Journal of International Business Studies (2023) 54, 731–754

www.jibs.net

Privacy please: Power distance and people's responses to data breaches across countries

Shilpa Madan[1], Krishna Savani[2,3] and Constantine S. Katsikeas[4]

[1] Pamplin College of Business, Virginia Tech, Blacksburg, Virginia 24061, USA; [2] Faculty of Business, The Hong Kong Polytechnic University, Li Ka Shing Tower, Hung Hom, Kowloon, Hong Kong; [3] Nanyang Business School, Nanyang Technological University, Singapore 639798, Singapore; [4] University of Leeds, Maurice Keyworth Building, Leeds LS2 9JT, UK

Correspondence:
S Madan, Pamplin College of Business, Virginia Tech, Blacksburg, Virginia 24061, USA
e-mail: shilpa.madan@vt.edu

Abstract
Information security and data breaches are perhaps the biggest challenges that global businesses face in the digital economy. Although data breaches can cause significant harm to users, businesses, and society, there is significant individual and national variation in people's responses to data breaches across markets. This research investigates *power distance* as an antecedent of people's divergent reactions to data breaches. Eight studies using archival, correlational, and experimental methods find that high power distance makes users more willing to continue patronizing a business after a data breach (Studies 1–3). This is because they are more likely to believe that the business, not they themselves, owns the compromised data (Studies 4–5A) and, hence, do not reduce their transactions with the business. Making people believe that they (not the business) own the shared data attenuates this effect (Study 5B). Study 6 provides additional evidence for the underlying mechanism. Finally, Study 7 shows that high uncertainty avoidance acts as a moderator that mitigates the effect of power distance on willingness to continue patronizing a business after a data breach. Theoretical contributions to the international business literature and practitioner and policy insights are discussed.
Journal of International Business Studies (2023) **54,** 731–754.
https://doi.org/10.1057/s41267-022-00519-5

Keywords: privacy; power distance; data breach; ownership; uncertainty avoidance; experiments

INTRODUCTION

With the expansion of digital technologies for managing customer, supplier, and employee information, data privacy has become a critical global issue. Data breaches refer to incidents in which people's private data are compromised and accessed against their consent or intent. In 2020, there were 3,932 publicly reported breaches in which hackers stored or exposed 37 billion personal records worldwide, making it the worst year on record for the extent of personal information compromised (Risk Based Security, 2021). A pervasive global issue (Apcela, 2018), data breaches are immeasurably costly for users, businesses, and society alike. For users, a data breach may lead to account theft, credit card theft, and identity theft (Martin & Murphy, 2017). For businesses, data breaches can lead to fines from regulators, customer turnover, loss of reputation, and legal costs. A conservative estimate suggests that the cost of data breaches to businesses globally will be

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1057/s41267-022-00519-5.

Received: 30 September 2020
Revised: 15 February 2022
Accepted: 22 February 2022
Online publication date: 19 May 2022

approximately US$5 trillion by 2024 (Muncaster, 2019). Finally, data breaches, such as the Cambridge Analytica leak that exposed 87 million Facebook users to politically targeted advertisements (Merrill & Goldhill, 2020), have the power to threaten democracies.

Although data breaches pose a threat to users, businesses, and governments worldwide, this issue has not been investigated from an international business perspective. Early research in international business has approached the concept of privacy from policy and governance standpoints, such as territoriality (Kobrin, 2001) and data flow (Samiee, 1984). The limited amount of current research has predominantly focused on how firms respond to data breaches, what costs they incur for breaches, and how breaches affect firm performance (Acquisti, Friedman, & Telang, 2006; Malhotra & Malhotra, 2011). Recent research has also provided policy recommendations, acknowledging that data breaches involve multiple parties, as people share their data both with other individuals and with companies (Kamleitner & Mitchell, 2019). As businesses expand internationally, companies need a clear understanding of how people in different countries respond to data breaches so that they can proactively manage the risks.

Prior research on privacy at the user level has primarily focused on individuals' *privacy concerns*. Specifically, research has examined the factors that affect people's likelihood of sharing their data with businesses. For example, people weigh perceived benefits (e.g., convenience) against potential risks before sharing their data (Culnan & Armstrong, 1999; Dinev & Hart, 2006). Users are more likely to share their data if they trust the firm (Dinev, Bellotto, Hart, Russo, Serra, & Colautti, 2006), if they have control over how the firm would use their data (Martin, Borah, & Palmatier, 2017; Spiekermann & Korunovska, 2017), or if the firm provides them with financial incentives (Gabisch & Milne, 2014; Xu, Teo, Tan, & Agarwal, 2009). In contrast, users are less likely to share their data if they have higher psychological ownership of their data (Menard, Warkentin, & Lowry, 2018; Morewedge, Monga, Palmatier, Shu, & Small, 2021), if they have a high need for control (Königs, 2022; Xu, Dinev, Smith, & Hart, 2011), or if they are concerned about social threats such as bullying or stalking (Krasnova, Günther, Spiekermann, & Koroleva, 2009). Nonetheless, except for Chatterjee, Gao, Sarkar, and Uzmanoglu's (2019) study, which suggests that users who feel more anger (vs. fear) toward data breaches are less (vs. more) sensitive to the scope of the data breach, limited scholarly research attention has been devoted to people's *responses* to data breaches.

In this research, we focus on people's responses to data breaches. Specifically, we examine people's willingness to continue patronizing a business after a data breach, which has significant implications for businesses, users, and public policy. For example, a business may not make significant investments in data security in a given country if residents of the country continue using its services and do not stop patronizing the firm after the data breach. Further, governments and policy institutions may be lax about instituting strict data management laws if citizens do not voice their concerns about privacy violations.[1]

To capture the full extent of the impact of data breaches on users' willingness to patronize a business, we examine people's willingness to continue patronizing a business either after their own data have been compromised (i.e., they have experienced a data breach) or after they are made aware that other users' data were compromised (i.e., they are informed about a data breach). Throughout this research, we follow the General Data Protection Regulation (GDPR) definition of a personal data breach: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR Info, 2018).

Given the extensive potentially negative consequences of data breaches, it is perhaps expected that people would be wary of using a firm's services after a data breach. However, there is a considerable variation in people's responses to data breaches at a cultural level. Survey data from the industry highlight these differences. For example, only 4% of users in Asia reported that they would stop using an app after a data breach was discovered (Yu, 2020). In contrast, 71% of US respondents stated they would stop doing business with a firm if it gave away sensitive data without permission (Anant et al., 2020). Similarly, 74% of U.K. consumers reported that they would not shop with an online business that had experienced a data breach in the past year (PCIPal, 2020). We acknowledge that these responses may be affected by the different methodologies, questions, and samples used by the various companies conducting these surveys. Despite these potential limitations, the cultural variations in people's responses are noteworthy.

These cross-country differences in people's reactions to data breaches raise an important question: What factors predict people's willingness to continue patronizing a business after a data breach? We posit a key role for the cultural value of *power distance*, which taps the extent to which people accept hierarchies and inequalities in power in society (Hofstede, 1980; Oyserman, 2006). Even within a society, individuals differ in the extent to which they accept inequality and hierarchy (Lian, Ferris, & Brown, 2012; Winterich & Zhang, 2014), termed as power distance beliefs. Power distance has been extensively studied in the international business literature but not in the context of data breaches (Dawar, Parker, & Price, 1996; Hui, Au, & Fock, 2004; Jiang, Colakoglu, Lepak, Blasi, & Kruse, 2015). In this research, we propose that power distance affects people's attributions of data ownership, and this, in turn, shapes their willingness to continue patronizing a business after a data breach.

People's ownership attribution, that is, their understanding of who owns the data they have shared with a business, is likely a critical determinant of their response to the loss of personal data in a data breach (Constant, Kiesler, & Sproull, 1994; Jarvenpaa & Staples, 2001). Here, we focus on the types of personal data that are usually shared with businesses as part of ongoing transactions, and that are often compromised in a data breach, including names, birthdays, email addresses, photographs, and other demographics (Gabisch & Milne, 2014; Kamleitner & Mitchell, 2018). We propose that individuals high in power distance beliefs are likely to view the firm as an authority figure, and believe that users are required to transfer ownership to this authority figure in lieu of using their services. Industry surveys find that 75% of users in Asia believe that the onus of protecting their data lies either with businesses or with the government (Yu, 2020), while only 25% of users in the US do so (PwC, 2018). Therefore, people in high power distance countries may believe that their data, once shared with a firm, are no longer theirs. This lack of perceived ownership may make these users more indifferent to the data breach, and, hence, these people may continue to patronize the firm even after the breach.

A data breach is a highly aversive incident that is rife with uncertainty about how the compromised data will be used by unauthorized third parties. Some people are affected by uncertainty more than others, and some cultures are higher in uncertainty avoidance than others (Hofstede, 1980). If people are averse to uncertainty, even if they have high power distance beliefs, they may be motivated to minimize future risk by not sharing any new data with the company after a data breach. Thus, we expect uncertainty avoidance to moderate the relationship between power distance beliefs and users' willingness to patronize a business after a data breach. Specifically, we argue that even users high in power distance beliefs will be more concerned about the potential risks of sharing new data with a firm following a data breach if they are also high in uncertainty avoidance.

In summary, we document and investigate power distance, an important construct in the international business literature, as an antecedent of users' willingness to patronize businesses after a data breach. We propose that users high in power distance beliefs attribute ownership of data to the firm and, thus, do not reduce their transactions with the company following a data breach. Finally, we identify uncertainty avoidance as a theoretically relevant moderator. The present research thus contributes a nuanced consumer-side perspective on a globally pertinent business issue in the digital age. Our focus on data breaches adds a novel perspective to prior research in the international business literature, that has primarily focused on people's *privacy concerns* when they are deciding whether to share their data (Bellman, Johnson, Kobrin, & Lohse, 2004; Milberg, Smith, & Burke, 2000).

Extant research in international marketing has leveraged cultural differences to explain substantive international marketing phenomena (e.g., Dawar et al., 1996; Magnusson, Peterson, & Westjohn, 2014). We contribute to this literature by identifying two novel consequences of power distance: ownership attributions and divergent responses to data breaches. We find that a distal cultural construct such as power distance can illuminate the variance in people's behavior in the context of data breaches. Further, given that most prior work on data breaches has focused on understanding what happens to the firm's stock price or customer transaction patterns using quantitative models, this research strand offers limited insights into how to manage users' expectations about data and data breaches before they occur, to reduce the damage from such incidents (for an exception, see Martin et al., 2017). Because increasing amounts of personal data are shared online, and data breaches are virtually inevitable, this research aspires to provide new insights for

international businesses, NGOs, and public policymakers to help them manage the fallouts from data breaches, and, more importantly, to safeguard the rights of consumers who are particularly vulnerable to such data breaches.

