xu, 2007) – those with individualistic values preferred to retain direct personal control; while those with collectivistic values preferred control via proxy mechanisms, such as government and industry self-regulation policies.

Although control is an important element of privacy, simply not having control will not necessarily result in an invasion of, or reduction in, privacy; as long as the information flows appropriately (Nissenbaum, 2009). Petronio and Altman's (2002) Communication Privacy Management Theory (CPM) used the metaphor of boundaries to illustrate the defining lines of ownership over information. They (2002) suggested a rule-based management system to manage access to information, with deviations from these rules resulting in a loss of information control, and subsequently, privacy violations. In this research, the perceived appropriateness of information management (IM) is examined rather than information control; as absolute control over communications data is not realistic. It is hypothesised that:

Hypothesis 4. As the level of information management increases, the level of privacy concerns will decrease.

3. Method

The four research hypotheses were empirically tested using data collected through an online survey. The survey consisted of five distinct sections i) self-censorship (SC); ii) privacy concerns (PC); iii) privacy awareness (PA); iv) perceived vulnerability (PV); and v) information management. Each section consisted of several statements which we refer to as measurement 'items'. Participants were asked to indicate the extent of their concern over, or approval of, each of these items. The items were developed using a mixture of existing and new measures, which were identified through a comprehensive review of the relevant literature. Existing measures, where possible, were used. These were, however, adapted to reflect some specific nature and characteristics of current Information and Communications Technologies (ICTs), and also to avoid any generalised responses concerning information privacy.

The items concerning privacy concerns (PC) and information management (IM) were developed and based on items that were originally identified by Smith et al. (1996) study. Our items about privacy awareness (PA) were developed based on items in Xu et al.'s (2008) study on the formation of individual privacy concerns. Our items on perceived vulnerability (PV) were based on the items developed in Dinev and Hart's (2004) study, which explored privacy concerns relating to government surveillance. Items concerning self-censorship (SC) were developed based on our general understanding of the current literature.

In 2016, we carried out a random sampling of UK residents across the country, by way of SurveyMonkey Inc, to increase the generalisability of the study to the UK population. As a visual mode of administration, online surveys are subject to less normative bias

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

than more direct methods, including face-to-face and telephone surveys (e.g., Grandcolas et al., 2003). Online surveys provide, however, a cost and time effective means to achieve large sample sizes across a wide geographical area (Hewson et al., 2015). Further, the Internet usage statistics from the UK Office of National Statistics (ONS) suggested that the internet was used daily or almost daily by 82% (41.8 million) of adults (16+) in Great Britain in 2016 (Office of National Statistics, 2016). More importantly, the purpose of this study was to examine UK adults' (18 or above) self-censorship in SNSs. We, therefore, were only concerned with the population that was actively using the Internet to communicate. Ethical approval was obtained from the host university. Measures were taken to ensure that Survey Monkey Inc. collected no identifiable information in order to maintain participants' anonymity and confidentiality. Permission was obtained from each of the participants surveyed. Each question in the survey was defined as voluntary, allowing participants to skip questions that they preferred not to answer. In total, 519 valid responses were retrieved (see: Table 1). This survey had a well distributed demographic sample, by age, gender, income group and geographic location.

Table 1. Descriptive statistics of the survey respondents (n = 519)

Age	18 - 29	104	20.0%
	30 - 44	131	25.2%
	45 - 59	130	25.0%
	60+	151	29.1%
	Prefer not to answer	3	0.6%
Gender	Female	264	50.9%
	Male	252	48.6%
	Prefer not to answer	3	0.6%
Income	£0 to £4,999	28	5.4%
	£5,000 to £9,999	32	6.2%
	£10,000 to £14,999	45	8.7%
	£15,000 to £19,999	40	7.7%
	£20,000 to £29,999	75	14.5%
	£30,000 to £39,999	60	11.6%
	£40,000 to £49,999	53	10.2%
	£50,000 to £59,999	23	4.4%
	£60,000 to £69,999	21	4.0%
	£70,000 to £79,999	16	3.1%
	£80,000 to £89,999	9	1.7%
	£90,000 to £99,999	8	1.5%
	£100,000 or more	18	3.5%
	Prefer not to answer	88	17.0%
Location	East	47	9.1%
	East Midlands	29	5.6%
	London	47	9.1%
	North East	13	2.5%
	North West	55	10.6%
	Northern Ireland	11	2.1%
	Scotland	49	9.4%
	South East	95	18.3%
	South West	46	8.9%
	Wales	25	4.8%
	West Midlands	41	7.9%
	Yorkshire and the Humber	52	10.0%
	Prefer not to answer	9	1.7%

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

An Exploratory Factor Analysis (EFA) was used to analyse the results. This is a widely used statistical technique, which has appeared in a range of academic areas in order to analyse survey data and to develop research instruments (Costello and Osborne, 2005). In this study, it was used to examine the inter-correlation of our survey items and also to reduce those items into factors for further analyses. The internal reliability of each factor was then tested. Therefore, the linear correlation between each factor was measured using Pearson's R correlation coefficients.

4. Results

4.1. Self-Censorship (SC)

Our findings show that many participants reported a level of self-censorship. Responses were loaded towards the higher end of the scale, with 63.1% of participants agreeing or strongly agreeing to self-censorship online. However, 22.3% either disagreed or strongly disagreed (see: Table 2).

