The Journal of the Southern Association for Information Systems

Volume 8 | Issue 1 Article 2

July 2021

Surveillance Concerns as Predictors of Obfuscation and the Chilling Effect in the Context of a Pandemic

Craig Van Slyke
Louisiana Tech University, crvanslyke@gmail.com

Grant Clary
Louisiana Tech University, wgc003@latech.edu

Mohamed Tazkarji
College of Charleston, tazkarjim@cofc.edu

Recommended Citation

Van Slyke, C., Clary, G., & Tazkarji, M. (2021). Surveillance Concerns as Predictors of Obfuscation and the Chilling Effect in the Context of a Pandemic. The Journal of the Southern Association for Information Systems, 8, 24-49. https://doi.org/10.17705/3JSIS.00016

Surveillance Concerns as Predictors of Obfuscation and the Chilling Effect in the Context of a Pandemic

Cover Page Footnote

Partial funding for this project was provided by an endowment for the McCallister Eminent Scholar Chair in Information Systems. doi:10.17705/3JSIS.00016

ABSTRACT

Potential negative consequences of digital surveillance represent an area of increasing concern due to the rising impact of digital and mobile technologies on daily life. The COVID-19 pandemic increased these concerns as governments worldwide turned to both digital and non-digital surveillance to help in the battle to control the spread of the disease. Due to this, surveillance creep (the use of supposedly limited-scope surveillance for increasingly pervasive purposes) is a growing concern. Concerns over digital surveillance have led to some individuals turning to protective measures, including obfuscation and the chilling effect. Obfuscation involves intentionally providing ambiguous or misleading information to interfere with surveillance activities. The chilling effect is the decision to not engage in some behavior due to concerns about the consequences of that behavior. Often, obfuscation is a general protective measure that guards against surveillance across applications and reflects general concerns about privacy and surveillance. In contrast, the chilling effect is application and concern specific. In this paper, we use a research model that draws on the health beliefs model and protection motivation along with data from a survey of American social media users to investigate antecedents of obfuscation and the chilling effect in the context of social media surveillance related to COVID-19. Results indicate that age, sex, social media experience, social media habit, and the perceived surveillance severity impact obfuscation. These same antecedents affect the chilling effect, as does perceived surveillance vulnerability. Although our research is exploratory, the results of our study hold implications for both research and practice.

Keywords

Surveillance, social media, pandemic, obfuscation, chilling effect

INTRODUCTION

In March of 2020, the World Health Organization (WHO) characterized the spread of COVID-19 as a pandemic (WHO, 2020). Since then, the disease has spread throughout much of the world. Governments worldwide have struggled with how to respond to the pandemic effectively. Governments have used various approaches to slowing the spread of COVID-19, including recommending or requiring masks, social distancing, isolation of suspected cases, and, in some cases, digital and non-digital surveillance. The WHO provides guidelines regarding COVID-19 surveillance objectives (French & Monahan, 2020). Governments are holding discussions with technology companies about the use of location data, facial recognition, and other digital data for contact tracing and for monitoring and enforcing isolation orders (Calvo et al., 2020). In China, mobile payment data is being used in concert with other data to generate infection risk scores that are being used to restrict access to stores, transportation services, and public spaces (Calvo et al., 2020). Some see such surveillance as necessary in light of COVID-19. For example, South Korea's use of granular location data and social network analysis to track and target individuals for treatment and isolation is being held up as an example for other countries to follow (French & Monahan, 2020).

This growing acceptance of digital surveillance may be among the most important enduring consequences of COVID-19 (Calvo et al., 2020). Surveillance creep, which is the use of supposedly limited-scope surveillance for increasingly pervasive and permanent purposes, is a growing concern (Malgieri, 2020; Calvo et al., 2020). Although surveillance may be a reasonable response to a pandemic, increased surveillance has negative consequences for well-being due to the sense that people are being controlled and therefore losing autonomy. This can lead people to reassert their autonomy by taking steps to evade surveillance (Calvo et al., 2020). In addition, people may view the extended use of COVID-19 data to be a risk to fundamental rights, which also may bring about efforts to resist surveillance (Malgieri, 2020). This could lead to negative consequences for the management of the COVID-19 pandemic.

For many people, social media is a major source of information and social connection, especially during times of crisis (Lee et al., 2015). Public health officials use social media platforms to provide a variety of information, including answers to medical questions, disseminating personalized messages, and monitoring

public reactions to health crises (Coiera, 2013; Huesch et al., 2016; Valente & Pitts, 2017). Social media may also be used among peers to seek or provide emotional or social support (Moorehead et al., 2013). So, during a time of crisis, many people will turn to social media to gather relevant information or to engage in relationship-oriented communications such as "checking in" or asking about the status of others.

Concerns over privacy may impact how people use social media, especially in uncertain times. By their very nature, social media systems tend to encourage people to share information about themselves. This information sharing may be overt, such as posting about one's status, or it may be secondary, such as Facebook's display of users' friends. Privacy concerns about inherently public disclosures have been the subject of considerable research (see Ellison et al. (2011) for an overview). However, to date, there has been relatively little research regarding how surveillance concerns impact social media behaviors. There is some research into citizens surveillance concerns, however. For example, a large survey of Americans indicate that government surveillance related to pandemics is a concern to many individuals (Auxier, 2020). However, a survey conducted in April 2020 indicates that 52% of Americans would find it acceptable for the government to use mobile phone data to track the activities of people who tested positive for COVID-19 in order to better understand the spread of the disease (Anderson & Auxier, 2020). However, eight months later another survey of Americans found that only 13% of respondents were very comfortable with private companies sharing location data with the government for the purpose of tracking the spread of COVID-19 (Johnson, 2021). This result is concerning, given that more than 70% of Americans believe that their online activities are tracked by private companies (Auxier et al., 2019). Taken together, these surveys indicate that COVID-19 surveillance is of sufficient concern to warrant further research.

In this study, we examine antecedents to two forms of responses to surveillance of social media activity, obfuscation, and the chilling effect, as they concern COVID-19 related surveillance. Obfuscation is “the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection” (Brunton & Nissenbaum, 2015). Obfuscation can occur offline or online. Online, individuals may engage in obfuscation in a variety of ways. Some of these provide protection across platforms. These include using a virtual private network to mask one's true Internet protocol (IP) address, using anonymous browsers, and disabling location-based services. People can also employ obfuscation techniques that are specific to social media, such as providing false information such as a false name or birthdate, tagging pictures of others as themselves, and posting false or misleading status updates.

The chilling effect is the decision not to commit some act due to concerns about the consequences of that act (Schauer, 1978). Although the chilling effect came to light in the context of how laws and regulations could inhibit behaviors related to freedom of speech and expression (Schauer, 1978), it can be applied to online activities, including social media. It is not unusual for social media users to pause before posting something to consider the potential consequences that might result from the post. For example, a user might conclude that posting a controversial opinion about a current event might cause the loss of friends or followers and therefore decide not to make the post. Surveillance concerns may also result in behavioral consequences. For example, government surveillance may exert a chilling effect on Internet search behavior (Marthews & Tucker, 2017a). Surveillance is not limited to governments. Private companies conduct much of the surveillance that occurs online. Increasingly, data sharing cooperation between governments and private organizations is blurring the line between government and private surveillance, which may increase surveillance concerns. This is an important development as it may serve to increase perceptions of surveillance due to the increased uncertainty about how the surveillance occurs and who is doing the surveilling. Interestingly, the chilling effect does not require actual surveillance – it only matters that the user believes that surveillance might occur and bring negative consequences (Marthews & Tucker, 2017b). So, it is reasonable to expect that concerns over social media surveillance would have similar chilling effects.

Obfuscation and the chilling effect are both responses to surveillance concerns, but they differ in at least one important way. Obfuscation typically offers broader protection that helps guard against surveillance across applications. For example, the use of a virtual private network (VPN) can mask one’s location

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

regardless of the application being used. Similarly, obfuscation is not concern specific; as an example, a VPN can protect against surveillance about COVID-19 or about one's consumer activities. In contrast, the chilling effect is more specific. The choice not to post to social media about COVID-19 due to surveillance concerns reflects a desire to guard against surveillance in this specific context.

Given the above, we believe it is useful to investigate the following research question:

> *In the context of social media surveillance related to COVID-19, what are the effects of individual characteristics, social media habit, and surveillance concerns on the use of obfuscation techniques and the chilling effect?*

To investigate this question, we surveyed 524 social media users who resided in the United States. Results indicate that the user's age, sex, and social media experience impact both obfuscation and the chilling effect, as did habit and perceptions of the severity of surveillance consequences. Perceptions of one's vulnerability to COVID-19 social media surveillance consequences were associated with the chilling effect, but not obfuscation. Despite being exploratory, our research holds implications for research and practice.