CONCEPTUAL BACKGROUND AND HYPOTHESES

Research on information privacy has largely focused on identifying factors that drive individuals to share their data online. This research is built on the privacy calculus model, or the idea that privacy-related decision-making is a rational process in which people assess the pros and cons of disclosing personal information (Culnan & Armstrong, 1999; Dinev & Hart, 2006). The privacy calculus model posits that "individuals are willing to disclose personal information in exchange for some economic or social benefit subject to the 'privacy calculus,' an assessment that their personal information will subsequently be used fairly and they *will not suffer negative consequences*" (Culnan & Armstrong, 1999: 106, emphasis added). In other words, according to this perspective, people are willing to share their personal data as long as they believe that the benefits gained by disclosure outweigh the potential risks, with the understanding that shared data will not be compromised (Culnan & Beis, 2003). The unfortunate reality is that data shared with businesses are getting compromised across the globe at an alarming rate (Chandler, 2019).

However, there is little research that investigates how users react to their data being compromised, as most extant research on data breaches has largely taken the firm's perspective. For example, firms that have experienced a major data breach typically suffer a sharp drop in their stock price (e.g., Acquisti et al., 2006; Martin et al., 2017; Richardson, Smith, & Watson, 2019). Other research has tracked customer transactions following data breaches to study firm performance (Chen & Jai, 2019; Janakiraman, Lim, & Rishika, 2018). This body of work on data breaches has primarily examined firm-related variables, including size, the degree of transparency about data use, and the level of control over the firm's use of data offered to customers (Martin et al., 2017), along with breach-related variables, such as the number of privacy invasions, reasons for the data breach, vividness of the breach (Chatterjee et al., 2019), and the role of organizational ethics in managing data breaches (Culnan & Williams, 2009). Recent research has also studied the most effective apology that firms may use to regain users' trust after a data breach (Bansal & Zahedi, 2015). The only empirical academic research study from the users' viewpoint suggests that users who are angry (vs. fearful) after a data breach are less (vs. more) sensitive to the scope of the data breach (Chatterjee et al., 2019).

To deepen our knowledge of people's reactions to data breaches, we focus on the antecedents of people's decision to continue patronizing a business after a data breach. Once a firm has experienced a data breach, rational agents might reduce the amount of new data they share with the firm because they have evidence that their data were compromised. Although one might expect that firms would invest more in data protection following a data breach, research shows that firms do not make any significant investments in upgrading their security infrastructure after data breach incidents (Murciano-Goroff, 2019). Nevertheless, there is cultural variation in the extent to which people patronize a business after a data breach. For example, 96% of Asian users are willing to continue using an app after a data breach (Ikeda, 2020), while only 29% of US users are willing to continue transacting with a business that loses their data (Anant et al., 2020). Given the considerable cultural variation in users' decisions following a data breach, we consider whether cultural values are important antecedents.

POWER DISTANCE AND PRIVACY

Power distance, one of Hofstede's core cultural dimensions, is defined as "the extent to which people accept and expect that power is distributed unequally in the society" (Hofstede, 2001: 83), or "the extent to which a society accepts and views as inevitable or functional human inequality in power, wealth, or prestige" (Oyserman, 2006: 503). Power distance does not reflect actual power disparity within a culture, but rather people's attitudes toward power disparity. Asian countries, such as China, Japan, Malaysia, and India, are typically higher in power distance than Western countries, such as Denmark, Austria, the US, and the UK (Hofstede, 2001). Power distance has been operationalized both as a country-level measure (Sivakumar & Nakata, 2001) and as an individual-level measure (power distance beliefs; Hui et al., 2004). Research in international business has found that individuals in high power distance countries rely less on impersonal and objective sources of

product information (e.g., *Consumer Reports;* Dawar et al., 1996), have a lower willingness to adopt new products (Dwyer, Mesak, & Hsu, 2005; Yaveroglu & Donthu, 2002), and are more susceptible to advertising on the Internet (Möller & Eisend, 2010).

Prior research on power distance in the domain of privacy has predominantly focused on people's willingness to *share* their data online and has yielded equivocal findings. For example, Milberg et al. (2000) find that respondents in high power distance countries expressed greater privacy concerns. However, Bellman et al. (2004) found that, although power distance is not associated with people's overall privacy concerns, people from low power distance countries are in favor of greater privacy regulations. This research has focused on country-level analyses and is thus silent on the underlying mechanisms that may explain the effect of power distance on people's privacy concerns (Bellman et al., 2004; Milberg et al., 2000). International businesses are no longer particularly concerned about whether or not people will share their data, but most people readily do so (Chandler, 2019). However, given the ubiquity of data breaches, international businesses need to know how people will respond when they experience or hear about a data breach. Thus, we focus our attention on whether power distance influences people's responses to data breaches (not their general privacy concerns), and on the underlying mechanism that shapes the effect of power distance on users' willingness to continue patronizing a business after a data breach. Given that most complex real-world phenomena are multiply determined, it is possible that the relationship between power distance and willingness to continue patronizing a business after a data breach is likely explained by various factors. Here, we consider users' attributions of who owns the data as one important underlying mechanism.

POWER DISTANCE AND OWNERSHIP ATTRIBUTIONS

In high power distance cultures, people accept that high power entities have control over low power entities (Khatri, 2009). In the context of data breaches, this acceptance of authority implies that low power entities might believe that data ownership rests with higher power entities, not with themselves (Davis, 1997; Joinson & Paine, 2007). In other words, they may attribute data ownership to the firm rather than themselves. The attribution of data ownership is particularly nebulous, as both individuals and firms have claims on ownership of data (Kamleitner & Mitchell, 2018). Although users may sign off on or accept a legal terms-and-conditions statement agreeing that the firm owns the data, their attribution of data ownership may differ from the legal reality. This is because, in digital contexts, in which most data breaches occur, users spend less than a minute browsing the terms and conditions, which average about 6000 words in length (Maronick, 2014). We operationalize ownership attribution on a *continuum* from 100% *user owned* to *100% company owned*, thus capturing a more nuanced understanding of the extent to which ownership attribution may be *shared* between the individual and the firm.

We posit that power distance influences the extent to which users attribute ownership of the shared data to themselves versus the business they share it with because of two key reasons. First, in high power distance cultures, users might believe that businesses have legitimately higher status or authority in society and, thus, command greater ownership over the shared data.[2] Therefore, users in high power distance countries may feel that they are *obligated* or *required* to transfer ownership to the business in lieu of using the services; consequently, these users might think that the authority figure (i.e., the company in this case) owns the data. In contrast, in low power distance cultures, users may feel that it was their choice to upload the data and, thus, the data are theirs. As users from low power distance countries believe that the company compromised the data that belong to them (the user), they are more likely to desist from patronizing the business after the breach.

Second, in high power distance cultures, people might be more willing to take the terms and conditions of using the business at face value, thus accepting that they have transferred ownership of the data to the business because they agreed to such a statement. If people believe that the data are no longer theirs after they share the data with a business, they might think that the data loss is the business's concern. Consequently, people will be less likely to reduce their ongoing transactions with the business.[3] Further, if people believe that the company owns the data, then they may also think that the company would be motivated to protect its data in the future and thus be less concerned about future data breaches. In contrast, in low power distance cultures, if people think that they own their data, they will feel violated as a result of a data breach and, hence, be less likely to

continue their transactions with the business. Figure 1 depicts our theoretical model. Formally, we hypothesize the following:

Hypothesis 1: Users in high power distance countries (or individuals high in power distance beliefs) are more willing to continue patronizing a business after a data breach than users in low power distance countries (or individuals low in power distance beliefs).

Hypothesis 2: Attribution of ownership mediates the effect of power distance beliefs on willingness to continue patronizing a business after a data breach, such that users with high power distance beliefs attribute ownership of the shared data more to the business and less to themselves, and, therefore, are more willing to continue patronizing the business after a data breach.

Importantly, our *ownership attribution* construct is distinct from *psychological ownership*, which captures people's feeling of ownership, or their possessive claim on objects or information (Pierce, Kostova, & Dirks, 2003). Prior research shows that high psychological ownership increases pro-environmental behavior (Hartl, Kamleitner, & Holub, 2020), caring for public goods (Peck, Kirk, Luangrath, & Shu, 2020), and attachment to brands (Kamleitner, Süssenbach, Thürridl, & Ruzeviciute, 2016). Within the context of information privacy, research has found that, when people feel a sense of ownership over their Facebook profiles, they attach a higher monetary value to those profiles if a third party is interested in their data (Bauer, Korunovska, & Spiekermann, 2012; Spiekermann et al., 2012). Recent research also shows that people with a greater pro-self (vs. pro-social) orientation feel less psychological ownership over others' data and, hence, are less likely to share it (Demmers, Weihrauch, & Mattison Thompson, 2021). Ownership attribution of shared data differs from psychological ownership: the former reflects people's understanding of who owns the data they share with a business, while the latter may relate to the extent to which people feel connected with their shared data, see these as a means to build and express self-identity, and feel that their shared data give them a sense of efficacy (see Spiekermann et al., 2012).