Table 2: Self-Censorship Frequency Table

Scale Item	Responses	Percentage
Strongly Disagree	134	6.5%
Disagree	326	15.8%
Neither agree not disagree	305	14.7%
Agree	786	35.6%
Strongly Agree	568	27.5%

The mean response to *'previously deciding not to post or communicate something online due to privacy concerns'* was 3.88, with 74.6% agreeing or strongly agreeing (Table 3). The mean response to *'having previously edited something before posting or communicating online due to privacy concerns'* was 3.84, with 74% agreeing or strongly agreeing. Those who had *'previously limited their use of SNSs due to privacy concerns'*, achieved a mean score of 3.72, with 65.7% agreeing or strongly agreeing. The mean response to having *'previously stopped using a SNS due to privacy concerns'* was 3.03, with 41.0% of participants disagreeing or strongly disagreeing.

Table 3: Individual survey item responses to the privacy related self-censorship factor

Item	1 Strongly Disagree	2	3	4	5 Strongly Agree	s.d	Mean
In the past, I have decided not to post or communicate something online due to privacy concerns.	4.4%	9.7%	11.2%	42.4%	32.2%	1.10	3.88
In the past, I have edited something before posting or communicating it online due to privacy concerns.	4.5%	9.3%	12.2%	46.3%	27.7%	1.07	3.84

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

In the past, I have limited my use of an online social messaging service due to privacy concerns.	5.0%	15.0%	14.3%	34.5%	31.2%	1.20	3.72
In the past, I have stopped using an online social messaging service due to my privacy concerns.	12.0%	29.0%	21.3%	19.1%	18.6%	1.31	3.03

4.2. Privacy Concerns (PC)

Here, our participants, in general, were concerned about their online privacy (see: Table 4). The data was loaded towards the higher end of the scale with 69.5% of participants somewhat to extremely concerned; while 30.5% were not at all concerned or only slightly concerned.

Table 4: Privacy Awareness Frequency Table Overview

Scale Item	Responses	Percentage
Strongly Disagree	216	10.5%
Disagree	357	17.4%
Neither agree not disagree	560	27.2%
Agree	548	26.6%
Strongly Agree	377	18.3%

In analysing items in the factor of privacy concerns (PC) (Table 5), concerns over *'online social messaging providers collecting too much information'* proved to have the highest mean response of 3.48, with 55.6% being somewhat to extremely concerned. Being *'watched or monitored when communicating online'* caused the least concern with a lower mean of 2.98, with 65.9% of participants being slightly to moderately concerned.

Table 5: Individual survey item responses to the privacy awareness perceptions factor

Item	1 Strongly Disagree	2	3	4	5 Strongly Agree	s.d.	Mean
I am aware of the privacy policies implemented by the online social messaging providers I use.	9.8%	22.4%	33.6%	24.5%	9.7%	1.12	3.02
I am aware that my personal information or communications could be made available to government agencies.	9.9%	12.6%	21.5%	24.4%	31.7%	1.31	3.56
I am aware of the wider issues around data privacy within the UK from the news and other sources	7.7%	13.3%	25.7%	31.9%	21.3%	1.19	3.46

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

I am aware of the types of information I have agreed online social messaging providers can store about me.	14.3%	20.7%	27.5%	25.2%	12.2%	1.23	3.00

4.3. Privacy Awareness (PA)

Under half of our participants (44.9%) either greed or strongly agreed that they were aware of privacy issues when communicating in SNSs. Over a quarter of the participants (27.9%) disagreed or strongly disagreed that they were aware of privacy issues. A similar number (27.2%) indicated neutrality (see: Table 6).

Table 6: Perceived Vulnerability Frequency Table

Scale Item	Responses	Percentage
Strongly Disagree	71	2.7%
Disagree	70	2.7%
Neither agree not disagree	285	11.0%
Agree	1118	43.2%
Strongly Agree	1045	40.4%

The mean of responses to the item of *'awareness of personal information could be made available to government agencies'* was 3.56 (Table 7), with 56.1% agreeing or strongly agreeing. The item on *'awareness of the types of information that SNSs are storing'* received a mean response of 3.0. This was followed closely by *'individuals' awareness of SNSs' privacy policies',* with a mean of 3.02.

Table 7: Individual survey item responses to the perceived vulnerabilities factor

Item	1 Strongly Disagree	2	3	4	5 Strongly Agree	s.d.	Mean
My personal information collected by online social messaging providers, could be sold to third parties.	3.3%	3.5%	10.6%	41.4%	41.2%	0.97	4.14
My personal information communicated or posted online could be misused.	2.1%	1.7%	9.6%	48.0%	38.5%	0.84	4.19
My personal information or communications could be made available to unknown individuals or companies without my knowledge.	2.1%	2.3%	8.1%	44.2%	44.3%	0.86	4.24
My personal information or communications could be made available to government agencies.	3.7%	4.2%	15.6%	35.6%	40.8%	1.03	4.06
My personal information or communications could be used inappropriately.	2.5%	1.7%	11.0%	46.7%	38.0%	0.87	4.16

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

4.4. Perceived Vulnerability (PC)

Our findings demonstrate that a large percentage of participants (83.6%) agreed or strongly agreed with the statement that their 'personal information and communications are vulnerable when communicating in SNSs' (Table 8). Just 5.4% of them did not agree.

Table 8: Appropriate Management Frequency Table Overview

Scale Item	Responses	Percentage
Strongly Disagree	107	24.5%
Disagree	746	36.0%
Neither agree not disagree	474	22.9%
Agree	234	11.3%
Strongly Agree	111	5.4%

Each item in this factor was in fact loaded towards the higher end of the scale (Table 9). The item on *'personal information or communications being made available to unknown individuals or companies without their knowledge'* received the highest mean response of 4.24, with 88.5% agreeing or strongly agreeing. The item *'personal information or communications being made available to government agencies'* received the lowest mean response of 4.06, with 76.4% agreeing or strongly agreeing.