BACKGROUND

Surveillance

Many definitions of surveillance exist. For our purposes, we define surveillance as "monitoring people in order to regulate or govern their behavior (Gilliom & Monahan, 2012, p. 2). This definition is concise while still covering the important elements of surveillance – watching or monitoring, and control. Although surveillance predates the rise of digital surveillance by many years, the rise of digital technologies led to a need to consider technology-mediated surveillance (Haggerty, 2006). We adapt the definition presented earlier to account for our context and define social media surveillance as the monitoring of people's social media activities for the purpose of influencing behavior.

Social media surveillance represents a clear privacy threat to users (van der Schyff et al., 2020). When faced with a potential threat, people appraise the associated risk, which helps determine whether someone adopts a coping response that protects against the threat. A threat appraisal is established by combining the perceived severity and vulnerability of the threat (Crossler and Belanger, 2014). In the context of social media surveillance, perceived severity is the individual's assessment of the seriousness of the threat from social media surveillance, while perceived vulnerability is the individual's assessment of their to social media surveillance (adapted from Milne et al., 2000). Collectively, we call these assessments social media surveillance concerns, which we define as a user's perception of the risk associated with social media surveillance. In this study, we are specifically interested in how concerns about social media activities related to COVID-19 affect protective behaviors. We draw on the health beliefs model (Rosenstock, 1974) and protection motivation theory (Floyd et al., 2000) and conceptualize social media COVID-19 surveillance concerns as an individual's appraisals of 1) the severity of the consequences of social media COVID-19 surveillance, and 2) their vulnerability to social media COVID-19 surveillance. Strong threat appraisals lead to a coping intention or behavior (Floyd et al., 2000; Crossler & Belanger, 2014). We investigate two forms of coping: the intentional use of *obfuscation* to camouflage their true online information and the *chilling effect*, which is a self-regulating protective action.

It is interesting to note that attitudes towards digital surveillance is likely to vary across cultures, which makes reaching a global consensus about digital surveillance difficult to achieve (Vecellio & Segate, 2019). Individuals of different cultures are likely to view their digital privacy differently (Li & Borah, 2018; Ma et al., 2020; Onishsi & Meheut, 2020). These differences should also be reflected in how individuals of different cultural traditions view digital surveillance, including surveillance about COVID-19. Asians may be more accepting of digital surveillance as a means for reducing the spread of disease due to their experience with recent epidemics, such as SARS (Cha, 2020). Because of this, we caution against generalizing the results of this study (which uses a survey of American adults) across cultures.

Understanding how those from various cultures view COVID-19 social media surveillance and how those views affect protective behaviors will require additional research.

Disease surveillance, sometimes referred to as public health surveillance, is collecting data about the disease, or public health, and the individuals who have the disease (Mariner, 2007). Some surveillance programs receive federal funding. For example, the United States Department of Homeland Security (DHS) laid out a plan for the National Biosurveillance Integration Center (NBIC). The NBIC uses information about health and disease events to help make well-informed decisions, save lives, and minimize the economic impact (United States Department of Homeland Security, ND). The Centers for Disease Control and Prevention (CDC) is a national public health agency within the United States Department of Health. The CDC also focuses on the nationwide health of US citizens. The purpose of surveilling public health is to identify people with communicable diseases so government officials can prevent an epidemic (Chiolero & Buckeridge, 2020). Actions include identifying where the individual acquired the disease and who else might have been infected – also referred to as contact tracing (Ahmed et al., 2020).

Benefits of public health surveillance include the potential for improved healthcare quality efficiency and reduced cost for the public (Halamka et al., 2009; Nsubuga et al., 2006). However, health surveillance systems should still consider the users' privacy (German et al., 2001). A core element of public health surveillance is the collection of data for analysis. Data sources can come in many different forms. Mobile Health (mHealth) is a set of mobile devices (e.g., apps on a smartphone) that allow users to reach out in a variety of ways (Kotz et al., 2016) even without a clinician. mHealth plays a large role in creating data for public health decision-makers such as the CDC or NBIC (Iwaya et al., 2018). The development of new data science and artificial intelligence (AI) tools has also given exponential growth to health-related data (Chiolero & Buckeridge, 2020). Other ways of collecting data include counting patients visiting emergency rooms, online searches, social media data, electronic health records (EHRs), or even pharmacy sales (Chiolero & Buckeridge, 2020).

This creates a dilemma, as the privacy of individually identifiable health data and public health promotion are at odds (Hodge, 2003). Avancha et al. (2012) proposed a privacy framework on mobile technology for healthcare. Their framework outlines actionable principles of individuals' privacy regarding mobile technology for healthcare. Some of the principles of the framework include openness and transparency of the healthcare's information policies, procedures, and technologies; individuals' ability to control the privacy of their healthcare information; specification of the purpose of how the information is collected, stored, and used; data quality and integrity; security of the system's infrastructure; and accountability of the system. Similarly, Iwaya (2018) reviewed privacy threats for public health surveillance systems and found many of the same principles (e.g., data quality, informed consent, transparency, security of data, and accountability). This weighing of costs (privacy) and benefits (improved health) has resulted in public health surveillance systems having guidelines in place to ensure the privacy of individuals (e.g., German et al., 2001).

Responses – Obfuscation and Chilling Effect

Obfuscation is a strategy of informational self-defense that acts as informational resistance, disobedience, or even covert sabotage; it disproportionately aids the weak against the strong (Brunton & Nissenbaum, 2013). In the surveillance context, obfuscation is used to protect personal data. This "intentional obfuscation" is defined as the production, inclusion, addition, or communication of misleading, ambiguous, or false data to evade, distract, or confuse data gatherers or diminish the reliability of data aggregations (Brunton & Nissenbaum, 2011). Thus, obfuscation is used to protect users from surveillance and tracking (Ridgeway, 2015).

As people become more reliant on information technology, obfuscation may represent a useful avenue of resistance against datafication (Howe, 2015). Disclosing personal information involves a risk because it leaves people feeling vulnerable (Derlega et al., 1993; Petronio, 2000). A person can use obfuscation

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

strategies to "pollute" data collected about them by doing things like posting fake data on social media accounts and providing incorrect personal information. These strategies protect personal data and preferences, but they can pollute one's social media streams and present a negative or confusing image.

The "chilling effect" has its roots in legal opinions regarding free speech rights. The "chilling effect" acts as a deterrent to free speech, expression, and association (Schauer, 1978). A chilling effect occurs when a person avoids a certain action because of a possible consequence. In a more general sense, chilling effects can be seen as the impact of surveillance on constraining specific behaviors (Foucault, 1977). There is little extant empirical research into the chilling effect as it relates to digital environments.

Social media networks (like Facebook, Twitter, and Instagram) involve the public disclosure of personal information (Taddei & Contena, 2013). Thus, social media users may experience chilling effects by constraining or refraining from certain actions due to the effect of other parties' access to their actions or posts. This was reflected clearly in previous research that reported data from 3.9 million Facebook users. This research reported that 71% of Facebook users had self-censored by editing at least one post over a period of 17 days (Das & Kramer, 2013). Another occasion where chilling effects come to play is when governments take steps to regulate the freedom of individuals (e.g., India). For example, government regulation had a chilling effect on the Indian social media community leading to widespread self-censorship practices and suppression of ideas in the marketplace (Litton, 2015).

Obfuscation and the chilling effect differ with respect to the extent to which they are specific to a particular surveillance threat. We conceptualize social media obfuscation to be the use of obfuscating techniques such as providing misleading information, such as a false birthdate or name. It is difficult and impractical to use these methods only for COVID-19 social media activities. So, obfuscation is a more general approach to protecting oneself from social media surveillance. In contrast, the chilling effect is more specific to the context of COVID-19. When someone considers the effects of a specific social media posting, they will naturally consider the particular context of the post. For example, posting an opinion about a recent movie will be evaluated differently than posting about having been in contact with someone who tested positive for COVID-19. Our operationalizations of obfuscation and the chilling effect match the degrees of context specificity discussed here.

HYPOTHESES DEVELOPMENT

In this section, we develop research hypotheses related to our research questions. Our hypotheses are related to three areas, individual characteristics, social media habit, and COVID-19 social media surveillance concerns. Individual characteristics and social media habit are general in nature, while surveillance concerns are specific to COVID-19 and social media. Because predictors of obfuscation and the chilling effect have not been widely studied, we consider our research to be exploratory. Therefore, we chose a variety of predictors that reflect user characteristics (age and gender), user behavioral proclivities (social media habit), and specific concerns about surveillance of social media behaviors related to COVID-19 (COVID-19 social media concerns). This selection provides a range of predictors that can be compared with respect to their efficacy in affecting protective behaviors related to COVID-19 social media surveillance.