MODERTING ROLE OF UNCERTRAINTY AVOIDANCE

A data breach is a highly aversive incident replete with uncertainty about how the compromised data may be used by data thieves. Reducing this uncertainty is an integral part of businesses' data breach response plans (e.g., by offering identity theft protection plans; Ablon et al., 2016). We posit that *uncertainty avoidance* – a cultural value related to people's distaste for uncertainty – moderates the relationship between power distance and the decision to patronize a business after a data breach. Specifically, uncertainty avoidance refers to "the extent to which members of a culture feel threatened by uncertain or unknown situations" (Hofstede, 2001: 161).[4]

It is possible to theorize a main effect of uncertainty avoidance, such that high uncertainty avoidance individuals would be more threatened by a data breach. Two kinds of uncertainties loom large in this case: one is how the compromised data might be misused, and the other is whether there might be additional data breaches following the previous data breach. The uncertainty associated with the former would depend on the specific remedial actions a business may take in response to

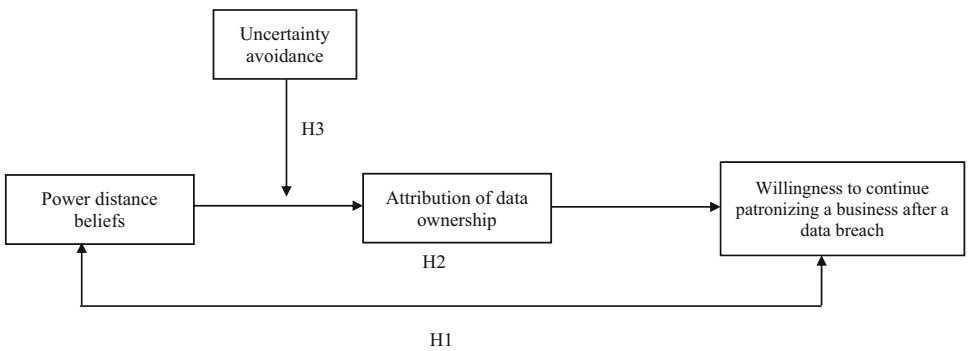

Figure 1 Conceptual model.

a data breach. These include, for example, free credit and identity monitoring following a credit report breach (e.g., Equifax's 2017 breach). The second kind of uncertainty is more relevant in our context, as it can shape whether users continue to patronize the business after a data breach.

We expect uncertainty avoidance to moderate the effect of power distance beliefs on people's willingness to patronize a business after a data breach. As high uncertainty avoidance individuals feel more threatened by uncertainty, they might be less willing to attribute data ownership to the business after a data breach as they are more concerned about the ways in which the data may get compromised again in the future, thereby weakening the effect of power distance beliefs on ownership attribution to the company and, consequently, willingness to continue patronizing the business after a data breach. Thus, for high uncertainty avoidance individuals, we expect the effect of power distance beliefs to be attenuated. In contrast, as users who are low in uncertainty avoidance are not particularly threatened by uncertainty, those with high power distance beliefs would continue to assign greater data ownership to the company, and be willing to patronize a business after a data breach, but not those with low power distance beliefs. Users low in power distance beliefs are not willing to patronize a business after a data breach in the first place, as they attribute data ownership to themselves (rather than the business). Thus, users low in power distance beliefs will continue to be unwilling to patronize a business after a data breach, regardless of whether they are high or low in uncertainty avoidance. Formally, we hypothesize the following:

Hypothesis 3: Uncertainty avoidance moderates the relationship between power distance beliefs and willingness to patronize a business after a data breach, such that high uncertainty avoidance weakens the effect of power distance beliefs on willingness to patronize a business after a data breach by reducing the extent to which users with high power distance beliefs attribute data ownership to the business (vs. themselves).

METHODS

We conducted eight studies to test these hypotheses. Study 1 tested Hypothesis 1 at the country level using archival data. We assessed whether people in high power distance countries continued to pay for an image enhancement app even after an alleged data breach with the app had been publicized. Study 2 tested Hypothesis 1 with victims of actual data breaches. Study 3 tested Hypothesis 1 in the context of the Facebook–Cambridge Analytica data breach in the US. Studies 4 and 5A sought to provide converging causal evidence for both Hypothesis 1 and Hypothesis 2 by manipulating power distance at the organizational and national levels, respectively. Importantly, Study 5B sought to provide additional evidence for the underlying mechanism by directly manipulating people's ownership attributions. Study 6 tested the underlying mechanism using an interaction design in the context of a recent data breach at Twitter. Finally, Study 7 tested the moderating role of uncertainty avoidance. Correlation tables are available in the Online Appendix. The data, code, and stimuli are available here https://osf.io/kgpcj/. Given concerns related to the use of online panels (e.g., Amazon Mechanical Turk; Dennis, Goodson, & Pearson, 2019; Ford, 2017), we only used valid responses that submitted the secret completion code on the online panel(s), and also conducted extensive additional analyses to test the robustness of our findings.[5] These analyses appear in the Online Appendix.

STUDY 1: COUNTRY-LEVEL POWER DISTANCE

Study 1 tests Hypothesis 1 at the country level. Using archival data, we test whether users in high power distance countries will continue to patronize a business even after a potential breach of user data is widely covered in the news media. We used data on the usage of FaceApp, an image-editing app launched in July 2019 (Akpan, 2019). FaceApp quickly became a viral sensation in many countries (Fowler, 2019), as millions of users uploaded their photos to the app to check how they would appear when they got older. However, several news organizations raised concerns about a data breach, highlighting that FaceApp may have sent the users' data to Russia (Grothaus, 2019). This can be classified as a breach, because most users likely assume that their data will be processed on their phone or at least remain in their own country. In the case of FaceApp, news reports mentioned that it was being sent to a foreign country where other countries' privacy laws are not applicable. It was also reported that FaceApp uploads users' photos to the cloud to process them rather than processing them on the user's phone, further increasing the

possibility of unauthorized access by third parties. This news was widely covered in the media (Crist, 2019).

Not surprisingly, given the data breach issues, people's interest in FaceApp began to drop dramatically after these news reports surfaced. We test whether people in high power distance countries continued downloading FaceApp even after this information was revealed in the news media.

METHOD

POWER DISTANCE SCORES

We obtained country-level values for power distance from Hofstede's website (https://geerthofstede.com/research-and-vsm/).

FACEAPP'S CONTINUED USAGE

We operationalized our dependent variable, the continued popularity of FaceApp, as the number of days FaceApp was the highest-grossing app in the Apple App Store in that country after the data breach issues were first reported in the media on July 17, 2019. The news reports quickly spread, receiving extensive coverage between July 17 and July 19, 2019. We tracked FaceApp's ranking in the App Store, based on gross revenues, from July 17 to August 16 on www.sensortowers.com, a mobile app intelligence tracking company. FaceApp was not the highest-grossing app in any country in our dataset after August 16, so we did not track the dependent variable after that date. We used the app's ranking by revenue in each country as an indicator of its popularity, because it provides a strict measure of the app's popularity in any country. Ranking by revenue shows the extent to which users were willing to pay for the app's functionality, not just to download the free version. Importantly, any variable varying across countries (e.g., the number of smartphone users, per-capita gross domestic product, Internet penetration) cannot serve as a confound, because the dependent variable is the number of days that FaceApp was the highest-grossing app in each country compared with other apps in that country.

COVARIATES

Because the news about FaceApp's data issues first broke in English-language media (Crist, 2019), we expected FaceApp's popularity to decline faster in English-speaking countries due to their early access to this information. Thus, we controlled for whether English was the primary language of the country. A search for FaceApp's news coverage revealed that the news was reported simultaneously across non-English-speaking countries in Latin America (Bocchini, 2019) and the EU (Olavario, 2019). Further, users' responses to FaceApp's data breach across countries may be affected by the regulatory framework. Different countries may have different privacy regulations, which may affect the popularity of FaceApp in these countries after the data breach. To account for these differences, we controlled for the presence of privacy regulations across these countries, including legislation about electronic transactions, consumer protection, privacy and data protection, and cybercrime (United Nations Conference on Trade and Development, 2020). All regulations were coded on a 3-point scale (1 = legislation in place, 0.5 = draft legislation, and 0 = no legislation).

RESULTS

The final sample consisted of 58 countries for which both power distance scores and the number of days that FaceApp was the highest-grossing app were available. As our dependent variable was a count variable, we analyzed the data using Poisson regression (Cameron & Trivedi, 2009; Gardner, Mulvey, & Shaw, 1995). We found a significant effect of power distance (b = .02, SE = .00, z = 5.44, $p < .001$), such that FaceApp continued to be the highest-grossing app for a greater number of days after the privacy issues surfaced in countries higher in power distance. In a second Poisson regression, we controlled for whether English was the primary language as well as data protection and privacy legislation across countries. The highest variance inflation factor was 1.15. The effect of country-level power distance continued to be significant (b = .015, SE = .0027, z = 5.44, $p < .001$). Because it is difficult to know for sure whether all non-English-speaking countries received the news of FaceApp's data issues in the specified time period, we also conducted separate analyses for English-speaking and non-English-speaking countries. The effect of power distance on the continued popularity of FaceApp remained significant in each case (see the Online Appendix for additional analysis and the complete list of countries in the dataset).[6]

DISCUSSION

Study 1 provides preliminary support for Hypothesis 1: people in high power distance countries are more willing to patronize a business after a data breach. Specifically, in high power distance

countries, people were more likely to download and pay for the app even after a potential breach of the data uploaded to the app was publicized. A limitation of this study is that we do not control for the amount of news coverage about FaceApp's data breach in each country. While an objective measure of the amount of news coverage is unavailable in the public domain, we acknowledge this as a potential alternative explanation for these results. We address this issue in subsequent studies in which we test our hypotheses within individual countries using both correlational and experimental designs.

STUDY 2: EXPERIENCE OF DATA BREACH

It could be argued that people's responses to data breaches would be different if they experience a data breach themselves, as opposed to only learning about a data breach that other users of a business experienced. Therefore, we designed Study 2 to provide another test of Hypothesis 1 with actual victims of data breaches.

METHOD AND RESULTS

We recruited actual data breach victims through a market research agency in the US. We carefully screened participants to ensure that they had actually experienced a data breach. Specifically, participants were first asked to specify the organization with which they had experienced the data breach. Next, they were required to upload a proof of communication (without identifying information) from the organization notifying them about the data breach. Participants who wrote incorrect or irrelevant text when asked for the name of the organization (e.g., "not sure") were eliminated. A total of 107 respondents (39.25% women, M_{age} = 45.44 years) completed the study. Participants named a heterogeneous set of organizations with which they had experienced data breaches (e.g., Equifax, Facebook, Google, PayPal).