Table 9: Individual survey item responses to the perception of the appropriateness of the management of information factor

Item	1 Strongly Disagree	2	3	4	5 Strongly Agree	s.d.	Mean
Online social messaging providers never share my personal information with anyone I have not intended.	22.9%	38.0%	27.7%	7.1%	4.2%	1.04	3.68
Government agencies only have access to my private information and online communications after they obtain strict permission.	22.7%	28.9%	26.0%	16.0%	6.4%	1.19	3.46
I have control over who has access to the private information and communications I post over online social messaging services.	23.6%	37.6%	20.5%	12.9%	5.4%	1.14	3.61
I have control over how the data that I post or communicate online is used.	28.7%	39.5%	17.2%	9.1%	5.4%	1.12	3.77

4.5. Information Management (IM)

Just over 60% of the participants either disagreed or strongly disagreed with the general statement that '*there was an appropriate management of the data that individuals disclose while posting and communicating online'* (Table 10). Just over 16% of them agreed or strongly agreed that '*the data which they disclosed in SNSs was managed appropriately'*.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Table 10: Privacy Concern Frequency Table

Scale Item	Responses	Percentage
Not at all concerned	329	10.6%
Slightly concerned	618	19.9%
Somewhat concerned	612	19.7%
Moderately concerned	838	27.0%
Extremely concerned	707	22.8%

The item on individuals' 'control over how data posted or communicated online is used' received the highest mean response of 3.77, with 68.2% disagreeing or strongly disagreeing that they had control over their data.

Table 11: Individual survey item responses to the privacy concerns when posting or communicating over the Internet factor

Item	1 Not at all Concerned	2	3	4	5 Extremely Concerned	s.d.	Mean
I am concerned that the information I post or communicate online will be used in a way that I have not foreseen.	6.6%	19.9%	24.2%	30.4%	19.0%	1.18	3.35
I am concerned about posting or communicating information online, because of what others might do with it.	8.3%	20.3%	19.4%	28.3%	23.6%	1.27	3.39
I am concerned that I am being watched or monitored when communicating online.	17.8%	22.6%	20.3%	23.0%	16.4%	1.35	2.98
I am concerned about posting information online, because I may never be able to delete it.	11.2%	21.1%	19.1%	25.5%	23.0%	1.33	3.28
I am concerned about posting or communicating information online, because someone might access it who I had not intended.	8.7%	19.3%	18.2%	29.8%	24.0%	1.28	3.41
I am concerned that online social messaging providers are collecting too much information about me.	11.0%	16.2%	17.1%	25.0%	30.6%	1.36	3.48

The item on *'government agencies only having access to individual private information and online communications after obtaining strict permission'* received the lowest mean response of 3.46 with 50% disagreeing or strongly disagreeing with the statement.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

4.6. Exploratory Factor Analysis

We used an Exploratory Factor Analysis (EFA) to determine the number of factors using two methods. We first analysed the Kaiser criterion of retaining factors with eigenvalues > 1.0, followed by a Cattell scree test (Cattell, 1966; Kaiser, 1960). Both methods identified five distinct factors (see: Table 12). To identify the significance of these factors' loadings, sample sizes > 400 were recommended to be loaded with a value > .258 (Stevens, 2012). The results of the EFA (see: Table 12) show that each item has a factor loading > .25, and each item is positively loaded to its anticipated factor. The factor loading values range from 0 to 1, with values closer to 1, which is indicative of a closer relationship between this factor and the latent variable (Beaumont, 2012).

Table 12: Exploratory Factor Analysis Results – Pattern Coefficients

Latent Variable	Item	Factor Loadings				
		Privacy Concerns	Information Management	Privacy Awareness	Perceived Vulnerability	Self-Censorship
Privacy Concerns	Item 1	0.85				
	Item 2	0.88				
	Item 3	0.72				
	Item 4	0.88				
	Item 5	0.68				
	Item 6	0.68				
Information Management	Item 1		0.87			
	Item 2		0.85			
	Item 3		0.65			
	Item 4		0.69			
Privacy Awareness	Item 1			0.79		
	Item 2			0.77		
	Item 3			0.70		
	Item 4			0.68		
Perceived Vulnerability	Item 1				0.89	
	Item 2				0.81	
	Item 3				0.82	
	Item 4				0.80	
	Item 5				0.63	
Self-Censorship	Item 1					0.73
	Item 2					0.83
	Item 3					0.72
	Item 4					0.45

Extraction Method: Maximum Likelihood.
Rotation Method: Oblimin with Kaiser Normalization.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Next, Cronbach's Alpha was used to estimate the reliability of each factor by measuring the consistency of their internal variables. Cronbach's Alpha was examined with each of the five factors. The results, along with the means and standard deviation are presented (see: Table 13). Each factor produced α > .80, which indicates a good internal consistency (George and Mallery, 2003). Both privacy concerns (PC) and perceived vulnerability (PV) scored α > .90, which indicates that some of the variables may be addressing the same item, and are therefore redundant. On removal of two items from the privacy awareness (PA) factor and one from the perceived vulnerability (PV) factor, the alpha scores were reduced. These reductions also indicate a more reliable internal consistency. The factor correlations were, therefore, performed with these items removed.