Individual Characteristics

A substantial body of research indicates that individuals differ in how they view and use information systems (IS) (e.g., Zmud, 1979; Agarwal & Prasad, 1999; Sabah, 2016), including social media (Gil de Zungia et al., 2017; Zhang et al., 2018). Some individual characteristics may also impact the extent to which individuals use obfuscation or are subject to the chilling effect. In this study, we are interested in three characteristics, age, sex, and social media experience.

Prior research has found generational differences in the use of information technology (e.g. Morris & Venkatesh, 2000; Lerouge et al., 2014), including social media (Kezer et al., 2016). Generally, this research has found that younger adults are more likely to use a variety of information technology, including social

media (Kezer et al., 2016). However, there is little extant research into age effects related to digital surveillance, even though age-based differences are thought to be important for understanding reactions to surveillance (Smith & Lyon, 2013).

One exception is a large study of American's beliefs and concerns about online surveillance (Auxier et al., 2019). Data from that survey indicate that older Americans tend to be less accepting of and more concerned about online surveillance, although the results are mixed. Younger adults are more likely to believe that they are being tracked by the government but are more likely to think that they benefit from data collection. For example, a larger proportion of young adults believe that it is acceptable for social media companies to engage in monitoring to identify users who show signs of depression and to connect these users to mental health services. Older adults feel less in control of who can access their personal information, including their private online communications, and are also less likely to believe that they experience benefits from data collection (Auxier et al., 2019). These concerns may result in older adults taking steps to protect themselves from surveillance. However, there is some evidence that younger Internet users are more likely to be subject to chilling effects in response to concerns about government surveillance (Penney, 2017), and to provide false information to marketers when using websites (Smith & Lyon, 2013). Another study, which was conducted in November 2020, found that older adults are less supportive of surveillance, including contact tracing related to public health. The oldest age group in the study (60 years of age and older) was the least supportive of surveillance (Zhang et al., 2020).

Despite the mixed evidence from earlier studies, we expect age to have a positive relationship with both obfuscation and the chilling effect. One reason for this thinking is that self-regulation has been shown to increase with age (van Deursen et al., 2015). Obfuscation and chilling effect behaviors are forms of self-regulation since they involve reactions to perceived negative outcomes from specific behaviors (providing true information or posting on social media). Self-regulatory behaviors in the context of our study are especially important, given older adults' greater concerns about privacy (Kezer et al., 2016). We should note, however, that prior research has demonstrated that younger users are more likely to engage in privacy-protective behavior when using social media. However, these differences may be due to more frequent use of social media, which leads to more familiarity about how to maintain privacy settings (Kezer et al., 2016). No special knowledge of privacy settings is required to use some obfuscation techniques or to refrain from posting information on social media (chilling effect).

Our expectations regarding the chilling effect also are based on younger users' greater use of social media for social interaction and for their greater likelihood of self-disclosure (Chang et al., 2015; Kezer et al., 2016). Although the situation is gradually changing, social media is integrated more into the lives of younger people (Lenhart et al., 2010), which makes it more difficult for younger social media users to refrain from posting on social media, even when they are concerned about surveillance. Empirical evidence supports the notion of younger adults using information technology for social purposes. For example, van Deursen et al. (2015) found that age had a negative impact on the social usage of smartphones and also found that age was negatively related to addictive and habitual smartphone behaviors.

The context of COVID-19 also plays a role in our thinking. At the time of data collection, COVID-19 seemed to be having disproportionate effects on older people (Dowd et al., 2020), which is likely to result in older adults being more focused on issues related to COVID-19 including potential consequences of surveillance. This may make concerns about COVID-19-related surveillance more salient to older adults, leading to increased chances that they will engage in protective behaviors. So, we expect age to be positively related to obfuscation and the chilling effect, as stated below.

H1a: Age will be positively related to obfuscation.

H1b: Age will be positively related to the chilling effect.

We also expect to see a relationship between sex and obfuscation and the chilling effect, although it is unclear whether women or men will be more likely to engage in protective measures. There is little research

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

on how women and men may view surveillance differently, even though this is an important area of research (Smith & Lyon, 2013). From the research that does exist, men seem more concerned about and less accepting of surveillance. For example, men are more likely to find laws intended to protect national security intrusive and are less likely to provide information to governmental agencies (Smith & Lyon, 2013). Generally, women are more accepting of digital surveillance. They also perceive more benefits of surveillance than men (Bayerl & Akhgar, 2015). Women, for example, are more likely to support surveillance if it could aid in crime prevention (Bayerl & Akhgar, 2015). Women are also more likely to disclose information online (Potoglou et al., 2017). But, women are more likely than men to delete information about themselves from social media profiles (Marett et al., 2011). Women are also slightly less likely to find employer surveillance of email messages acceptable (Smith & Lyon, 2013). However, there are reasons to believe that women may be more sensitive to the misuse of social media postings. Women may be more concerned about their privacy in general (Baruh et al., 2017), and on social media sites in particular (Hoy & Milne, 2010). Females are substantially more likely to be the victim of cyberstalking (Paullet et al., 2009; DreBing et al., 2014), which may make them more sensitive to surveillance in any form. Empirical findings related to gender differences in privacy concerns and privacy-protective behaviors are mixed, however (Baruh et al., 2017).

Responses to COVID-19 may also shed light on how men and women differ with respect to COVID-19 related surveillance. Women are more concerned about the effects of COVID-19 (van der Vegt & Kleinberg, 2020). They are also more likely than men to view COVID-19 as a severe problem (Galasso et al., 2020; ven der Vegt & Kleinberg, 2020). Women also are more likely to view restrictive governmental policies as agreeable; they are also more likely to comply with such policies (Galaaso et al., 2020). It seems reasonable to expect that women may also be more likely to find digital surveillance about COVID-19 to be acceptable, which may lead to fewer efforts to escape the effects of this surveillance. A 2021 survey of American adults indicates that females are more concerned about COVID-19 related surveillance than are males (Johnson, 2021). Similarly, a 2020 survey found females less supportive of COVID-19 related surveillance (Zhang, 2020). As the above discussion demonstrates, there is conflicting evidence regarding how women and men respond to surveillance. However, taken as a whole, we believe that females are more likely to take protective measures, as reflected in the following hypotheses. However, these hypotheses should be considered exploratory.

H2a: Females will be more likely than males to engage in obfuscation.

H2b: Females will be more likely than males to engage in the chilling effect.

We expect the length of time one has been using social media to impact obfuscation and the chilling effect. More experienced users are more likely to have experienced consequences from surveillance or other privacy violations, making them more likely to be concerned about such events. This, in turn, increases the likelihood that they will take steps to avoid future consequences from surveillance. In addition, experience with social media may lead to greater knowledge of how to avoid undesirable data collection. Empirical evidence indicates that users with more Internet experience view surveillance less favorably than their less experienced peers (Bayerl & Akhgar, 2015). It is reasonable to expect a similar situation with social network users. Thus, we expect the length of time one has been using social media to be positively related to both obfuscation and the chilling effect.

H3a: The length of time one has used social media is positively related to obfuscation.

H3b: The length of time one has used social media is positively related to the chilling effect.

Habit

Habit may also impact the extent to which social media users engage in actions intended to protect against surveillance. Habits are sequences of acts that develop into automatic, unconscious responses to specific environmental cues (Verplanken & Aarts, 1999). Habit-driven behaviors require minimal cognitive effort because they are largely unconscious actions. In addition, habitual behavior is non-reflective in that the

individual does not engage in a purposeful decision with respect to performing the behavior (Limyem et al., 2007; Ortiz de Guinea, 2009; Polites & Karahanna, 2012; Chiu & Huang, 2014; van Deursen et al., 2015). Habit has been empirically demonstrated to be related to information systems continuance intentions (Chiu & Huang, 2014) and behaviors (Limayem et al., 2007). These findings have also been found with respect to social media (Chiu & Huang, 2014; Wang et al., 2015). This is not surprising because social media use is often habitual (Alhabash & Ma, 2017).

Because habit is based on previous behaviors (Limayem et al., 2007), higher levels of habitual behavior are associated with more frequent use of social media. Individuals who use social media more frequently are more exposed to negative consequences from privacy violations, which should make the users more sensitive to potential risks from surveillance. This, in turn, should lead them to take action to avoid negative consequences from surveillance. These actions could include either obfuscation or the chilling effect. However, habit may also lead one to use social media to communicate about COVID-19 without reflecting on risks, which would argue for habit to have a negative relationship with the chilling effect. We believe that the desire to avoid surveillance risks will override the more automatic social media behavior. So, we expect habit to have positive relationships with obfuscation and the chilling effect. Given the lack of research on these relationships, we acknowledge that H4b is exploratory.

H4a: Social media habit will have a positive relationship with obfuscation.

H4b: Social media habit will have a positive relationship with the chilling effect.