We asked participants to rate the extent to which they continued patronizing the business after the data breach using four items: (1) How often did you use [the business] after the data breach? (7-point scale: 1 = less often than before, 7 = more often than before), (2) how much did you use [the business] after the data breach? (7-point scale: 1 = less than before, 7 = more than before), (3) because of this data breach, did you think of not patronizing [the business]? (7-point scale: 1 = definitely yes, 7 = definitely not), and (4) because of this data breach, did you think of cutting ties with [the business]? (7-point scale: 1 = definitely yes, 7 = definitely not). Participants also responded to the 5-item power distance beliefs scale (e.g., People in higher positions should make most decisions without consulting people in lower positions; α = .85; Yoo, Donthu, & Lenartowicz, 2011). We averaged the four items assessing participants' willingness to continue patronizing the business after the data breach (α =.79), which we used as the dependent measure. Consistent with Hypothesis 1, participants' power distance beliefs were positively correlated with their willingness to continue patronizing the business [r = .27, 95% CI (.085, .44), p = .005]. In addition, people's willingness to stop patronizing a business after a data breach may be affected by the number of alternatives available for the services provided by these businesses. However, controlling for the number of alternatives available did not affect the results (see Online Appendix for this additional analysis). Further, heterogeneity in the severity of the data breach across businesses in this study may have also affected users' willingness to continue patronizing the business. We address this possibility in the next study.

STUDY 3: FACEBOOK–CAMBRIDGE ANALYTICA DATA BREACH

While Study 2 is important because it tests Hypothesis 1 with actual victims of a data breach, some variance in participants' responses may be driven by the heterogeneity in the type of organization(s) with which they experienced the data breach (e.g., business, higher education, government) and the severity of the individual data breach. We designed Study 3 to eliminate this variance by keeping the target organization constant. To increase the practical relevance of this research, the context for Study 3 was the Facebook–Cambridge Analytica data breach, perhaps the most widely publicized and consequential data breach to date (Wong, 2019). Specifically, we investigated whether users with high power distance beliefs would be more likely to continue patronizing Facebook even after this data breach was revealed. We also assessed the extent to which people blamed Facebook for the breach. We reasoned that users high in power distance beliefs would blame Facebook less, because they would attribute greater ownership of the compromised data to Facebook than to themselves. We chose to conduct this study

in only one country, the US, as the Cambridge Analytica leak was most relevant to US residents.

METHOD

A total of 119 US participants (47.9% women, M_{age} = 38.2 years) completed the study on Amazon Mechanical Turk. Participants responded to the power distance beliefs scale (α = .87), same as in Study 2. Next, participants were told that Facebook's CEO, Mark Zuckerberg, was recently called to the US Senate to testify about a personal data breach for 87 million users. These individuals' personal data were shared with a company called Cambridge Analytica, which then used this information to target these Facebook users with political advertising. Participants were requested to consider that they received a notification from Facebook informing them that their data were shared with Cambridge Analytica.

We then asked participants how they would respond to this data breach. Our measure used four items (i.e., post less information on Facebook, review their privacy settings, delete highly personal information, and sign a petition asking Facebook to follow stricter protocols), all on a 7-point scale ranging from not at all likely to extremely likely (α = .79). We averaged the responses to these items to form a measure of reduced willingness to use Facebook after this data breach. We also asked participants how much they blamed Facebook for this loss of privacy, also on a 7-point scale ranging from not at all to extremely.

RESULTS

We regressed participants' reduced willingness to use Facebook on their power distance beliefs. We found that participants with high power distance beliefs were less likely to reduce their Facebook use (b = –.201, SE = .091, β = –.201, $t_{(117)}$ = 2.16, p = .033), in support of Hypothesis 1. Further, as we expected, they were also less likely to blame Facebook for the loss of privacy (b = –.31, SE = .087, β = –.31, $t_{(117)}$ = 3.52, p = .001). We provide additional analysis in the Online Appendix.

Study 3 offers further support for Hypothesis 1 at the individual level. Together, Studies 1–3 show that power distance strongly predicts users' reactions to data breaches at both global and individual levels.

STUDY 4: CAUSAL EVIDENCE MANIPULATING ORGANIZATIONAL POWER DISTANCE

In recent years, the internal employee information of numerous multinational corporations has been publicly exposed (Osborne, 2020). We manipulated power distance at an organizational level to test employees' willingness to continue using a software recommended by the organization, even after being informed that a security problem with the software led to their personal information being compromised (Hypothesis 1). We also tested the underlying mechanism of ownership attribution (Hypothesis 2). This study was inspired by a recent internal data breach incident at a multinational company, but the stimuli presented to participants were hypothetical to avoid any confounds due to familiarity or other past experience with the company.

METHOD

A total of 201 US participants (57.21% women, M_{age} = 44.13 years) completed the study on CloudResearch. We used a power distance (low vs. high) between-subjects design for this study. To manipulate power distance, participants were told that they had recently joined the VIF Corporation as marketing support staff. Participants were then asked to read a brochure containing VIF Corporation's organizational values. Participants were either assigned to the *low power distance* condition or the *high power distance* condition. In the *high power distance* condition, participants were told that VIF Corporation believed in a hierarchical culture. The following is an excerpt from the brochure they read:

> VIF Corporation owes its success in large part to a clear and hierarchical company structure. We believe that of course, the senior management has greater power than all other employees in VIF. We believe that the company functions most efficiently when employees follow the established structure and hierarchy. We do not expect managers to consult their subordinates for important decisions.

Participants in the *low power distance condition* read that the VIF Corporation valued a flat and egalitarian culture. The following is an excerpt from the brochure they read:

> VIF Corporation owes its success in large part to an egalitarian and flexible company structure. We do not believe that the senior management has greater power than all other employees in VIF. We believe that the company functions most efficiently when employees at all levels work with one another in an egalitarian way. We expect managers to consult with their subordinates for important decisions.

After reading the brochure, all participants were asked to describe the culture at VIF Corporation in an open-ended question. As a manipulation check, all participants responded to the item "VIF Corporation is … [an egalitarian organization (1) to a hierarchical organization (7)"].

Participants next read that VIF Corporation uses a software called ChatterBox for internal communications. To ensure that participants understood that ChatterBox was not critical to company operations and only intended as an internal communications tool, they were told that ChatterBox was like Facebook, but for VIF employees. Participants read that there was a data breach due to a lapse in VIF's security, and their personal data (e.g., name, gender, profile photo, communication with coworkers) were compromised. They indicated their willingness to continue using ChatterBox by responding to four items (e.g., "How likely are you to start using alternative means of communication, such as WhatsApp or Slack, to communicate with your co-workers?" "How likely are you to reduce what you share or discuss on ChatterBox"?), all on 7-point scales ranging from not at all likely to extremely likely. As it is unlikely that employees in any company can refuse to use company software, we ensured that our dependent measure assessed "reduction" in use, which the employees could do, rather than completely boycotting the software, which may not be feasible.

Participants also indicated who they thought owned the data collected on ChatterBox on a 100-point slider scale (1 = the employee has full ownership, 100 = VIF has full ownership of the data).[7] Participants were asked to select any point on the slider scale to indicate the ownership between the employee and VIF corporation. Moreover, because reading about a strongly hierarchical company may be aversive for US participants, we measured their mood through the question "How do you feel right now?" through four items (e.g., bad/good, sad/cheerful) using 7-point bipolar scales.

RESULTS

MANIPULATION CHECK

A t test found that participants in the *high power distance* condition (M = 6.82, SD = .69) were more likely to believe that VIF was a hierarchical organization than participants in the *low power distance* condition (M = 1.44, SD = .96; $t_{(198)}$ = 45.33, $p <$ .001, Cohen's d = 6.41), thus indicating that the manipulation was successful.

MAIN EFFECT (Hypothesis 1)

We reverse-coded and averaged the four items assessing employees' willingness to continue using ChatterBox as before (α =.79) to form our dependent measure, such that higher scores indicated participants' greater willingness to continue using ChatterBox as they did before the data breach. Confirming Hypothesis 1, a t test revealed that participants in the *high power distance* condition (M = 2.92, SD = 1.39) were more willing to continue using ChatterBox despite the data breach than those in the *low power distance* condition (M = 2.45, SD = 1.32; $t_{(199)}$ = 2.47, p = .014, Cohen's d = .35). This provides causal evidence for Hypothesis 1. Participants' mood was unaffected by the manipulation (p = .29).

MEDIATION THROUGH ATTRIBUTION OF OWNERSHIP (HYPOTHESIS 2)

We reverse-coded the ownership attribution measure, such that higher scores indicated greater ownership residing with the individual employee (vs. VIF Corporation). As hypothesized, a t test indicated that participants in the *high power distance* condition (M = 15.64, SD = 24.56) attributed lower data ownership to the employee than participants in the *low power distance* condition (M =30.049, SD = 27.55; $t_{(199)}$ = 3.91, $p <$ .001, Cohen's d = .55). We also ran a bootstrapped analysis using Model 4 of Hayes' (2013) PROCESS macro (20,000 resamples). As expected, we found a significant indirect effect of power distance on employees' willingness to continue using the software after a data breach through lower attribution of data ownership to the employees [b = .14, SE = .063, 95% CI (.037, .28)]. The direct effect was no longer significant (b = .33, SE = .201, 95% CI (− .054, .72)], which indicates full mediation.

DISCUSSION

This study provides causal evidence that high power distance increases the willingness to continue using goods and services affected by a data breach (Hypothesis 1), and that high power distance reduces the attribution of ownership to the individual, leading to greater willingness to continue using a service despite a data breach (Hypothesis 2). We also tested the role of trust in the organization as an alternative mechanism, but did

not find support for it (see Online Appendix for additional analysis).

STUDY 5A: CAUSAL EVIDENCE MANIPULATING NATIONAL POWER DISTANCE

The goal of Study 5A was to conceptually replicate the key finding of Study 4 by manipulating national culture rather than organizational culture. To enhance the ecological validity of this research, we adapted the study based on an existing Covid-19 contact-tracing app (Baharudin, 2021; TraceTogether, 2021). As people likely have strong views about Covid-19 and related technologies in their own country, we adapted this incident to create a hypothetical situation.

METHOD

The materials, analysis plan, and sample size for this study were pre-registered (https://osf.io/zkv8h/?view_only=2da70613711445448f681f1e0c907ff2).[8] We posted the study for 200 behavioral laboratory participants at a large university in the US. In response, 200 participants (64.17% women, M_{age} = 20.48 years) completed the study. Participants were randomly assigned to either the *high power distance* or the *low power distance* condition. They read a short article about the Solomon Islands, a small island state in the Pacific Ocean. In the *high power distance* condition, participants were told that the people of the Solomon Islands believed in hierarchy. The following is an excerpt from the article they read:

> The people of the Solomon Islands believe that a well-functioning society needs to be hierarchical in nature. They believe that, of course, some individuals, institutions, and organizations have greater power than others. In other words, they accept that power is distributed unequally in the society. They believe that differences in hierarchy are necessary to maintain social order.