Table 13. Internal Consistency of each factor

Latent Variable	α	Mean	s.d.
Privacy Concerns	0.93	3.60	0.93
Information Management	0.86	2.37	0.94
Privacy Awareness	0.83	3.25	0.99
Perceived Vulnerability	0.91	4.15	0.78
Self-Censorship	0.81	3.62	0.93

In particular, we examined the correlation coefficient on our survey data using Pearson's R and discovered that *privacy concerns* (PC) is an antecedent of *self-censorship* (SC); and *privacy awareness* (PA), *perceived vulnerability* (PV), and *information management* (IM) are three antecedents of *privacy concerns* (PC) (see: Table 14). These results also demonstrate statistically significant correlations among these factors.

Table 14. Pearson's R correlation results between each factor

Latent Variable	Privacy Concerns	Information Management	Privacy Awareness	Perceived Vulnerability
Information Management	-.230*			
Privacy Awareness	.245*	-.06		
Perceived Vulnerability	.569*	-.368*	.222*	
Self-Censorship	.563*	-.158*	.184*	.467*

*. Correlation is significant at the 0.05 level (2-tailed).

5. Discussions based on the four hypotheses

This paper looks to understand self-censorship behaviours in SNSs, and how certain factors that can cause end-users to become concerned about their privacy can increase levels of self-censorship. We performed an extensive UK wide survey in 2016 (post-Snowden), and analysed this data using a series of statistical methods. In this section we present a structured discussion of the results of our analysis in relation to each of the four proposed hypotheses that were developed from out literature review.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

In doing so, we contribute to the understand of self-censorship behaviour within SNSs, and suggests descriptive explanations for these findings.

5.1. Hypothesis 1. As the level of privacy concerns increases, the level of self-censorship will increase.

The first hypothesis tested the validity of privacy concerns (PC) as an antecedent factor to self-censorship (SC). This, if validated, would merit further analyses to better understand how privacy concerns are formed. Previous researchers identified PC as having a significant influence on self-disclosure levels when transacting online (Dinev, Hart, Mullen, 2008) but did not measure self-censorship in SNSs directly. Other research has identified self-censorship behaviours within SNSs (Das and Kramer, 2013) but not measure correlations with privacy concerns. The findings of the EFA (see: Table 12) demonstrate that self-censorship (SC) and privacy concerns (PC) are distinct factors with a strong correlation (r = .563) (see: Table 14), supporting our hypothesis.

Our findings suggest that the sample of participants were more concerned over inappropriate use of information that they have disclosed at some point in the future, than being actively monitored. This is an interesting finding, but perhaps, not surprising. Being actively monitored would require users to believe that they are being activity targeted by some form of surveillance, differentiating them from the larger population. They may feel that, whilst they are conforming to the laws and norms of the larger society, there is little need for concern over this form of active surveillance. However, the uncertainty of the future and the relative permanence of online data are likely to be the causes of this increased concern over the future use of information disclosed online from less active forms of surveillance. This is particularly significant as the asymmetry between end-users, governments, and SNSs increases as a result of improvements in electronic surveillance and security (Dinev, Hart, Mullen, 2008), meaning end-users are much less aware of how their data is being used for surveillance purposes.

5.2. Hypothesis 2. As the level of privacy awareness increases, the level of privacy concerns when posting and communicating online will increase.

Privacy awareness (PA) can help educate individuals to understand risks to their privacy, and thus, help them make more informed decisions online (Kani-Zabihi and Helmhout, 2012). The results of the factor correlation (see: Table 14) show a statistically significant positive correlation between privacy awareness (PA) and privacy concerns (PC) (r = .245) (see: Table 14). This supports our hypothesis that as the level of privacy awareness increases, the level of privacy concern when posting and communicating online will also increase. From our findings (see: Table 7), the effectiveness of privacy policies in increasing awareness received a mean response of 3.02. The awareness of the types of information being collected by SNSs achieved a mean response of 3.00. These two means are much lower than the other two means of the remaining two items in this factor (see: Table 7). These findings may suggest that

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

existing privacy awareness measures used by SNSs are not sufficiently effective in raising awareness of privacy related issues to users in SNSs. This still coincides with the findings in Jensen and Potts' (2004) work that was carried out more than a decade ago.

Our findings indicate that while transparency by government bodies and commercial organisations are often demanded to better safeguard against privacy violations by users in SNSs, greater awareness may lead to higher levels of concern (see: Table 7) and may increase rates of self-censorship online. Yet, if transparency was to facilitate higher levels of trust, this may have the opposite effect. Those with higher pre-existing concerns about privacy may possess less trust in their data custodians; and may be more likely to seek out other sources of information to better understand potential risks. The model of privacy developed by Adams and Sasse (2001) supported the need for trust in information receivers when evaluating the privacy of information. Previous research, however, found a strong positive relationship between trust and disclosure online (Dinev and Hart, 2006). Therefore, we could postulate that a lack of trust would result in an increase in self-censorship. Our research was also interested in how privacy awareness (PA) directly affects self-censorship (SC) when communicating in SNSs. We found a positive, statistically significant correlation ($r = .184$; see: Table 14) to support previous research (Hoffman et al., 1999).

Past research suggested that privacy concerns (PC) vary between adults and teenagers (Barnes, 2006). By way of a one-way ANOVA on the privacy awareness (PA) factor with 'age' as the independent variable, we tested this theory on our data and did not find a statistically significant difference ($p = .43$). Perhaps, this is because we did not have any data from teenagers as the lowest participant age category in this study was 18-29 (20%).