Surveillance concerns (severity and vulnerability)

Risk perception is often used when studying privacy concerns (Belanger & Crossler, 2011). Risk perceptions have been defined in privacy research as an individual's beliefs regarding the probability of gains or losses due to privacy violations (Van Slyke et al., 2006). Surveillance denotes a risk as there is privacy loss inherent in surveillance. Specifically, these risks might include accidental exposure, insider snooping, insider submission, external breaching, security deficiencies, scams, and uncontrolled secondary information usage (Rindfleish, 1997; Dinev et al., 2008). Consistent with previous studies (e.g., Dinev et al., 2008), we view surveillance as a privacy-related risk for individuals to consider.

Online surveillance risks are based on perceived threats to the privacy of one's information. When a surveilling actor has access to personal information, an individual may develop concerns about the associated risks (Yao et al., 2007). Responses to these concerns may include an unwillingness to provide information and provision of intentionally false information or misleading (Dinev et al., 2006; Xu et al., 2008; Li, 2012; Nam, 2018).

Priors studies have found that consumers fabricate (falsify information or provide incomplete information) their information online (Lin et al., 2007; Youn, 2009). There is limited empirical research using the term "obfuscation" as a protective measure for protecting online information privacy, but obfuscation is conceptually similar to fabrication. Obfuscation serves as an active defense mechanism to camouflage what "true" information about oneself. In the context of surveillance, one might provide disinformation (deliberately lying) online about oneself to mitigate the risks of online surveillance.

We also expect that concerns about COVID-19 related social media surveillance cause users to implement protective mechanisms due to the risks involved. As previously mentioned, the chilling effect is the decision not to commit an act due to concerns about the potential consequences. Recent research shows a significant relationship between online surveillance and a lack of online activities (Penney, 2017; Tanriverdi & Chen, 2018). Prior studies also show other privacy concerns resulting in refraining from use (Zviran, 2008; Youn, 2009; Li, 2012).

Online information protection typically assesses risk in two ways: severity and susceptibility (Youn, 2005; Mohamed & Ahmad, 2012). These factors are drawn from the health beliefs model (Hochbaum, 1958; Rosenstock, 1960; Champion & Skinner, 2008) and later protection motivation theory (PMT) (Rogers, 1975). Both of these theories have been used in studies of information security behaviors (see Moody et al.,

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

2018), which leads us to believe that they may also be applicable to a study of digital surveillance protective behaviors.

Perceived severity denotes how serious an individual believes a threat will be to them (Milne et al., 2000). Threats of surveillance thus refer to how harsh and intense the misuse of their data being surveilled can be. Perceived severity has been shown in past research to be a strong predictor of behavioral intention (Floyd et al., 2000; Herath & Rao, 2009; Crossler & Belanger, 2014). Therefore, we expect a high perceived severity of surveillance will result in the intention to use obfuscation as a way to hide personal information from the surveilling actor. Similarly, since perceived severity is expected to reflect increased concerns about misuse of their information, one might be less inclined to share any information online due to the chilling effect. This relationship has been shown to be significant in the literature (Penney, 2017; Tanriverdi & Chen, 2018). Because the effects of perceived severity have been shown across several contexts, we expect perceptions of the severity of the threat from social media behaviors related to COVID-19 to also influence protective behaviors. Thus, we state the following hypotheses regarding the impact of perceived surveillance severity.

> H5a: Perceived COVID-19 social media surveillance severity will have a positive association with obfuscation.
>
> H5b: Perceived COVID-19 social media surveillance severity will have a positive association with the chilling effect.

Perceived vulnerability is how susceptible one feels to an imposed threat (Milne et al., 2000). Perceived vulnerability pertains to the perceived potential risk when personal information is revealed (Dinev & Hart, 2004). An individual might expect they are highly susceptible to surveillance problems. Heightened perceived vulnerability is expected to lead to the use of obfuscation to cover up personal information online. Consistent with this logic, we hypothesize perceived vulnerability (i.e., how vulnerable they are to the threats of surveillance) will cause an individual to be less likely to disclose personal information online. We expect this influence to hold in the context of social media behaviors related to COVID-19, as reflected in the following hypotheses:

> H6a: Perceived COVID-19 social media surveillance vulnerability will have a positive association with obfuscation.
>
> H6b: Perceived COVID-19 social media surveillance vulnerability will have a positive association with the chilling effect.

Figure 1 shows our hypotheses in the form of a research model. In the next section, we describe the research method used to test these hypotheses.

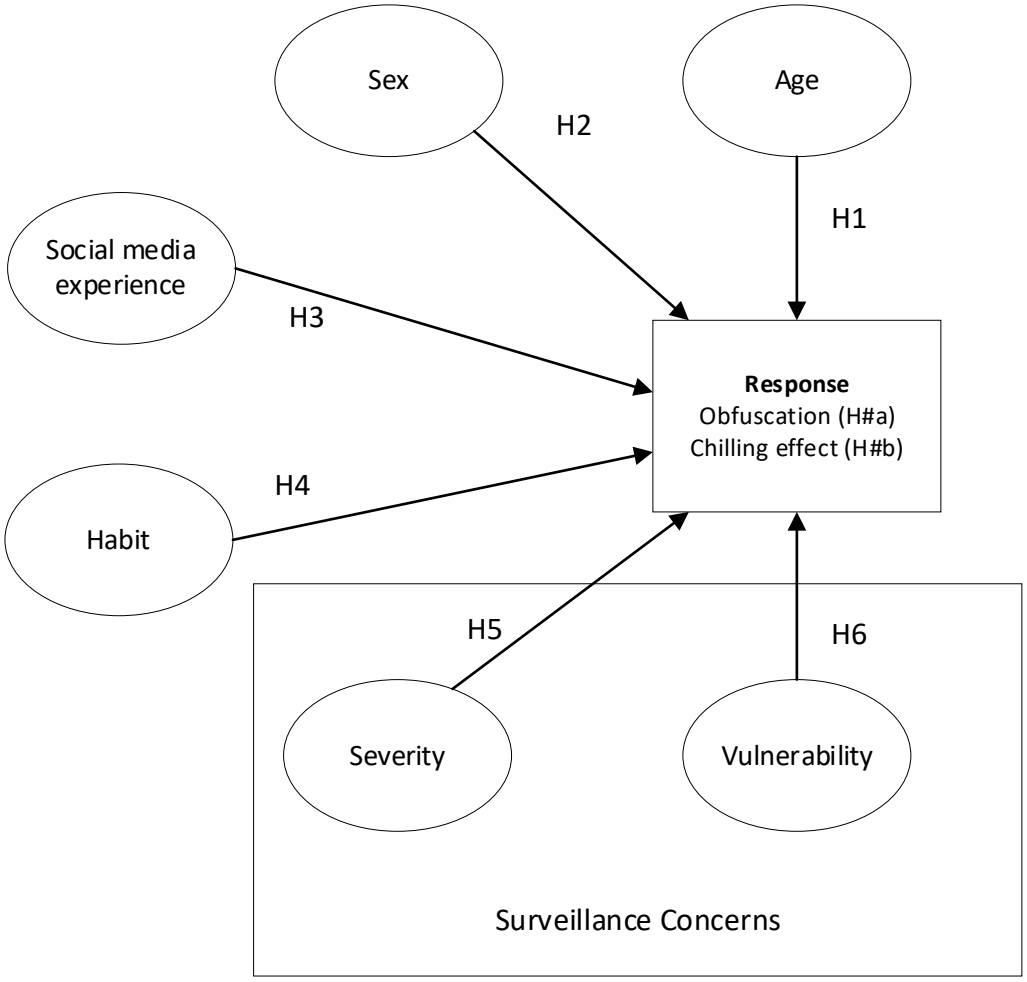

Figure 1. Research Model

Note: Severity and Vulnerability in the figure refer to perceived COVID-19 social media surveillance severity and vulnerability, respectively.

METHOD

To test the hypotheses presented in the last section, we conducted an online survey of adults residing in the United States of America who used social media. We used an online survey panel provider (Qualtrics) to recruit participants.

Sample

Before the main data collection, we conducted a pre-test by inviting several social media users to complete the survey. The pre-test revealed minor problems in survey administration and question-wording. These were resolved before the main data collection. Pre-test responses were not included in subsequent data analysis.

For the main data collection, fifty individuals initially responded to the survey; we then paused data collection to allow an analysis of these responses for issues with survey administration, data quality, and measurement scales. No problems were found, so these responses were retained, and data collection resumed until we received 500 responses. Responses that failed either of two attention check items were rejected, as were incomplete responses. We then applied data quality checks by identifying straight line

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

responses, which we operationalized as 66% or more of the responses corresponding to scale endpoints, and by examining text-based responses for inappropriate or nonsensical responses. Thirty-two problematic responses were identified. These responses were deleted, and data collection resumed briefly. After this data collection, 524 valid responses were received in total. Demographic data for the respondents are provided in Table 1.