Participants in the *low power distance* condition read that the people of the Solomon Islands believed in equality and egalitarianism. The following is an excerpt from the article they read:

> The people of Solomon Islands believe that a well-functioning society needs to be egalitarian in nature. They believe that no individual, institution, or organization has greater power than others. In other words, they strive to ensure that power is distributed equally in society. They believe that egalitarianism is necessary to maintain social order.

All participants were then asked to describe the culture of Solomon Islands in an open-ended question. As a manipulation check, they responded to three items (e.g., "Hierarchy is often times necessary to maintain social order," "Hierarchy is inevitable") on 7-point scales ranging from do not agree to agree strongly.

Next, participants were told that, in recent months, there had been a consistent increase in the number of Covid-19 cases in the Solomon Islands. To help with contact tracing, the government introduced the TraceInfection app.[9] The app uses Bluetooth technology to identify people who were physically close to each other on a given day. Participants also read that the app is being used by 89% of people in the Solomon Islands. Similar to Study 4, to assess ownership attributions, participants indicated who they thought owns the data collected on the TraceInfection app on a 100-point slider scale (1 = the individual has full ownership of the data, 100 = the government has full ownership of the data).

Participants subsequently read that Solomon Island's government recently acknowledged that data collected through the contact-tracing app were used by the police for criminal investigations, and that, in the future, the data may be used to investigate any breaches of existing rules. Participants were then asked to imagine that they were a citizen and longtime resident of the Solomon Islands. Participants then indicated their willingness to continue using the contact-tracing app despite this potential data breach as a Solomon Island citizen (e.g., "How likely do you think that you will continue using the TraceInfection app?") on a 7-point scale from not at all likely to extremely likely.

RESULTS

MANIPULATION CHECK

A *t* test indicated that participants in the *high power distance* condition (M = 5.49, SD = 1.43) were more likely to agree that citizens of the Solomon Island accept hierarchy in their society than participants in the *low power distance* condition (M = 3.073, SD = 1.66; $t_{(198)}$ = 11.042, $p < .001$, Cohen's d = 1.56), thus indicating that the manipulation was successful.

MAIN EFFECT (HYPOTHESIS 1)

As hypothesized, a *t* test revealed that participants in the *high power distance* condition (M = 4.09, SD = 1.83) were more likely to indicate that they would continue using the app than those in the *low power distance* condition (M = 2.59, SD = 1.66; $t_{(198)}$ = 6.071, $p < .001$, Cohen's d = .86), thus providing causal evidence for Hypothesis 1.

MEDIATION THROUGH ATTRIBUTION OF OWNERSHIP (HYPOTHESIS 2)

We reverse-coded this measure such that higher scores indicated greater ownership residing with the individual (vs. the government). As hypothesized, a *t* test indicated that participants in the *high power distance* condition (M = 21.1, SD = 20.00) attributed lower data ownership to the individual than participants in the *low power distance* condition (M = 38.091, SD = 30.029; $t_{(197^{10})}$ = 4.702, $p <$ .001, Cohen's d = .67).

To test the mediation hypothesis, we ran a bootstrapped analysis using Model 4 of Hayes' (2013) PROCESS macro (20,000 resamples). We found a significant indirect effect of the power distance manipulation on willingness to continue using the app through lower attribution of data ownership to the individual (b = .16, SE = .087, 95% CI (.0042, .35)], thus providing evidence for Hypothesis 2. The direct effect was also significant (b = 1.37, SE = .26, 95% CI (.86, 1.88)], which indicates partial mediation.

DISCUSSION

Study 5A provides additional causal evidence for our key hypothesis that power distance increases people's willingness to continue using a service after a data breach in an ecologically valid setting. This study provided further experimental evidence for the proposed underlying mechanism that in high power distance cultures people to attribute less data ownership to themselves, which increases their willingness to continue patronizing the service after a data breach. We conceptually replicated these results with US residents on CloudResearch™ in an additional study (please see Online Appendix for details).

STUDY 5B: MANIPULATING OWNERSHIP ATTRIBUTION

Study 5B provides another test of the role of ownership attribution as the underlying mechanism (Hypothesis 2) by using the experimental causal chain paradigm (Spencer, Zanna, & Fong, 2005). Although Studies 4 and 5A provided support for the underlying causal chain using a mediation analysis, this method suffers from numerous shortcomings (Zhao, Lynch, & Chen, 2010). We thus used the experimental causal chain method to show mediation (Spencer et al., 2005). Study 5A tested the first half of the causal chain, that is, experimentally manipulating power distance to influence people's ownership attribution of their data. Study 5B tests the second half of the causal chain, that is, whether experimentally manipulating the ownership attributions would influence people's willingness to continue patronizing a service after a data breach. Specifically, we experimentally vary whether people believe that they have ownership of their data or the entity with which they shared their data.

METHOD

A total of 98 US-based participants (42.42% female, M_{age} = 35.23 years) on Prolific Academic completed the study.[11] We randomly assigned them to either the ownership-attribution-to-self condition or the ownership-attribution-to-provider condition. Participants read that the Solomon Islands, a small state in the Pacific Ocean, had introduced a contact tracing app to reduce the spread of Covid-19. In the ownership-attribution-to-self condition, participants were told that "When users install the app, the terms of use state that all personal and location data collected by the app belongs to the user." In the ownership-attribution-to-provider condition, participants read that, "When users install the app, the terms of use state that all personal and location data collected by the app belongs to the government."

Participants then responded to the manipulation check question "According to the terms of use, who owns the data collected on the TraceInfection app?" (1 = the government has full ownership, 4 = the user and the government equally own the data, and 7 = the user has full ownership of the data). Next, participants read that the Solomon Island's government recently announced that the police would have full access to the data collected through the contact-tracing app as part of their crime investigations. All participants then indicated their willingness to stop using the contact-tracing app using 3-items (e.g., "If you were a resident of Solomon Islands, what is the likelihood that you would uninstall the TraceInfection app?" on a 7-point scale ranging from not at all likely to *extremely likely*).

RESULTS

MANIPULATION CHECK

A *t* test indicated that participants in the ownership-to-self condition (M = 5.601, SD = 2.101) attributed greater data ownership to themselves compared to participants in the ownership-

attribution-to-provider condition (M = 1.43, SD = 1.068; $t_{(96)}$ = 12.13, $p < .001$, Cohen's d = 2.46), indicating that the manipulation was successful.

MAIN EFFECT (HYPOTHESIS 1)

We reverse-coded and averaged the three items assessing people's willingness to continue using the app (α = .89) to form our dependent measure, such that higher scores indicated greater willingness to continue using the app. As hypothesized, a t test revealed that participants in the ownership-attribution-to-provider condition (M = 3.98, SD = 1.87) were more willing to continue using the app than those in the ownership-attribution-to-self condition (M = 3.15, SD = 1.85; $t_{(96)}$ = 2.19, p = .031, Cohen's d = .44).

DISCUSSION

When considered together, Study 5A and Study 5B provide evidence for the underlying mechanism using the experimental causal chain method (Spencer, Zanna, & Fong, 2005). These studies suggest that ownership attributions mediate the effect of power distance on support for willingness to continue patronizing a service after a data breach.

STUDY 6: PROCESS BY INTERACTION

Study 6 provides another test of the role of ownership attribution as the underlying mechanism (Hypothesis 2) by using a mediation by moderation design. Specifically, we experimentally vary whether people believe that they have ownership of their data or the business with which they shared their data. We used a recent data breach on Twitter as the context for this study (Romm, 2019).

METHOD

A total of 141 business school undergraduate students (67.83% female, M_{age} = 20.37 years) completed the study for course credit. We randomly assigned them to either the ownership-attribution-to-self condition or the ownership-attribution-to-business condition. Those in the ownership-attribution-to-self condition read that, when they upload their information to any app or website, they retained ownership of their data; that is, simply uploading their data does not transfer data ownership. Participants in the ownership-attribution-to-business condition read that when they upload their information to any app or website, they transfer ownership of their data to the app; in other words, the app owns the data.

As a manipulation check, participants indicated their attribution of data ownership when they uploaded their information to any website or app. They indicated who owns the data when they share their personal information and pictures. Participants responded on a 100-point slider scale (1 = they retain full ownership, 100 = the app has full ownership).

Subsequently, participants were asked to imagine that they used Twitter regularly. Recently, they received an email from Twitter stating that, due to a coding error, some of their personal information, including their name, gender, profile photo, and location data, were shared with Twitter's ad partners even when their personal preference was not to do so. This scenario was based on an actual Twitter data breach (Romm, 2019). Participants then indicated their willingness to continue using Twitter after experiencing this data breach using two items ("How willing are you to continue using Twitter?" and "How likely are you to continue using Twitter?"), both measured on seven-point scales ranging from not at all to extremely. The average of these items (r = .87) formed our dependent variable. As in Study 2, we measured power distance using a five-item scale (α = .73; Yoo et al., 2011).

RESULTS

First, a t test showed that participants in the ownership-attribution-to-business (M = 72.24, SD = 26.13) condition assigned greater ownership of data to app/website, compared to participants in the ownership-attribution-to-self (M = 42.38, SD = 28.98, $t(136^{12}) = 6.36$, $p < .0001$, Cohen's d = 1.08) condition. In accordance with Hypothesis 2, we expected participants' power distance to be positively correlated with their willingness to continue using Twitter, despite a data breach, when they were told that the app/website owns the data (i.e., in the ownership-attribution-to-business condition). However, we expected the relationship between power distance and willingness to continue using Twitter, despite a data breach, to be attenuated when participants were told that they (the users) own the data (i.e., ownership-attribution-to-self condition).

To test this, we regressed participants' willingness to continue using Twitter on their power distance beliefs (mean-centered), ownership attribution

(business = –1, self = 1), and their interaction (mean-centered). The highest variance inflation factor was 1.11. Lending support to Hypothesis 1, this analysis revealed a significant effect of power distance beliefs (b = .48, SE = .16, β = .26, $t_{(137)}$ = 3.05, p = .003) and a nonsignificant effect of ownership attribution manipulation (b = .036, SE = .26, β = .011, $t_{(137)}$ = .14, p = .89). More importantly, and as we expected, the interaction was significant (b = –.701, SE = .32, β = –.19, $t_{(137)}$ = 2.22, p = .028). We found that, in the ownership-attribution-to-business condition, power distance beliefs predicted willingness to use Twitter after the data breach (b = .83, SE = .24, β = .38, $t_{(69)}$ = 3.39, p = .001), in support of Hypothesis 2. However, this link was nonsignificant in the ownership-attribution-to-self condition (b = –.13, SE = .19, β = .081, $t_{(137)}$ = .67, p = .504) (see Figure 2). We provide additional analysis in the Online Appendix.