5.3. Hypothesis 3. As the level of perceived vulnerability increases, the level of privacy concerns when posting and communicating online will increase.

The increased vulnerability of users is an inherent consequence of placing more trust in an information receiver (Riegelsberger et al., 2009). When SNSs users are more aware of how their data will be managed, uncertainty is reduced which may lead to users feeling less vulnerable. If privacy concerns (PC) are affected by the factor of perceived vulnerability (PV), then the more vulnerable users feel, the more likely they are to self-censor.

We analysed the data to explore whether perceived vulnerability (PV) directly affected concerns over privacy (PC). The factor correlation performed (see: Table 14) found a positive correlation between these two factors ($r = .569$) supporting the hypothesis: as perceived vulnerability increases, privacy concern levels also increase. We also identified three statistically significant correlations between reported perceived vulnerability (PV) when communicating in SNSs with (i) self-censorship (SC) behaviour ($r = .467$); (ii) users' awareness of privacy (PA) ($r = .222$*); and (iii) users' perceptions of the appropriate usage and management of their data (IM) ($r = -.368$). These findings

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

support our suggestion that these three factors are interrelated – perceived vulnerability would be reduced when users are more aware of the fact that their data is managed more appropriately according to norms and policies of their SNSs.

In exploring the responses to items in the perceived vulnerability (PV) factor, our participants reported being most vulnerable in relation to other individuals or companies having access to their data without their knowledge. This had a mean response of 4.24 (see: Table 9). The vulnerability felt from other individuals may result in users' performing self-censorship in order to regulate privacy boundaries within these environments (Sleeper et al. 2013; Wisniewski, Lipford & Wilson 2012). Yet, those participants felt the least vulnerable towards having their data made available to government agencies, with a mean response of 4.06 (see: Table 9). This contrast suggests that either our participants have more confidence in our government agencies, or perhaps, they feel that the risk of having their vulnerabilities exploited by a Government actor is less than from other individuals or commercial entities. Unlike other studies which have explored self-censorship online, our study did not specifically focus on disclosures related to sensitive topics such as NSA surveillance (Hampton et al., 2014), or Government military interventions (Stoycheff, 2016). From an end-user's perspective, the likelihood, purpose, and impact of surveillance is likely to have an effect on levels of self-censorship. For users discussing everyday topics online, the perceived negative impact of surveillance from Governments is likely to be low. However, corporate surveillance may use disclosed information for commercial gain (e.g., micro-targeting of political adverts), causing users to self-censor to limit this risk. Moreover, individuals may exploit information disclosed online for their own personal gain (e.g., gossip). In these instances, self-censorship may act as a self-presentation tool, allowing users to more effectively shape their online identities to enhance the impression they "give off" to other users in their online social networks (Liu et al., 2017).

5.4. Hypothesis 4. As the level of information management increases, the level of privacy concerns will decrease.

In exploring the factor of appropriate management of information, our survey items investigated aspects of appropriate information sharing and perceptions of control. In examining perceived appropriate information management (IM) as an antecedent factor to privacy concerns (PC), we found a statistically significant negative correlation ($r = -.230$) (see Table 14). This suggests that as perceptions of appropriate information management increase, levels of privacy concerns fall. While existing literature does not directly address this factor empirically, several studies have examined the broader factor of information control and found no statistically significant correlation (Dinev and Hart, 2004). The items developed as a part of Dinev and Hart's (2004) study, however, placed a greater focus on the perceived need to have control. This study has focused on the perceptions of information management and its appropriateness, which are two different variables. Previous research that considered the perception of control found a statistically significant correlation (Xu et al., 2008), which supports our findings.

Information control forms a part of this factor. However, it is important to recognise that absolute control over information disclosed online is not realistic or feasible. The ways that online data is now shared, stored and used, require a reconceptualization

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

of both data management expectations and practices. A shift from absolute control to appropriate management strategies requires an understanding of user expectations and norms of appropriate information management. In the previous section we suggest users may self-censor as a means of managing privacy boundaries between them, and other users in their online social networks. The finding that this factor negatively correlates with privacy concerns and directly correlates with self-censorship suggest that when users feel that their data flows in a way they deem appropriate, the need to self-censor is reduced. This support the need for SNSs to provide transparent usable information management features for users to be able to manage their privacy boundaries effetely, to help reduce users perceived need to self-censor, and facilitate trust. Further research is needed to better understand some general expectations of users when they communicate in SNSs for these information management features to be effective.

In the analysis of the individual items in this factor (see: Table 11), control over how data is used, received a higher mean response (M = 3.77) than control over who has access to the data (M = 3.61). This suggests that our participants felt they had more control over how their data are used, than who had access to their data. Our participants also had less confidence in government agencies only accessing their data after obtaining strict permissions (M = 3.46) than SNSs providers never sharing their personal information with anyone they had not intended (M = 3.68).

6. Conclusion and limitations

This research has extended the literature on online self-censorship, showing that privacy concerns increase the levels of self-censorship in SNSs. It has provided support for three antecedent factors to privacy concerns which impact upon the level of self-censorship when communicating in SNSs. The extension is supported by both Communication Privacy Management (CPM) theory, and Privacy as Contextual Integrity (Nissenbaum, 2010). Both theories support the need for appropriate flow when information is disclosed, and subsequently shared through collectively held boundaries. When a privacy violation occurs, it is as a result of the information disclosed flowing in an inappropriate way, outside of the boundaries that have been defined. These violations may occur as a result of perceived vulnerabilities within the systems being used to communicate. Unless the users are made *aware* of the potential flow of information outside of the agreed boundaries, violations will occur, increasing both privacy concerns and the levels of self-censorship.