Sex	Female – 267 (50.9%) Male – 256 (48.8%) Non-binary – 1 (0.2%)
Age	Mean – 41.21 years Standard deviation – 14.95 years
Country of birth*	USA – 450 (85.7%) Other – 104 (14.3%)
Ethnicity**	White – 417 (79.6%) African-American – 39 (7.4%) Hispanic – 28 (5.3%) Other or more than one – 40 (7.6%)
Years of social media use	< 1 year – 7 (1/3%) 1 year to 2.9 years – 22 (4.2%) 3 to 4 years – 40 (7.6%) > 4 years 455 (86.7%)
Number of social media platforms used regularly	1 – 115 (22.0%) 1 to 3 – 232 (44.2%) 4 or more – 177 (33.8%)

Table 1. Demographic Data

Notes: * - All respondents resided in the USA; ** - less than 100% due to rounding

The final sample was relatively balanced with respect to the sex of the respondents, with 50.9% of the respondents reporting as female. The mean age of the respondents was 41.2 years. Most of the respondents were born in the United States of American. All currently reside in the USA. The respondents were overwhelmingly white (79.6%). Most respondents were quite experienced with social media – 86.7% reported using social media for over four years. Most (78%) used more than one social media platform regularly.

Measures

Existing validated scales were used when possible. Scale items for perceived severity and perceived vulnerability were adapted for the context of this study. New scales were developed for obfuscation use and the chilling effect. Items for these new scales were developed by the authors and reviewed by information systems experts prior to data collection. Scale items and their sources are provided in Table A1 of Appendix A. We represented sex as a dummy variable with female = 1, and male = 0. Social media experience was coded as a dummy variable with those reporting more than four years of social media experience as 1 and those with less than four years of experience as zero.

Descriptive statistics for the scales representing the latent variables are shown in Table 2.

Scale	Mean	Std. Dev.
Severity	4.34	1.72
Vulnerability	3.21	1.36
Habit	2.30	1.36
Obfuscation	6.28	1.10
Chilling effect	4.86	1.76

Table 2. Scale Descriptive Statistics

RESULTS

We used partial least squares structural equation modeling (PLS) using SmartPLS 3.0 (Ringle et al., 2015) to assess our measures and research model. Descriptive statistics were calculated using SPSS Version 26.

Measurement Model

The measurement model confirms the reliability and validity of our measurement scales. Table 3 shows results related to internal consistency and convergent validity. Internal consistency was evaluated using Cronbach's coefficient alpha and composite reliability scores. These should be greater than or equal to 0.70, which was the case for all of our scales. All factor loadings were significant ($p < 0.001$), indicating convergent validity. Further evidence of convergent validity comes from values for Average Variance Explained (AVE), which should be greater than or equal to 0.50. All scales had AVE values higher than 0.50, indicating acceptable convergent validity.

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

Table 3. Internal consistency and convergent validity

Construct	Item	Loading	Cronbach's Alpha	Composite Reliability	AVE
Severity			0.919	0.936	0.712
	Sev1	0.897			
	Sev2	0.912			
	Sev3	0.921			
	Sev4	0.807			
	Sev5	0.750			
	Sev6	0.757			
Vulnerability			0.907	0.929	0.685
	Vul1	0.729			
	Vul2	0.851			
	Vul3	0.820			
	Vul4	0.822			
	Vul5	0.888			
	Vul6	0.847			
Habit			0.897	0.934	0.824
	Habit1	0.892			
	Habit2	0.936			
	Habit3	0.896			
Obfuscation			0.842	0.894	0.678
	Obf1	0.788			
	Obf2	0.811			
	Obf3	0.857			
	Obf4	0.836			
Chilling effect			0.911	0.938	0.791
	Chill1	0.896			
	Chill2	0.931			
	Chill3	0.932			
	Chill4	0.792			

We performed three tests for discriminant validity. The first test involved comparing the square root of AVE to inter-scale correlations, as shown in Table 4. In all cases, the square root of the AVE was substantially higher than the highest inter-scale correlation, indicating acceptable discriminant validity (Fornell & Larcker, 1981).

Table 4. Inter-scale Correlations

	1	2	3	4	5	6	7	8
1. Severity	**0.843**							
2. Vulnerability	0.338	**0.827**						
3. Habit	0.025	0.165	**0.908**					
4. Obfuscation	0.239	0.106	0.102	**0.823**				
5. Chilling effect	0.323	0.260	0.224	0.314	**0.889**			
6. Age	0.072	0.064	0.259	0.181	0.290	**N/A**		
7. SM years	0.107	-0.015	-0.154	0.138	0.091	0.078	**N/A**	
8. Sex - Female	0.048	0.126	0.113	0.151	0.330	0.175	-0.077	**N/A**

Notes: Off-diagonals - Inter-scale correlations; Diagonals – Square root of AVE
SM years = Years using social media; N/A = Not applicable

The second check compares scale item loadings across scales. For appropriate discriminant validity, all scale items should have higher loadings on their intended scales than on any other scales. In all cases, items loaded more strongly on the intended scale than on any other scales, indicating discriminant validity.

An additional check on discriminant validity comes from examining heterotrait-monotrait (HTMT) ratios, which is a more robust discriminant validity check than the approach used above (Henseler et al., 2015). HTMT ratios clearly less than one or with a 95% confidence limit upper bound of less than one indicate discriminant validity. Table 5 shows the HTMT ratios for each latent variable scale. All HTMT ratios are well below 1.0, and all confidence interval upper bounds are similarly well below 1.0, indicating discriminant validity.

Table 5. Heterotrait-Monotrait Ratios

	1	2	3	4
1. Severity				
2. Vulnerability	0.377 (0.465)			
3. Habit	0.053 (0.119)	0.176 (0.275)		
4. Obfuscation	0.263 (0.347)	0.119 (0.208)	0.105 (0.183)	
5. Chilling effect	0.347 (0.437)	0.282 (0.366)	0.231 (0.308)	0.354 (0.440)

Note: The value in parentheses is the upper bound of the 95% confidence interval.

We took three steps to assess the extent of common method variance in our study. First, we performed a Harman single-factor test by loading all study scale items into an exploratory factor analysis (maximum likelihood extraction with no rotation). This analysis yielded seven factors; the highest variance accounted for by any single factor was 22%. We also applied two variations of the more conservative marker variable technique, which uses theoretically unrelated variables to assess common method variance. We included

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

two such variables, blue attitude and preference for sweet foods. To assess common method variance, we examined the correlations between these two marker variables and all other study variables. The average correlations for blue attitude and preference for sweet foods were 0.073 and 0.079, respectively, indicating that common method variance is not a serious problem (Malhotra et al., 2006; Son & Kim, 2008).

Structural Model

Latent variable relationships corresponding to the hypotheses presented in our research model were evaluated by examining the structural model. Table 6 shows the path coefficients and p-values for each hypothesis. As the table indicates, there was general support for our research model. With four exceptions, the hypotheses were supported at $p < 0.01$. H2a and H3a were supported at $p < 0.05$, and H4a was supported at $p < 0.10$. H6a was not supported. Sex was coded with females represented by 0, and males represented by 1. The positive signs on the path coefficients for the sex to obfuscation and sex to chilling effect indicate that females are more likely to engage in both obfuscation and to experience the chilling effect[1].

Table 6. Hypothesis Testing Results

	Obfuscation (H#a)		Chilling effect (H#b)	
Hypothesis/Predictor	**Path coefficient**	**p-value**	**Path coefficient**	**p-value**
H1: Age	0.116	0.002	0.175	< 0.001
H2: Sex - female	0.122	0.004	0.265	< 0.001
H3: Years – social media use	0.127	0.011	0.094	0.016
H4: Habit	0.072	0.085	0.139	0.001
H5: Severity	0.209	< 0.001	0.246	< 0.001
H6: Vulnerability	0.003	0.942	0.111	0.006

Notes: Female was coded as 1, and male as 0.

DISCUSSION

Overview

Our work represents an early effort to better understand what leads to these important reactions to perceived surveillance risks. Obfuscation and the chilling effect are interesting and understudied reactions to surveillance. As is the case with many protective behaviors, they are responses to perceived threats, so their utility is uncertain. If the perceived threat is real, then the effort involved in obfuscating or the potential loss of benefit that results from not posting to social media may be beneficial. But if the threat is only imagined, then the effort or benefit loss is for naught. One factor that makes these protective reactions interesting is that both represent a potential loss of benefits from the use of social media, both for the user and for others. The user loses the benefits that may come from using accurate information, such as connections that may come from the obfuscated data. For example, choosing not to post to social media (the chilling effect) also represents the loss of potential benefits from the post, such as social support or reciprocal information sharing. In the context of a pandemic, there are additional potential losses from obfuscation and the chilling effect. If enough individuals engage in obfuscation or the chilling effect, the effectiveness of social media disease surveillance is reduced. This is especially problematic due to the increasing use of social media surveillance for public health applications, including COVID-19 tracking (Campos-Castillo & Laestadius, 2020).