DISCUSSION

Study 6 demonstrates that making ownership attribution salient may be a potential intervention to discourage users high in power distance beliefs from continuing to patronize a service after a data breach. Although this relationship holds only when users attribute data ownership to the business (and not to the self), we did not observe a main effect of ownership attribution on willingness to patronize the business (which we consistently found in the previous three studies). This could be due to two key differences between the design of this study and that of the previous studies. First, Studies 4 and 5A–5B measured (or manipulated) ownership attribution and willingness to patronize the business with reference to the same app (i.e., ChatterBox for Study 4 and the contact tracing app for Studies 5A and 5B). In contrast, Study 6 manipulated ownership attribution in general but asked about users' willingness to use Twitter after the data breach. Second, this study was conducted with a younger, student sample. The mean levels of power distance beliefs in the student sample were much lower than the general sample used in the other studies, in which power distance beliefs were measured (see Online Appendix for details). It is possible that being exposed to the message that businesses have ownership of their data (in the ownership-attribution-to-business condition) may be highly aversive to individuals in this sample who were predominantly low in power distance beliefs and, therefore, may have reacted against this message.

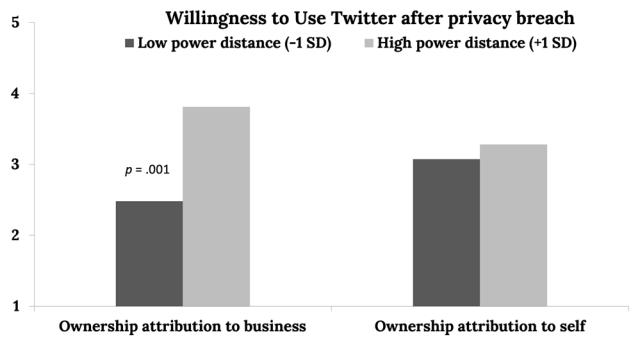

Figure 2 Interaction between power distance beliefs and ownership attribution on willingness to use Twitter after a data breach in Study 6

STUDY 7: MODERATING ROLE OF UNCERTAINTY AVOIDANCE

We designed Study 7 to accomplish multiple objectives. We test the moderating role of uncertainty avoidance (Hypothesis 3), the main effect of power distance beliefs (Hypothesis 1), and the mediating role of ownership attribution (Hypothesis 2).

METHOD

A total of 250 US participants (52.40% female, M_{age} = 43.6 years) completed the study on CloudResearch. We told participants that they recently heard about a new app called FacePlay. They read that FacePlay is an image-editing app powered by advanced "selfie editing technology" that allows them to transform their selfies. Participants then saw an image illustrating the functionality of the app, its ability to correct and/or enhance facial features, apply make-up, and change the backgrounds of images. We used the typical functionality included in such apps to create the description of features offered by FacePlay.

Participants were asked to consider that they recently came across a news article claiming that FacePlay saves users' images in their database without their consent, thus compromising users' privacy. Participants were further told that FacePlay's privacy policy says that it can use these pictures for research and development and can share these pictures with third-party agencies.

WILLINGNESS TO USE AND RECOMMEND THE APP

We asked participants to indicate their preference for the app using four items (e.g., "How willing are you to use FacePlay?" "How likely are you to

recommend FacePlay to friends and family?"), all on seven-point scales ranging from not at all to extremely. The average of these items (α = .98) formed our dependent variable.

POWER DISTANCE

We measured power distance beliefs using the five-item scale (α = .94) as in Study 2.

OWNERSHIP ATTRIBUTIONS

Similar to previous studies, we asked participants, "When you use an app, where you add your personal information and pictures, according to you, who owns that information? On the scale below, where 1 = you retain full ownership of your information and 100 = the app has full ownership of your information; please choose any point to indicate the sharing of ownership between you and the app."

UNCERTAINTYncertainty avoidance

We measured participants' uncertainty avoidance using five items (e.g., "It is important to have instructions spelled out in detail so that I always know what I am expected to do") on a five-point scale, ranging from strongly disagree to strongly agree (α = .81; Yoo et al., 2011).

RESULTS

MAIN EFFECT (HYPOTHESIS 1)

The average willingness to use and recommend the FacePlay app was our dependent measure. Regressing participants' willingness to use the app on their power distance beliefs revealed a significant positive effect (b = .71, SE = .058, β = .62, $t_{(248)}$ = 12.28, p < .001), lending support to Hypothesis 1.

MEDIATION THROUGH OWNERSHIP ATTRIBUTION (HYPOTHESIS 2)

We reverse-coded our measure of ownership attribution so that higher numbers indicated greater ownership with the user (vs. the app). Regressing ownership attribution on power distance beliefs revealed a significant negative effect (b = –8.64, SE = 1.28, β = –.39, $t_{(248)}$ = 6.75, p < .001), such that participants with high power distance beliefs attributed lower data ownership to themselves. To test the mediation hypothesis, we ran a bootstrapped analysis using Hayes' (2013) PROCESS macro (Model 4; 20,000 resamples). We found a significant indirect effect of power distance beliefs on greater willingness to use the FacePlay app through lower ownership attribution of personal data to the user (b = .071, SE = .022, 95% CI (.0302, .12)]. The direct effect was significant as well (b = .64, SE = .062, 95% CI (.52, .76)], which indicates partial mediation.

MODERATING EFFECT OF UNCERTAINTY AVOIDANCE (HYPOTHESIS 3)

To assess the moderation hypothesis, we regressed participants' willingness to use FacePlay on power distance beliefs (mean-centered), uncertainty avoidance (mean-centered), and their interaction. The highest Variance Inflation Factor was 1.06. This revealed a significant effect of power distance beliefs (b = .73, SE = .057, β = .64, $t_{(246)}$ = 12.78, p < .001) and a nonsignificant effect of uncertainty avoidance (b = .072, SE = .17, β = .022, $t_{(246)}$ = .43, p = .67). More importantly, as we hypothesized, the interaction was significant (b = –.33, SE = .11, β = –.15, $t_{(246)}$ = 2.97, p = .003). Simple slopes analysis at one standard deviation above and below the mean for uncertainty avoidance showed that, for low uncertainty avoidance participants (–1 SD), power distance beliefs predicted the willingness to use the app (b = .93, SE = .092, β = .803, $t_{(246)}$ = 10.12, p < .001) such that high power distance beliefs led to greater willingness to use the app. However, for high uncertainty avoidance participants, the relationship between power distance beliefs and willingness to use the app was attenuated (b = .54, SE = .082, β = .47, $t_{(246)}$ = 6.62, p < .001) (see Fig. 3).

Finally, we tested the moderated mediation model using PROCESS Model 7 (Hayes, 2013) with power distance beliefs (mean-centered) as the predictor (X), willingness to use the app as the dependent variable (Y), attribution of data ownership as the mediator (M), and uncertainty avoidance (mean-centered) as the moderator (W). Bootstrapping (20,000 resamples) revealed a significant index of moderated mediation (b = –.04, SE = .03, 95% CI (–.103, –.004)]. Specifically, the positive indirect effect of power distance beliefs on willingness to use the FacePlay app through reduced attribution of data ownership to the user (vs. the app) was significant for low uncertainty avoidance participants (–1 SD: b = .10, SE = .04, 95% CI (.04, .18)]. However, this indirect path was weaker for high uncertainty avoidance participants (+1 SD: b = .04, SE = .02, 95% CI (.006, .085)].

DISCUSSION

The results of Study 7 show that uncertainty avoidance moderates the effect of power distance beliefs on willingness to patronize a business after a

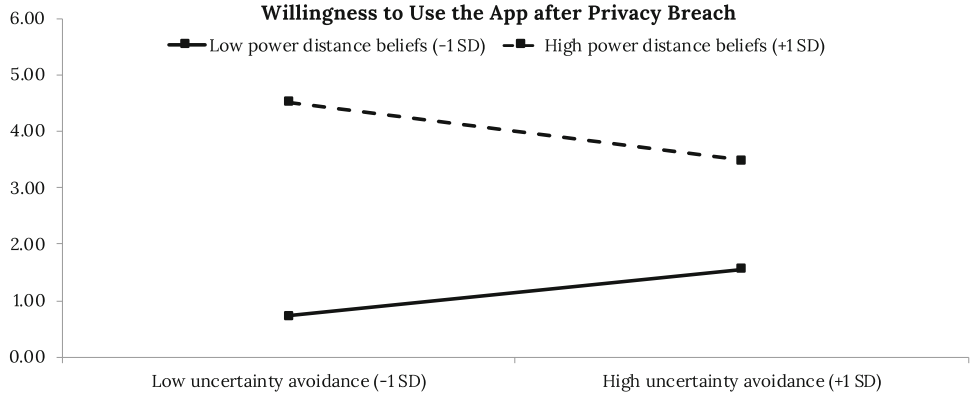

Figure 3 Interaction between power distance beliefs and uncertainty avoidance on willingness to use an app after a data breach in Study 7

data breach. For low uncertainty avoidance participants, power distance beliefs were a significant predictor of willingness to use an app with data breach issues because they attributed low ownership of their data to themselves. For high uncertainty avoidance participants, the link between power distance beliefs and willingness to use the app was attenuated because they attributed greater data ownership to themselves (rather than the app). Although we found support for the hypothesized interaction effect, it is surprising that there was no main effect of uncertainty avoidance on willingness to continue using the app after the data breach. One potential explanation may be that uncertainty avoidance was measured toward the end of the study, and the data breach scenario may have been less vivid in participants' minds by that time.