Our findings have shown higher levels of privacy concerns and self-censorship as compared to privacy awareness and confidence in the appropriate management of personal data. There is a high level of awareness of government surveillance, yet most of our participants feel that government surveillance is not likely to affect them personally. Yet, commercial and social threats to their data are perceived as much more likely. Our participants were more concerned about *how* their data is used, than *who* has access to it. The growing trend for companies and governments to employ data science tools to discover new details about individuals from their online personal data

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

may contribute to this finding. However, a lack of awareness over the types of information being collected by SNSs and how that data is being used stems from the low usability of existing privacy awareness mechanisms (e.g., privacy policies). Our research has identified the need to understand individuals' perceptions of surveillance in order to help to reduce online privacy concerns. We also need to create environments where individuals' views can be freely expressed since failure to create this kind of environments may lead to increased levels of self-censorship. This would in term lead to a 'Spiral of Silence', where individuals' views only conform to those of a community majority. Further, failure to collectively assess surveillance-oriented security technologies will certainly lead to an absolute surveillance society (Mitchener-Nissen, 2014).

Our research method using a general public survey also required participants to remember past actions and concern and which might be subject to bias. To achieve an in-depth understanding of self-censorship in SNSs, qualitative research methods are also required to capture, in detail, both individuals' perceptions, attitudes, concerns and their behaviours. For example, it will be important to discover whether participants are making judgements based upon their own, or friends' personal experiences or on their perceptions gained from media reports. It would also be a useful addition to the research methodology to collect case studies where participants felt that they had been adversely treated by data they had disclosed which was subsequently used in a way they had not foreseen. Moreover, the research method that we used relied on self-reported behaviours which may not necessarily translate into in situ behaviour. As our survey included questions that specially related to privacy and surveillance, asking these questions may have had a priming effect on participants, and affected subsequent answers. Future researchers should explore ways to reduce this form priming, such as randomising the order of the questions.

This research was carried out in 2016 in the United Kingdom. During this time, governments and international bodies such as the EU, were developing new laws affecting both firms and individuals using the internet. The UK Parliament passed the Investigatory Powers Act 2016, sometimes known as the 'Snoopers Charter', which requires Internet and mobile phone companies to keep records of customer's browsing activity, social media use, emails, voice calls, online gaming and text messages for a year (Gayle, 2015). The recently released General Data Protection Regulation (GDPR) is increasingly tightening up the laws on personal data, including making it simpler for people to withdraw consent for their personal data to be used; letting people ask for data to be deleted; requiring firms to obtain "explicit" consent when they process sensitive personal data; expanding personal data to include IP addresses, DNA and small text files known as cookies; and letting people get hold of the information organisations hold on them much more freely (ICO 2017). All these will further alter the landscape of self-censorship online.

7. References

Adams, A. and Sasse M.A. (2001), "Privacy in multimedia communications: Protecting users, not just data", in Blandford, A. and Vanderdonckt, J. (Ed.), *People and Computers XV—Interaction without Frontiers*, Springer, London, pp. 49-64.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Anderson, D. (2015). "A question of trust – Report of the investigatory powers Review", available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf (accessed 1 July 2018).

Allmer, T. (2011). "A critical contribution to theoretical foundations of privacy studies", *Journal of Information, Communication and Ethics in Society*, Vol. 9 No. 2, pp. 83-101.

Altman, I. (1976). "A Conceptual Analysis", *Environment and Behavior*, Vol. 8 No. 1, pp. 7–29.

Bansal, G., Zahedi, F.M. and Gefen, D. (2010), "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", *Decision support systems*, Vol. 49 No. 2, pp. 138-15.

Barnes, S.B. (2006), "A privacy paradox: Social networking in the United States", *First Monday,* Vol. 11 No. 9, available at: http://firstmonday.org/article/view/1394/1312 (accessed 1 July 2018).

Beaumont, R. (2012), "An introduction to Principal Component Analysis & Factor Analysis using SPSS 19 and R (psych package)", available at: http://www.floppybunny.org/robin/web/virtualclassroom/stats/statistics2/pca1.pdf (accessed 1 July 2018).

Buitelaar, J.C. (2014), "Privacy and narrativity in the internet era", *The Information Society*, Vol. 30 No. 4, pp. 266-281.

Byeon, S. and Chung, S. (2012), "The chilling effect of anonymity and organizational membership in social network service", *Korean Journal of Journalism and Communication Studies*, Vol. 56 No. 4, pp. 105-132.

Byeon, S., Chung, S. and Jin, B. (2017), "Self-censorship on large corporations in SNS: the effect of news exposure, knowledge, and perceived power", *Digital Policy, Regulation and Governance*, Vol. 19 No. 2, pp. 139-152.

Cattell, R.B. (1966). "The scree test for the number of factors", *Multivariate Behavioral Research*, Vol. 1 No. 2, pp. 245-276.

ComRes. (2015), "Big Brother Watch – Online Privacy", available at: http://comresglobal.com/wp-content/uploads/2015/03/Big-Brother-Watch_UK-Tables_9-March-2015.pdf (accessed 1 July 2018).

ComRes. 2013, "Big Brother Watch Online Privacy Survey", available at: http://www.comresglobal.com/wp-content/themes/comres/poll/Big_Brother_Watch_Online_Privacy_Survey.pdf (accessed 1 July 2018).