[1] Analysis of variance (ANOVA) confirms that females are more likely to engage in obfuscation and to exhibit the chilling effect (both $p < 0.001$).

Overall, the efficacy of our research model was confirmed, although the r-square value for obfuscation is low relative to that for the chilling effect. We suspect that this is the result of obfuscation being a general protective mechanism, as opposed to the chilling effect, which was specific to the context of social media surveillance regarding COVID-19. Two of our antecedents, perceived severity, and perceived vulnerability, were specific to COVID-19 surveillance and, unsurprisingly, were stronger predictors of the chilling effect than obfuscation. Future research should explore these relationships further by substituting or adding general surveillance severity and vulnerability for our COVID-19 specific antecedents.

The effect of habit on obfuscation was only marginally significant, perhaps because obfuscation is a protective action that can, but does not necessarily, involve social media posts. For example, the obfuscating effects of a virtual private network are not limited to social media sites. Otherwise, the results related to specific hypotheses were similar across obfuscation and the chilling effect.

Implications for Research

Our research provides several implications for future research. First, we offer an early study of protective responses to perceived surveillance. As noted throughout the paper, we believe that reactions to surveillance will be increasingly important as the use and awareness of surveillance grows. So, understanding some factors that lead to protective responses is a useful starting point for future research.

In particular, we provide a theoretically grounded conceptualization of perceived surveillance risk by including perceived vulnerability and perceived severity. These constructs have their roots in the health beliefs model and protection motivation theory and align with common conceptualizations of perceived risk. Our conceptualization was also empirically confirmed, especially in the case of the chilling effect. Our work provides a starting point for investigations of surveillance in other contexts. Future research could adapt our definitions and measures of perceived vulnerability and perceived severity for different contexts. For example, surveillance concerns could alter various online behaviors, such as Internet search, sensitive email communication, social support seeking, and health information seeking.

Researchers interested in analytics may find it worthwhile to investigate the impacts of obfuscation and the chilling effect on the performance of predictive models. The effects of obfuscation, in particular, may be a serious problem for these models. According to the responses to our survey, obfuscation is quite common. If this is the case, more generally, the predictive efficacy of models that include obfuscated data may be questionable. This raises several interesting issues, including the degree of "noise" introduced by obfuscated data, the extent to which commonly obfuscated data elements (such as location as represented by IP addresses) are used in popular models, and the potential downstream consequences of models affected by obfuscation.

As noted earlier, the effects of obfuscation and the chilling effect could negatively impact epidemiology studies and, by extension, public health. Something as simple as spoofing location data or falsely tagging friends in photos could cause errors in models of disease "hot spots" and disease spread and lead to errors in contact tracing. The chilling effect may have similar impacts. Future research should further investigate how obfuscation and the chilling effect impact these public health applications.

The key to understanding some of the effects noted above may be understanding the cognitive processes related to obfuscation and the chilling effect. Understanding how people weigh the privacy benefits of these protective measures against the loss of utility of related systems. For example, how do people value the protective benefit of using a VPN to mask their location as opposed to the loss of the benefits of location-based search results? As surveillance and datafication increase, and as people become more aware of the potential negative consequences of surveillance, it will be increasingly important to understand the mental drivers of protective measures.

Implications for Practice

Our findings also hold several implications for practice. We discuss these in the paragraphs that follow.

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

The chilling effect may lead individuals who are concerned about surveillance to miss out on potential benefits from using social media to communicate about health-related issues. As mentioned earlier, social media can be an important source of social support and information in times of crisis. Surveillance concerns may lead people to choose not to seek or provide such social support or to withhold information that may be useful to others. This leads to a need for those promoting social media uses to find a way to mitigate surveillance concerns, which will be a challenge since the business models for some social media providers relies on data surveillance.

Taken as a whole, our results present a bit of a conundrum for those who want to engage in data surveillance. Unless they want their surveillance to be completely invisible to users (a stance made increasingly difficult due to increasing data privacy regulations), they must somehow convince users that there will not be harm from the surveillance. However, in doing so, they are likely to raise awareness of surveillance and (possibly) its potential harms. A message intended to ease fears about data collection and use will necessarily bring awareness to the fact that data are being collected and used, which may make users wonder about what is not being clearly disclosed.

Organizations using data about online activities need to be cognizant of the extent and effects of obfuscation. The trend towards increasing the use of analytics based on social media and other data related to online behaviors may be insufficiently aware of the potential consequences of obfuscation and the chilling effect. Widespread use of these protective behaviors will almost certainly have adverse effects on the accuracy of models that rely on such data.

The overarching practical implication of our research concerns an inherent dilemma in data surveillance, especially as it concerns social media. Much of the value and the harm of data surveillance comes from using the data to better understand users and their (supposed) needs and behaviors. However, as awareness of how the data are being used increases, users may be more likely to act in ways that reduce the effectiveness of the data surveillance. If enough users engage in obfuscation, predictive models may become inaccurate, leading to negative consequences for those who depend on such models. This has consequences for all sorts of data surveillance, but it may be especially harmful to public health applications.

Limitations

As is the case with any study, the research presented in this paper has a number of limitations. Perhaps the most important of these is that the data were collected during a unique period, the COVID-19 pandemic. This may have heightened concerns regarding surveillance. So, care should be taken when generalizing our results. However, we expect that the relationships found in our study will persist in other contexts, although we cannot offer empirical evidence to support our contention. Future research is necessary for establishing the robustness of our findings to other contexts. To reduce variability due to respondents' nationalities, we collected data from a single country (the United States). Future research may want to replicate our study using samples from different countries or cultures. Although the percentage of our sample that reported being white (79.6%) is close to the percentage for the United States population (72.3%) (United States Census Bureau, 2021). We did include ethnicity as a control variable, but future research should investigate the effects of ethnicity in more depth.

Our study also rests on several assumptions. For example, we assumed that respondents found some benefit in using social media, which is a precondition for making the effort to engage in protective measures. The levels of use reported by our respondents seem to confirm our assumption. Also, care should be taken in extending our findings to the use of other digital services. Social media is in large part concerned with disclosures about oneself, which likely increases surveillance concerns. Other online activities may be less focused on disclosure, although virtually any online activity discloses some information about oneself. However, these disclosures are often less apparent than they are in the context of social media, which may change the relationships found in our study. Future research should build on our findings by investigating our model in other contexts, such as Internet searching and the use of location-based services.

Our study took place during a unique time. The world was thrown into disarray by the COVID-19 pandemic; some efforts to curb the spread of the disease included digital surveillance measures. As a result, it is likely that current events shaped our findings (especially since we specifically asked about COVID-19 related surveillance in some cases). It would be interesting to replicate our study to compare whether our model holds when COVID-19 surveillance is no longer an immediate concern.

CONCLUSION

In this paper, we empirically tested a model of antecedents to two means of protecting oneself against possible negative consequences of social media surveillance, obfuscation, and the chilling effect, in the context of a pandemic. Our results indicate that individual differences, surveillance concerns, and habit affect both protective measures. Our findings provide insights into these understudied phenomena and provide a useful starting point for further research into obfuscation and the chilling effect. As social media and digital surveillance continue to grow, understanding people's perceptions of and reactions to surveillance will become increasingly important, not only from an instrumental perspective but also as a critical ethical issue confronting digital societies. Although social media surveillance can bring significant benefits, especially during a health crisis, there also exists a serious risk of harm, especially since surveillance is often poorly understood by users and is also typically not highly regulated. Even proponents of surveillance should understand drivers of obfuscation and the chilling effect. If the use of these protective measures grows, there will be a detrimental effect on practices that depend on surveillance. Our paper aims to make the IS field aware of these two factors that were previously overlooked and the antecedents affecting these two factors. We hope that this paper will open the door for IS researchers to further investigate factors that are used by internet users to protect themselves from digital surveillance in the light of social crises.