GENERAL DISCUSSION

In today's data-driven digital world, data breaches are an important issue that international firms must contend with. Across eight studies using archival, correlational, and experimental methods, we find converging evidence that power distance influences people's willingness to continue patronizing a business after a data breach. Study 1 reveals that people in high power distance countries would continue to download an app even after a potential data breach was highlighted in the news. Study 2, conducted with actual victims of data breaches, offers stronger evidence in support of the hypothesis that power distance beliefs shape people's responses to data breaches. Study 3 provides further evidence for the role of power distance at an individual level using the Facebook–Cambridge Analytica data breach. Studies 4 and 5A provide causal evidence and, more importantly, identify an underlying mechanism such that participants in *high power distance* conditions attributed less ownership of data to the individual and more to the organization (Study 4) and the government (Study 5A). In turn, this increased their willingness to continue using the service in question. Studies 5B and 6 offer additional evidence for the underlying mechanism. Finally, Study 7 demonstrates that high uncertainty avoidance attenuates the relationship between power distance beliefs and willingness to continue patronizing a business after a data breach. The effect sizes range from medium (Study 4: $d = .35$) to large (Study 1: irr = 1.02; Study 5A: $d = .87$), indicating that power distance is a strong predictor of variance in countries' and individuals' differential responses to data breaches.

THEORETICAL CONTRIBUTIONS

Although data breaches affect consumers, firms, and countries worldwide, they are an understudied phenomenon in international business. Extant research has studied users' willingness to disclose their data to companies, a question that has become all but moot as sharing data with businesses has become so ubiquitous in current times (Chandler, 2019). Today, it is more important that businesses understand how their users will respond in the event that shared data become compromised. Multinational firms across markets have suffered from data breaches, and such breaches seem almost inevitable. How much a data breach affects a firm's business across different countries is highly dependent on how people in that country respond to the breach. Hence, we contribute to the

international business literature by studying this novel perspective on data breaches.

Our focus on data breaches differentiates the present research from past work in international business, which has mainly focused on privacy in the context of territoriality and governance issues related to data exchange over the Internet (Kobrin, 2001) and data flow constraints across national borders (Samiee, 1984). In addition, prior international business research has studied the role of cultural values in influencing people's privacy concerns (Bellman et al., 2004; Milberg et al., 2000). However, this research has focused on country-level analyses that are silent on the underlying mechanism that may explain the effect of power distance on people's privacy concerns across different markets. To our knowledge, the current research is the first to identify a core cultural value as an antecedent of people's willingness to continue patronizing a business after a data breach, both if they themselves experienced the data breach or knew about the data breach. It thus deepens the understanding of variations in people's responses to data breaches across international markets, and provides more precise insights into the role of power distance and the underlying mechanism of ownership attribution.

Extant international business literature has studied the consequences of power distance at both country (e.g., Dwyer et al., 2005; Qiu, 2014) and organizational (e.g., Lin, Chen, Herman, Wei, & Ma, 2019; Smith & Hume, 2005) levels. We contribute to this literature by identifying two novel consequences of power distance: ownership attributions and divergent responses to data breaches. Our work suggests that power distance is consequential for a broader range of outcomes than previously conceptualized. Further, methodologies and sample selection in prior research prevent a causal understanding of the phenomenon (see discussion of Bellman et al., 2004 and Milberg et al., 2000 above). In this research, we provide converging causal evidence for the role of power distance in determining people's willingness to continue patronizing a business after a data breach. Given the focus of international business research, we developed two different manipulations of power distance: at organizational and national culture levels, respectively. Future work could use these manipulations to provide a causal understanding of other phenomena being studied. In addition, our finding that uncertainty avoidance moderates the effect of power distance contributes to the international business literature on how national cultural values interact to influence substantive outcomes (Kirkman, Lowe, & Gibson, 2006).

The current research also contributes to the attribution-of-ownership literature (Constant et al., 1994). In today's information economy, people's data have become a highly valued market good (Kamleitner & Mitchell, 2018). Given the high value associated with personal data, people's perceptions of who owns the data they share with businesses is a consequential and highly contested topic. We identify power distance beliefs as a novel antecedent of people's ownership attributions, such that people high in power distance beliefs attribute lower data ownership to themselves. This finding is noteworthy, because ownership attributions are nebulous and are multiply determined by the types of data being shared and the specific terms and conditions. We find that a distal predictor – the cultural value of power distance (power distance beliefs) – shapes people's understanding of who owns the data they share with businesses on a day-to-day basis. This finding has important consequences, because believing that shared data are owned by businesses (vs. the user) leads individuals who are high in power distance beliefs to be less bothered by data breaches that affect their information, and thus the data breach does not affect their willingness to continue patronizing the business after a data breach. This evidence provides a nuanced understanding of the significant role that cultural values play in influencing users' daily interactions with businesses across the globe.

MANAGERIAL IMPLICATIONS

Given the deleterious consequences of data breaches for both individuals and firms, prevention of data breaches is arguably the best strategy. Hence, firms, first and foremost, have an ethical responsibility to protect their users' data. However, there is consensus among security experts that, given the extent of personal and business transactions, which are increasingly conducted online, data breaches are inevitable (Apcela, 2018). The present research finds that people's responses to data breaches vary across international markets, and offers insights for international business practitioners into how to manage people's expectations and reduce backlash due to data breaches.

In low power distance countries, people attribute greater ownership of their shared data to themselves, even if they have legally given up their rights to these data. To that end, managers need to

proactively shape people's expectations about data ownership and data sharing, especially in low power distance countries. For example, multinational firms should explicitly clarify the legal terms and conditions of data ownership upfront when people sign up for a service, and ensure that this information is particularly prominent in low power distance markets. Indeed, a pilot study we conducted with US residents showed that clarification of legal ownership rights (which assigns data ownership to the business) led to a significant reduction in blame assigned to the company for a data breach.[13]

Further, users in low power distance countries should continue to hold firms accountable to strengthen their security infrastructure. Empirical research shows that companies only make limited investments in security infrastructure even after experiencing a data breach (Murciano-Goroff, 2019). These users' lower willingness to continue patronizing the business after a data breach may force these firms to strengthen their efforts to protect user privacy in the interest of business.

Due to their willingness to continue patronizing a business after a data breach, those in high power distance countries may be especially vulnerable to repeated data breaches. Users in these countries may be less likely to take legal or other actions against a firm that loses or mishandles their data. Thus, firms might fail to strengthen their privacy infrastructure in high power distance markets. NGOs in high power distance countries might take proactive steps to highlight the need for privacy protections, particularly among local firms, as international firms might have more stringent privacy policies if they also operate in low power distance countries. Hence, policymakers and NGOs must hold firms accountable for managing and protecting users' data, as users in high power distance countries may not be willing to do so themselves. NGOs and policymakers in high power distance countries may also take steps to educate consumers about data ownership. Explicitly clarifying data ownership (as legally relevant) may help attenuate the relationship between power distance beliefs and willingness to continue patronizing businesses after a data breach if legal terms attribute data ownership to the user.

LIMITATIONS AND DIRECTIONS FOR FURTHER RESEARCH

In the present research, we test our main hypothesis that power distance at a national level, and power distance beliefs at an individual level, affect the willingness to continue engaging with businesses after a data breach with actual victims of data breaches. However, there may be variation in how significantly these individuals were affected by the data breach (e.g., whether they were the victim of password theft or an identity threat). This represents a potential limitation that could be addressed by recruiting a sample of victims who experienced a uniform and consequential data breach, such as credit card theft. Further, in this research, we designed manipulations to prime power distance at national and organizational levels, respectively, to investigate this issue from an international perspective. Future research could replicate these studies employing individual-level power distance manipulations used in the literature, such as the reasons listing task (Zhang et al., 2010), along with the relevant manipulation check items. Additionally, in Study 3, we assessed users' willingness to use Facebook less (i.e., post less information), and to delete personal information from Facebook, but not completely delete their Facebook account or uninstall the app from their phone. While the other studies use these measures (e.g., uninstall the app; Study 5B), future research may test this option in the context of Facebook.

Our mediator measure allowed participants to indicate the ownership of data between the individual and the business. However, users may not assign ownership to either themselves or to the business, or may be unsure about who owns the data. To test this idea, we conducted a post test where we asked participants, "When you use an app, where you add your personal information and pictures, according to you, who owns that information?" An overwhelming 96.5% of the participants believed that the data are either owned by the user, the app, or shared by both (see Online Appendix for details). Thus, the current measure can adequately capture 96.5% of users' understanding of data ownership when they upload any information to an app or website. However, future research on the subject can develop a measure that captures users' understanding of data ownership attributions to include those who are unclear or unsure.

Future empirical work might investigate other moderators that attenuate or exacerbate the link between power distance and willingness to continue patronizing a business after a data breach. Our pilot study (see Note 2) shows that, in general, power distance is associated with people's tendency

to view businesses as higher in status. However, specific firm characteristics may affect this link. Depending on the size of their operations, firms may have different statuses across international markets. While a firm may be perceived as higher in the societal hierarchy in one country, the same firm may be perceived as a startup in another. Arguably, users high in power distance countries may not construe a small startup as being high in the social hierarchy, and, consequently, may not perceive reduced ownership of their data when they share these with such an organization. Researchers could examine this directly by manipulating the status of the organization involved in the data breach across countries varying in power distance.

Across our studies, we find that power distance similarly affects people's responses to data breaches that they either experienced themselves (as demonstrated in Studies 2–6) or heard about other users experiencing (as demonstrated in Studies 1 and 7). We find that, even when participants were not directly affected by the data breach themselves, power distance shaped their willingness to continue to use the services of a business whose other users were affected by a data breach. However, future research might directly test whether personal experience moderates the effect of power distance. Possibly, personal experience of a data breach might weaken the effect of power distance on willingness to patronize the business if users acutely experienced the cost of the data breach. Alternatively, learning about a data breach that others suffered might weaken the effect of power distance on willingness to patronize the business if the service that suffered the data breach has low loyalty, or has many alternatives and is easily substitutable.

At a broader level, like most complex phenomena, people's responses to data breaches are multiply determined. In Study 4, we found that the relationship between power distance and willingness to continue using the software after a data breach was fully mediated by ownership attributions. However, in Studies 5A and 7, the effect was partially mediated. Hence, there may likely be other reasons, apart from lower ownership attributions, which may explain the relationship between power distance and their willingness to continue patronizing a business after a data breach (e.g., the extent to which they expect the organization to take remedial action, or expect another breach in the future). Future research can contribute to this body of knowledge by examining these additional potential mediators.