Corritore, C.L., Kracher, B. and Wiedenbeck, S. (2003), "On-line trust: concepts, evolving themes, a model", *International Journal of Human Computer Studies*, Vol. 58 No. 6, pp. 737-58.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Costello, A.B. and Osborne, J.W. (2005), "Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis", *Practical Assessment, Research & Evaluation*, Vol. 10 No. 7, pp. 1-9.

Culnan, M.J. and Armstrong, P.K. (1999), "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", *Organization Science*, Vol. 10 No.1, pp. 104-15.

Das, S. and Kramer A.D.I. (2013), "Self-Censorship on Facebook", in AAAI Conference on Weblogs and Social Media (ICWSM), available at: https://research.fb.com/publications/self-censorship-on-facebook/ (accessed 1 July 2018).

Dinev, T. and Hart, P. (2004), "Internet privacy concerns and their antecedents-measurement validity and a regression model", *Behaviour & Information Technology*, Vol. 23 No. 6, pp. 413-22.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7-29.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Dinev, T., Hart, P. and Mullen, M.R. (2008), "Internet privacy concerns and beliefs about government surveillance–An empirical investigation", *The Journal of Strategic Information Systems*, Vol. 17 No. 3, pp. 214-33.

Dunfee, T.W., Smith, N.G and William T.R. (1999), "Social contracts and marketing ethics", *The Journal of Marketing*, Vol. 63 No. 3, pp. 14-32.

Fried, C. (1968), "Privacy", *The Yale Law Journal,* Vol. 77 No. 3, pp. 475–93.

Froomkin, A.M. (2000), "The death of privacy?", *Stanford Law Review*, Vol. 52 No. 5, pp. 1461-1543.

Frye, N.E. and Michele, M.D. (2010), "When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure", *Computers in Human Behavior*, Vol. 26 No. 5, pp. 1120-27.

Gayle, D. (2015), "Theresa May to revive her 'snooper's charter' now Lib Dem brakes are off", *The Guardian*, 9 May.

George, D. and Mallery, P. (2003), "SPSS for Windows Step by Step", available at: https://wps.ablongman.com/wps/media/objects/385/394732/george4answers.pdf (accessed 1 July 2018).

Gov.uk. (2016). "Investigatory Powers Bill", available at: https://www.gov.uk/government/collections/investigatory-powers-bill (accessed 1 July 2018).

Grandcolas, U., Rettie, R., & Marusenko, K. (2003), "Web Survey Bias: Sample or Mode Effect?", *Journal of Marketing Management*, Vol. 19 No. (5-6), pp. 541-61.

Hampton, K. N., Rainie, H., Lu, W., Dwyer, M., Shin, I., & Purcell, K. (2014). *Social media and the'spiral of silence'*. PewResearchCenter.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Hewson, C., Vogel, C. and Laurent D. (2015), *Internet Research Methods*, Sage.

Hoffman, D.L., Novak, T.P. and Peralta, M. (1999), "Building consumer trust online", *Communications of the ACM*, Vol. 42 NO. 4, pp. 80-85.

Information Commissioner's Officer (ICO) (2017), "Overview of the EU General Data Protection Regulation (GDPR)", available at: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf (accessed 1 July 2018).

House of Commons. (2015), "Privacy and Security: A modern and transparent legal framework", available at: http://www.statewatch.org/news/2015/mar/uk-isc-privacy-and-security-report.pdf (accessed 1 July 2018).

Jensen, C. and Potts C. (2004), "Privacy policies as decision-making tools: an evaluation of online privacy notices", in proceedings of the SIGCHI conference on Human Factors in Computing *Systems, Vienna, Austria, pp*. 471-78.

Kaiser, H.F. (1960), "The application of electronic computers to factor analysis", *Educational and Psychological Measurement*, Vol. 20 No. 1, pp. 141-51.

Elahe, K.Z. and Helmhout, M. (2012), "Increasing service users' privacy awareness by introducing on-line interactive privacy features", in Laud P. (eds) *Information Security Technology for Applications. NordSec 2011.* Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, Vol. 7161, pp. 131-48.

Krasnova, H., Günther, O., Spiekermann, S. and Koroleva, K. (2009). "Privacy concerns and identity in online social networks", *Identity in the Information Society*, Vol. 2 No. 1, pp. 39-63.

Liu, Y., Rui, J. R., & Cui, X. (2017). Are people willing to share their political opinions on Facebook? Exploring roles of self-presentational concern in spiral of silence. *Computers in Human Behavior*, *76*, 294-302.

Lyon, David (2015), *Surveillance after Snowden*, John Wiley & Sons.

MacAskill, E., Borger, J., Hopkins, N., Davies, N. and James B. (2013). "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications, *The Guardian*, 21 June.

Margulis, S.T. (2003), "Privacy as a social issue and behavioral concept", *Journal of Social Issues*, Vol. 59 No. 2, pp. 243-61.

Margulis, S.T. (1977). "Conceptions of privacy: Current status and next steps", *Journal of Social Issues*, Vol. 33 No. 3, pp. 5-21.

Marthews, A., & Tucker, C. E. (2017). Government surveillance and internet search behavior.

Mitchener-Nissen, T. (2014), "Failure to collectively assess surveillance-oriented security technologies will inevitably lead to an absolute surveillance society", *Surveillance & Society*, Vol. 12 No. 1, pp. 73-88.