REFERENCES

1. Agarwal, R., & Prasad, J. (1999) Are individual differences germane to the acceptance of new information technologies? *Decision Sciences*, 30, 2, 361-391.
2. Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., ... & Jha, S. K. (2020). A survey of covid-19 contact tracing apps. *IEEE Access*, 8, 134577-134601.
3. Alhabash, S., & Ma, M. (2017) A tale of four platforms: Motivations and uses of Facebook, Twitter, Instagram, and Snapchat among college students? *Social Media+ Society*, 3, 1, 2056305117691544.
4. Auxier, B., Rainie, L., Anderson, M., & Perrin, A. K. M. & Turner, E. (2019) *American and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, Pew Research Center, November 19.
5. Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR)*, 45(1), 1-54.
6. Baruh, L., Secinti, E., & Cemalcilar, Z. (2017) Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67, 1, 26-53.
7. Bayerl, P. S., & Akhgar, B. (2015) Surveillance and falsification implications for open source intelligence investigations. *Communications of the ACM*, 58, 8, 62-69.
8. Bélanger, F., & Crossler, R. E. (2011) Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, 35, 4, 1017-1041.
9. Brunton, F., and Nissenbaum, H. (2011) Vernacular resistance to data collection and analysis: A political philosophy of obfuscation, *First Monday* 16,5.
10. Brunton, F., & Nissenbaum, H. (2013) Political and ethical perspectives on data obfuscation. In M. Hildebrandt & K. De Vries (Eds.), *Privacy, Due Process and the Computational Turn* (pp. 164–188). New York: Routledge.

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

11. Brunton, F., & Nissenbaum, H. (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.
12. Calvo, R. A., Deterding, S., & Ryan, R. M. (2020) Health surveillance during covid-19 pandemic. *BMJ*, 369:m1373.
13. Campos-Castillo C., and Laestadius L. (2020) Racial and Ethnic Digital Divides in Posting COVID-19 Content on Social Media Among US Adults: Secondary Survey Analysis, *Journal of Medical Internet Research*, 22, 7, e20472.
14. Chang, P. F., Choi, Y. H., Bazarova, N. N., & Löckenhoff, C. E. (2015) Age differences in online social networking: Extending socioemotional selectivity theory to social network sites. *Journal of Broadcasting & Electronic Media*, 59, 2, 221-239.
15. Chiolero, A., & Buckeridge, D. (2020). Glossary for public health surveillance in the age of data science. *J Epidemiol Community Health*, 74(7), 612-616.
16. Chiu, C. M., & Huang, H. Y. (2015) Examining the antecedents of user gratification and its effects on individuals' social network services usage: the moderating role of habit. *European Journal of Information Systems*, 24, 4, 411-430.
17. Coiera, E. (2013) Social networks, social media, and social diseases. *BMJ*, 346:f3007.
18. Crossler, R., & Bélanger, F. (2014) An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: the DATA BASE for Advances in Information Systems*, 45, 4, 51-71.
19. Das, S., & Kramer, A. (2013) Self-censorship on Facebook. In *Proceedings of ICWSM*, 120–127.
20. Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993) *Self-Disclosure*. Newbury Park, CA: Sage.
21. Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006) Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management*, 14, 4, 57-93.
22. Dinev, T., & Hart, P. (2004) Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, 23, 6, 413-422.
23. Dinev, T., Hart, P., & Mullen, M. R. (2008) Internet privacy concerns and beliefs about government surveillance–An empirical investigation. The *Journal of Strategic Information Systems*, 17, 3, 214-233.
24. Dowd, J. B., Andriano, L., Brazel, D. M., Rotondi, V., Block, P., Ding, X., Liu, Y. & Mills, M. C. (2020) Demographic science aids in understanding the spread and fatality rates of COVID-19. *Proceedings of the National Academy of Sciences*, 117, 18, 9696-9698.
25. DreBing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014) Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking*, 17, 2, 61-67.
26. Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011) Negotiating privacy concerns and social capital needs in a social media environment. In *Privacy Online* (pp. 19-32). Springer, Berlin, Heidelberg.
27. Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000) A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30, 2, 407-429.
28. Fornell, C. G., & Larcker, D. F. (1981) Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18, 1, 39–50.
29. Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison*. London: Penguin Books.
30. French, M., & Monahan, T. (2020) Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19? *Surveillance & Society*, 18, 1, 1-11.

31. Galasso, V., Pons, V., Profeta, P., Becher, M., Brouard, S., & Foucault, M. (2020) *Gender Differences in COVID-19 Related Attitudes and Behavior: Evidence from a Panel Survey in Eight OECD Countries* (No. w27359). National Bureau of Economic Research.
32. German, R. R., Horan, J. M., Lee, L. M., Milstein, B., & Pertowski, C. A. (2001). Updated guidelines for evaluating public health surveillance systems; recommendations from the Guidelines Working Group.
33. Gil de Zúñiga, H., Diehl, T., Huber, B., & Liu, J. (2017) Personality traits and social media use in 20 countries: How personality relates to frequency of social media use, social media news use, and social media use for social interaction. *Cyberpsychology, Behavior, and Social Networking*, 20, 9, 540-552.
34. Gilliom, J., & Monahan, T. (2012) SuperVision: *An Introduction to the Surveillance Society*. University of Chicago Press.
35. Haggerty, K. D. (2006) Tear down the walls: on demolishing the panopticon. *Theorizing Surveillance*, 37-59.
36. Halamka, J. D. (2009). Making Smart Investments In Health Information Technology: Core Principles: Five core principles that build on experience and expertise already gained in the fledgling US health IT industry could help avoid the misspending of stimulus and recovery funds. *Health Affairs*, 28(Suppl1), w385-w389.
37. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015) A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43, 1, 115-135.
38. Herath, T., & Rao, H. R. (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, 18, 2, 106-125.
39. Hodge Jr, J. G. (2003). Health information privacy and public health. *The journal of law, medicine & Ethics*, 31(4), 663-671.
40. Howe D. (2015) Surveillance countermeasures: expressive privacy via obfuscation. *APRJA Datafied* Research, 4, 1, 88-98.
41. Hoy, M. G., & Milne, G. (2010) Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, 10, 2, 28-45.
42. Huesch, M. D., Galstyan, A., Ong, M. K., & Doctor, J. N. (2016) Using social media, online social networks, and internet search as platforms for public health interventions: a pilot study. *Health Services Research*, 51, 1273-1290.
43. Ifinedo, P. (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, *Computers & Security*, 31, 83-95.
44. Iwaya, L. H., Fischer-Hübner, S., Åhlfeldt, R. M., & Martucci, L. A. (2018, June). mhealth: A privacy threat analysis for public health surveillance systems. In *2018 IEEE 31st International Symposium on Computer-Based Medical Systems (CBMS)* (pp. 42-47). IEEE.
45. Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016) Age differences in privacy attitudes, literacy and privacy management on Facebook. Cyberpsychology: *Journal of Psychosocial Research on Cyberspace*, 10, 1, article 2.
46. Kotz, D., Gunter, C. A., Kumar, S., & Weiner, J. P. (2016). Privacy and security in mobile health: a research agenda. *Computer*, 49(6), 22-30.
47. Lee, J., Agrawal, M., & Rao, H. R. (2015) Message diffusion through social network service: The case of rumor and non-rumor related tweets during Boston bombing 2013. *Information Systems Frontiers*, 17, 5, 997-1005.

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

48. Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010) *Social media & mobile internet use among teens and young adults. Millennials*. Chicago: Pew Internet & American Life Project.
49. LeRouge, C., Van Slyke, C., Seale, D., & Wright, K. (2014) Baby boomers' adoption of consumer health technologies: survey on readiness and barriers. *Journal of Medical Internet Research*, 16, 9, e200.
50. Li, Y. (2012) Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, 54, 1, 471-481.
51. Limayem, M., Hirt, S. G., & Cheung, C. M. (2007) How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, 31, 4, 705-737.
52. Lin, J. L., & Liu, J. Y. C. (2007, March) Privacy preserving itemset mining through fake transactions. In Proceedings *of the 2007 ACM Symposium on Applied Computing* (pp. 375-379).
53. Litton, A. (2015) The state of surveillance in India: The central monitoring system's chilling effect on self-expression. *Washington University Global Studies Law Review*, 14, 4, 798–822.
54. Malgieri G. (2020) Data protection and research: A vital challenge in the era of COVID-19 pandemic. *Computer Law & Security Review*, 37, 105431. https://doi.org/10.1016/j.clsr.2020.105431
55. Malhotra, N. K., Kim, S. S., & Patil, A. (2006) Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, 52, 12, 1865-1883.
56. Marthews, A., & Tucker, C. E. (2017a) Government surveillance and internet search behavior. Available at SSRN 2412564.
57. Marthews, A., & Tucker, C. (2017b) The Impact of Online Surveillance on Behavior. In D. Gray & S. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* (437-454). Cambridge: Cambridge University Press. doi:10.1017/9781316481127.019
58. Marett, K., McNab, A.& Harris, R. (2011) Social networking websites and posting personal information: An evaluation of protection motivation theory, *AIS Transactions on Human-Computer Interaction*, 3, 3, 170-188.
59. Mariner, W. K. (2007). Mission creep: public health surveillance and medical privacy. *BUL Rev*., 87, 347.
60. Menard, P., Bott, G. & Crossler, R. (2017) User motivation in protecting information security: Protection motivation theory versus self-determination theory, *Journal of Management Information Systems*, 34, 4, 1203-1230.
61. Miller, B. K., & Chiodo, B. (2008) Academic entitlement: Adapting the equity preference questionnaire for a university setting. In *Southern Management Association Meeting*, St. Pete Beach, FL.
62. Milne, S., Sheeran, P., & Orbell, S. (2000) Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30,1, 106-143.
63. Mohamed, N., & Ahmad, I. H. (2012) Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28, 6, 2366-2375.
64. Moorhead, S. A., Hazlett, D. E., Harrison, L., Carroll, J. K., Irwin, A., & Hoving, C. (2013) A new dimension of health care: systematic review of the uses, benefits, and limitations of social media for health communication. *Journal of Medical Internet Research*, 15, 4, e85.
65. Morris, M. G., & Venkatesh, V. (2000) Age differences in technology adoption decisions: Implications for a changing work force. *Personnel Psychology*, 53, 2, 375-403.
66. Nam, T. (2019) What determines the acceptance of government surveillance? Examining the influence of information privacy correlates. *The Social Science Journal*, 56, 4, 530-544.