Martin, K, and Shilton, K. (2016). "Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices", *The Information Society*, Vol. 32 No. 3, pp. 200-16.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Matzner, T. (2014), "Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data"", *Journal of Information, Communication and Ethics in* Society, Vol. 12 No. 2, pp. 93-106.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Noelle-Neumann E. (1993), *The spiral of silence: Public opinion, our social skin*, University of Chicago Press.

Noelle-Neumann E. (1974), "The spiral of silence a theory of public opinion", *Journal of communication*, Vol. 24 No. 2, pp. 43-51.

NTIA. (2016). "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities", available at: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (accessed 1 July 2018).

Office of National Statistics. 2016. "Internet Users in the UK - Office for National Statistics.", available at: https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016 (accessed 1 July 2018).

Petronio, S. and Altman, I. (2002), *Boundaries of privacy: Dialectics of Disclosure*, State University of New York Press.

Phelps, J., Nowak, G. and Ferrell, E. (2000), "Privacy concerns and consumer willingness to provide personal information", *Journal of Public Policy & Marketing*, Vol. 19 No. 1, pp. 27-41.

Posner, R.A. (1978), "The right of privacy", *Georgia Law Review*, Vol. 12 No. 3, pp. 393-422.

Postmes, T., Spears, R. and Lea, M. (2002), "Intergroup differentiation in computer-mediated communication: effects of depersonalization", *Group Dynamics*, Vol. 6 No. 1, pp. 3-16.

Richards, N.M. (2012). "Dangers of surveillance", *The Harvard Law Review*, Vol. 126 No. 7, pp. 1934-65.

Riegelsberger, J., Sasse, M.A. and McCarthy, J.D. (2009), "Trust in mediated interactions", in Joinson, A.N., Katelyn, Y.A., McKenna, T.P. and Reips, U.D. (eds.), *The Oxford handbook of Internet psychology*, Oxford University Press, pp. 53-69.

Royal United Services Institute. (2015). "A Democratic Licence to Operate", available at: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf (accessed 1 July 2018).

Schauer, F. (1978), "Fear, risk and the first amendment: unraveling the chilling effect", *Boston University Law Review*, Vol. 58 No. 685, pp. 685-732.

Schau, H.J., and Gilly M. (2003). We are what we post? Self-Presentation in Personal Web Space. Journal of Consumer Research 30(3): 385-404.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Sidhu, D.S. (2007), "The chilling effect of government surveillance programs on the use of the internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, Vol. 7 No. 2, pp. 375-93.

Sleeper, M., Rebecca B., Das, S., McConahy, A.L., Wiese, J. and Cranor, L. (2013), "The post that wasn't: exploring self-censorship on facebook", in *Proceedings of the 2013 conference on Computer supported cooperative work*, *San Antonio, Texas, USA*, pp. 793-802.

Smith, H.J., Milberg, S.J. and Burke, S.J. (1996). "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly*, Vol. 20 No. 2, pp. 167-96.

Snowden, E. (2015), "We are Edward Snowden, Laura Poitras and Glenn Greenwald from the Oscar-winning documentary CITIZENFOUR. AUAA.", available at: https://www.reddit.com/r/IAmA/comments/2wwdep/we_are_edward_snowden_laura_poitras_and_glenn/ (accessed 1 July 2018).

Solomon, D.H. and Samp, J.A. (1998), "Power and problem appraisal: perceptual foundations of the chilling effect in dating relationships", *Journal of Social and Personal Relationships*, Vol. 15 No. 2, pp. 191-209.

Solove, D.J. (2007), "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, p. 745.

Stevens, J.P. (2012), *Applied multivariate statistics for the social sciences*. Routledge.

Stoycheff, E. (2016), "Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA internet monitoring", *Journalism & Mass Communication Quarterly*, Vol. 93 No. 2, pp. 296-311.

Stutzman, F.C. and Hartzog, W. (2012), "Boundary regulation in social media", in *Proceedings of the ACM 2012 conference on computer supported cooperative work*, *New York, USA,* pp. 769-78.

Sun, S., Cegielski, C.G., Lin J. and Hall, D.J. (2016), "Understanding the Factors Affecting the Organizational Adoption of Big Data", *Journal of Computer Information Systems*, Vol. 58 No. 3, pp. 193-203.

Wilton, R. (2017) "After Snowden – the evolving landscape of privacy and technology", *Journal of Information, Communication and Ethics in Society*, Vol. 15 No. 3, pp. 328-35.

Wisniewski, P., Lipford, H., & Wilson, D. (2012, May). Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 609-618). ACM.

Woo, J.S., Na, H.S. and Choi, J.M. (2010), "An empirical analysis of the effect of the real-name system on internet bulletin board", *Korean Journal of Policy Studies*, Vol. 48 No. 1, pp. 71-96.

Xu, H. (2012), "Reframing Privacy 2.0 in Online Social Networks", *University of Pennsylvania Journal of Constitutional Law*, Vol. 14 No. 4, pp. 1077–1102.

Journal **XX** (XXXX) XXXXXX DOI: 10.1108/JICES-07-2018-0060

Xu, H. (2007), "The effects of self-construal and perceived control on privacy concerns", *ICIS 2007 proceedings*. Paper 125.

Xu, H., Dinev, T., Smith, H.J. and Hart, P. (2008), "Examining the formation of individual's privacy concerns: Toward an integrative view", *ICIS 2008 proceedings*, Paper 6.

Zhong, Z., Wang, T. and Huang, M. (2017), "Does the Great Fire Wall cause self- censorship? The effects of perceived internet regulation and the justification of regulation", *Internet Research*, Vol. 27 No. 4, pp. 974-90.