67. Nsubuga, P., White, M. E., Thacker, S. B., Anderson, M. A., Blount, S. B., Broome, C. V., ... & Trostle, M. (2006). Public health surveillance: a tool for targeting and monitoring interventions. *Disease control priorities in developing countries*, 2, 997-1018.
68. Ortiz de Guinea, A. O., & Markus, M. L. (2009) Why break the habit of a lifetime? Rethinking the roles of intention, habit, and emotion in continuing information technology use. *MIS Quarterly*, 33, 3, 433-444.
69. Paullet, K. L., Rota, D. R., & Swan, T. T. (2009) Cyberstalking: An exploratory study of students at a mid-Atlantic university. *Issues in Information Systems*, 10, 2, 640-649.
70. Penney, J. (2017) Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review*, 6, 2, DOI: 10.14763/2017.2.692
71. Petronio, S. (2000) The boundaries of privacy: Praxis of everyday life. In S. Petronio (Ed.), *Balancing the Secrets of Private Disclosures* (pp. 37–49). Mahwah, NJ: Lawrence Erlbaum Associates, Inc.
72. Polites, G. L., & Karahanna, E. (2012) Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly*, 36, 1, 21-42.
73. Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017) Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior*, 75, 811-825.
74. Ridgway, R. (2015) Personalization as currency. *APRJA Datafied Research*, 4(1), 16-29.
75. Rindfleisch, T. C. (1997) Privacy, information technology, and health care. *Communications of the ACM*, 40, 8, 92-100.
76. Ringle, C.M., Wende, S., and Becker, J.-M. (2015) SmartPLS 3, www.smartpls.com.
77. Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs*, 2(4), 328-335.
78. Sabah, N. M. (2016) Exploring students' awareness and perceptions: Influencing factors and individual differences driving m-learning adoption. *Computers in Human Behavior*, 65, 522-533.
79. Schauer, F (1978) Fear, risk and the First Amendment: Unraveling the "chilling effect", *Boston University Law Review*, 58, 705-714.
80. Smith, E., & Lyon, D. (2013) Comparison of survey findings from Canada and the USA on surveillance and privacy from 2006 and 2012. *Surveillance & Society*, 11, 1/2, 190-203.
81. Son, J. Y., & Kim, S. S. (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32, 3, 503-529.
82. Taddei, S., & Contena, B. (2013) Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29, 3, 821–826.
83. Tanriverdi, H., & Chen, H. (2018) Government's Digital Surveillance and Citizens' Self-Censorship of Technology Use, *Proceedings of the Thirty Ninth International Conference on Information Systems*, San Francisco.
84. United States Census Bureau (2021). American Community Survey 2019 1-Year Estimates Data Profiles, https://data.census.gov/cedsci/table?q=United%20States&g=0100000US&tid=ACSDP1Y2019.DP05.
85. United States Department of Homeland Security. (No Date). Retrieved from: https://www.dhs.gov/national-biosurveillance-integration-center
86. Valente, T. W., & Pitts, S. R. (2017) An appraisal of social network theory and analysis as applied to public health: challenges and opportunities. *Annual Review of Public Health*, 38, 103-118.

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

87. van der Schyff, K., Flowerday, S., & Furnell, S. (2020) Duplicitous social media and data surveillance: An evaluation of privacy risk. *Computers & Security*, 94, 101822.

88. van der Vegt, I., & Kleinberg, B. (2020) Women worry about family, men about the economy: Gender differences in emotional responses to COVID-19. *arXiv preprint* arXiv:2004.08202.

89. van Deursen, A. J., Bolle, C. L., Hegner, S. M., & Kommers, P. A. (2015) Modeling habitual and addictive smartphone behavior: The role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender. *Computers in Human Behavior*, 45, 411-420.

90. Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006) Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7, 6, Article 16.

91. Verplanken, B., & Aarts, H. (1999) Habit, attitude, and planned behaviour: is habit an empty construct or an interesting case of goal-directed automaticity?. *European Review of Social Psychology*, 10, 1, 101-134.

92. Wang, C., Lee, M. K., & Hua, Z. (2015) A theory of social media dependence: Evidence from microblog users. *Decision Support Systems*, 69, 40-49.

93. World Health Organization (WHO) (2020) Timeline of WHO's response to COVID-19, https://www.who.int/news-room/detail/29-06-2020-covidtimeline.

94. Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008) Examining the formation of individual's privacy concerns: Toward an integrative view. *Proceedings of the Twenty Ninth International Conference on Information Systems*, Paris.

95. Yao, M. Z., Rice, R. E., & Wallis, K. (2007) Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, 58, 5, 710-722.

96. Youn, S. (2005) Teenagers' perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49, 1, 86-110.

97. Youn, S. (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43, 3, 389-418.

98. Zhang, D., Feng, X., & Chen, P. (2018) Examining microbloggers' individual differences in motivation for social media use. *Social Behavior and Personality: An International Journal*, 46, 4, 667-681.

99. Zhang, B., Kreps, S., McMurry, N., & McCain, R. M. (2020). Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *Plos One*, 15(12), e0242652.

100. Zmud, R. W. (1979) Individual differences and MIS success: A review of the empirical literature. *Management* Science, 25, 10, 966-979.

101. Zviran, M. (2008) User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems*, 48, 4, 97-105.

APPENDIX

Table A1 shows the scale items used in this study, along with their sources.

Table A1. Scale Items

Perceived severity	If the government were watching my social media communications about COVID-19 it would be a severe problem.	Menard et al. 2017
	If the government were watching my social media communications about COVID-19 it would be serious problem.	Menard et al. 2017
	If the government were watching my social media communications about COVID-19 it would a significant problem.	Menard et al. 2017

	Threats to my privacy through government surveillance of my social media posts about COVID-19 are (Harmless – Harmful)	Ifnedo 2012
	I view government surveillance of my social media posts about COVID-19 as (Harmless – Harmful)	Ifnedo 2012
	Loss of privacy resulting from government surveillance of my social media posts about COVID-19 is a serious problem for me.	Ifnedo 2012
Perceived vulnerability	I know the government could be monitoring my social media communications about COVID-19.	Ifnedo 2012
	The likelihood of the government monitoring my social media communications about COVID-19 is: (Unlikely – Likely)	Ifnedo 2012
	My social media communications about COVID-19 are vulnerable to government surveillance.	Ifnedo 2012
	My social media communications about COVID-19 are at risk for being monitored by the government.	Menard et al. 2017
	It is likely that my social media communications about COVID-19 will be monitored by the government.	Menard et al. 2017
	It is possible that social media communications about COVID-19 will be monitored by the government.	Menard et al. 2017
Habit	Social media is part of my daily routine.	van Deursen et al. 2015
	I use social media automatically.	van Deursen et al. 2015
	It's a habit to use social media.	van Deursen et al. 2015
Obfuscation use	How often do you provide false information about yourself (such as name, home or work address, or birth date), on social media? (Never … Always)	New
	I have provided false information about myself (such as name, birthdate, or home or work address) on social media.	
	I have provided false pictures of myself on social media.	
	I have posted false status updates about myself on social media.	
Chilling effect	I have edited a social media post about COVID-19 due to concerns about government surveillance.	New
	I have deleted a social media post about COVID-19 due to concerns about government surveillance.	
	I have reworded a social media post about COVID-19 due to concerns about government surveillance.	

https://aisel.aisnet.org/jsais/vol8/iss1/2
DOI: 10.17705/3JSIS.00016

	I have decided not to post something about COVID-19 on social media due to concerns about government surveillance.	
Blue attitude	I prefer blue to other colors.	Miller & Chiodo 2008;
	I like the color blue.	Miller & Chiodo 2008;
	I like blue clothes.	Miller & Chiodo 2008;
Food preferences	I prefer sweet foods to savory foods.	New
	I prefer cookies to potatoes.	
	For a snack, I would rather eat candy than potato chips.	