Given the broad ramifications of data breaches on businesses and society, researchers should assess other antecedents (e.g., national socioeconomic, legal factors) that may shape consumers' responses to data breaches across countries. For example, individual countries' economic ideology (Ralston, Holt, Terpstra, & Kai-Cheng, 1997) may influence the degree to which they hold firms accountable for data breaches and their desire to reduce their business transactions with them. People in countries with free markets may believe that it is the users' choice to share data, and that any repercussions of this choice should be borne by the user. Further, other cultural values may affect users' responses to data breaches. For example, cultural tightness–looseness may be relevant (e.g., Madan, Basu, Ng, & Ching Lim, 2018). Tight cultures have strong social norms and demand adherence, while loose cultures have weak social norms and a high tolerance for non-conforming behavior (Gelfand et al., 2011). It is possible that, in tighter cultures, people might be more upset about data breaches as companies failed to follow the norm of protecting users' data. It would be interesting if future research could test this to provide country-specific insights.

More importantly, individuals in high power distance countries need to understand the downsides of data breaches and hold firms accountable for keeping their data safe. Future research efforts could investigate interventions to increase such individuals' willingness to protect their data and reduce their engagement with organizations after data breaches. One potential reason people may continue to engage with businesses after a data breach is because they perceive a lack of choice or available alternatives. Educating people about the alternatives or choices available to them for commonly used services might reduce the exit barriers in case of a data breach.

ACKNOWLEDGEMENTS

This research was supported by a Security, Privacy, and Trust Pillar Grant awarded by Pamplin College of Business to Shilpa Madan and a Nanyang Assistant Professorship grant awarded by Nanyang Technological University to Krishna Savani. We would like to thank Andrea Low, Tara Hackett, Dayana Bulchand, and Sylvia Chin for invaluable assistance with this research. We would also like to thank the participants

at the Association for Consumer Research 2019 conference for their feedback.

NOTES

[1]We created an aggregate score assessing the prevalence of country-level privacy regulations using data from the UNCTAD (2020), which was based on each country's laws related to consumer protection, privacy, electronic transactions, and cybercrime. As expected, we found a significant negative correlation (r = -.33, p = .0026), such that high power distance was associated with fewer privacy regulations at the country level.

[2]We conducted a pilot study to verify our key assumption that users with high power distance beliefs are more likely to view businesses as authority figures in society. One hundred US participants recruited on CloudResearch completed the study. Participants responded to the power distance beliefs scale (e.g., "People in higher positions should make most decisions without consulting people in lower positions"; α = .84; Yoo et al., 2011) and six items measuring their perceived authority of businesses in society (adapted from Rigby, 1982, 1987; e.g., "Businesses are authority figures in our society," "It is difficult to challenge the authority of businesses in our society"; α = .73), all on 7-point scales ranging from completely disagree to completely agree. Regressing participants' perceived authority of businesses in society on their power distance beliefs revealed a significant effect of power distance beliefs (b = .32, SE = .078, β = .38, $t_{(98)}$ = 4.12, $p < .001$).

[3]We conducted a pilot test to understand users' perception of who is to be blamed for a data breach in general. That is, we assessed whether users believe that businesses are "doing their best" to protect their data from harm and thus blame businesses less. We recruited 100 US participants on CloudResearch™ and told them that their data on a social media platform/a hotel/and a financial services firm had been compromised in a data breach. We asked: "Do you think that the social media platform/hotel/financial services firm failed to adequately protect your data?" and "Do you think that the social media platform/hotel/financial services firm could have done more to protect your data from harm?" We found that, overwhelmingly, users believe that companies can do more to protect their data ($M_{\text{socialmedia}}$ = 6.035, M_{hotel} = 5.93, $M_{\text{financialservices}}$ = 5.95, respectively, on a 7-point scale, all significantly greater than the scale midpoint of 4). This finding indicates that users tend to blame businesses for data breaches in general and believe that businesses have not done enough to protect users' data.

[4]According to Hofstede (1980, 2001), residents of countries high in uncertainty avoidance have a low tolerance for ambiguity in day-to-day situations and tend to avoid risks. On the other hand, desire for control refers to the need to have agent-ends control over one's environment and surroundings (Burger & Cooper, 1979; Leotti, Iyengar, & Ochsner, 2010; Skinner, 1996). Importantly, people may or may not be uncertainty avoidant in domains in which they have no control (e.g., some people might be bothered about unpredictable weather whereas others are not bothered, even though no one has any control over the weather). Hence, conceptually, uncertainty avoidance versus desire for control are distinct constructs, and they may yield different predictions in the context of privacy. For example, an individual high in uncertainty avoidance may not download a less-known app to avoid any associated risks. However, an individual high in desire for control may download the app but actively restrict its access privileges (i.e., not letting the app access contacts, location, and other personal information) in order to regulate the app's ability to cause any untoward issues.

[5]The pattern of results remains unchanged if we include the responses that did not submit the completion code.

[6]The effect was significant both for non-English speaking countries (b = .011, SE = .0031, z = 3.62; $p < .001$) and for English-speaking countries (b = .026, SE = .0056, z = 4.64; $p < .001$).

[7]We undertook extensive testing of this measure. Please see Online Appendix for details.

[8]We report the analysis with all participants in the manuscript. We had pre-registered to exclude participants who self-reported that they took a break during the study. The results with this exclusion are consistent with these results and with the pre-registered analysis plan. The Online Appendix provides the complete analysis.

[9]This is a fictitious name.

[10]One participant did not respond to the mediator measure.

[11]A power analysis using the following inputs (t test: means: differences between two independent means, tails: two, effect size (d, from Study 5A)

= 1.025, α = .05, power = 99%, allocation ratio N2/N1 = 1) yielded a sample size of 72. Keeping with the current norms, we rounded this to n = 100.

[12]One participant did not respond to the manipulation check.

[13]A pilot study (n = 196 US participants) found that clarification of legal ownership rights (that attributed ownership to the business) led to significant reduction in blame assigned to the company for the data breach (M = 4.91, SD = 2.23 vs. M = 6.49, SD = .98, $t(194)$ = 6.43, $p < .0001$).

REFERENCES

Ablon, L., Heaton, P., Lavery D. C., & Romanosky S. 2016. *Consumer attitudes toward data breach notifications and loss of personal information*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR1187.html.

Acquisti, A., Friedman, A., & Telang, R. 2006. Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94. https://aisel.aisnet.org/icis2006/94.

Akpan, N. 2019. Is FaceApp a security risk? 3 privacy concerns you should take seriously. *PBS NewsHour*. https://www.pbs.org/newshour/science/is-faceapp-a-security-risk-3-privacy-concerns-you-should-take-seriously (Accessed 23 September 2020).

Anant, V., Donchak, L., Kaplan, J., & Soller, H. 2020. The consumer-data opportunity and the privacy imperative. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative# (Accessed 17 March 2021).

Apcela. 2018. *Data breach statistics: By source, industry, country & size.* https://www.apcela.com/blog/data-breach-statistics/ (Accessed 23 September 2020).

Baharudin, H. 2021. Police's ability to use TraceTogether data raises questions on trust: Experts. *The Straits Times*. https://www.straitstimes.com/singapore/politics/polices-ability-to-use-tracetogether-data-raises-questions-on-trust-experts (Accessed 15 February 2021).

Bansal, G., & Zahedi, F. M. 2015. Trust violation and repair: The information privacy perspective. *Decision Support Systems,* 71(March): 62–77.

Bauer, C., Korunovska, J., & Spiekermann, S. 2012. On the value of information-what Facebook users are willing to pay. *ECIS 2012 Proceedings*. Barcelona, Spain: AIS.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society,* 20(5): 313–324.

Bocchini, B. 2019. Brazil consumer rights agency notifies FaceApp, Apple, Google. Agencia Brasil. https://agenciabrasil.ebc.com.br/en/geral/noticia/2019-07/brazil-consumer-rights-agency-notifies-faceapp-apple-google (Accessed 21 September 2020).

Burger, J. M., & Cooper, H. M. 1979. The desirability of control. *Motivation and Emotion,* 3(4): 381–393.

Cameron, A. C., & Trivedi, P. K. 2009. *Microeconometrics using Stata* (Vol. 5). College Station, TX: Stata Press.

Chandler, S. 2019. We're giving away more personal data than ever, despite growing risks. *VentureBeat*. https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/ (Accessed February 17, 2021).

Chatterjee, S., Gao, X., Sarkar, S., & Uzmanoglu, C. 2019. Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research,* 101(August): 183–193.

Chen, H. S., & Jai, T. M. C. 2019. Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management,* 82(September): 326–334.

Constant, D., Kiesler, S., & Sproull, L. 1994. What's mine is ours, or is it? A study of attitudes about information sharing. *Information Systems Research,* 5(4): 400–421.

Crist, R. 2019. FaceApp was a test. We didn't pass. *CNET*. https://www.cnet.com/news/faceapp-privacy-concerns/ (Accessed 21 September 2020).

Culnan, M. J., & Armstrong, P. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science,* 10(1): 104–115.

Culnan, M. J., & Bies, R. J. 2003. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues,* 59(2): 323–342.

Culnan, M. J., & Williams, C. C. 2009. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly,* 33: 673–687.

Davis, J. F. 1997. Property rights to consumer information: A proposed policy framework for direct marketing. *Journal of Direct Marketing,* 11(3): 32–43.

Dawar, N., Parker, P. M., & Price, L. J. 1996. A cross-cultural study of interpersonal information exchange. *Journal of International Business Studies,* 27(3): 497–516.

Dennis, S. A., Goodson, B. M., & Pearson, C. 2019. Online worker fraud and evolving threats to the integrity of MTurk data: A discussion of virtual private servers and the limitations of IP-based screening procedures. *Behavioral Research in Accounting,* 32(1): 119–134.

Demmers, J., Weihrauch, A. N., Mattison Thompson, F. H., & Your data is (not) my data. 2021. The role of social value orientation in sharing data about others. *Journal of Consumer Psychology*.. https://doi.org/10.1002/jcpy.1255.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. 2006. Privacy calculus model in e-commerce: A study of Italy and the United States. *European Journal of Information Systems,* 15(4): 389–402.

Dinev, T., & Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research,* 17(1): 61–80.

Dwyer, S., Mesak, H., & Hsu, M. 2005. An exploratory examination of the influence of national culture on cross-national product diffusion. *Journal of International Marketing,* 13(2): 1–27.

Ford, J. B. 2017. Amazon's Mechanical Turk: A comment. *Journal of Advertising,* 46(1): 156–158.

Fowler, G. A. 2019. You downloaded FaceApp. Here's what you've just done to your privacy. *The Washington Post*. https://www.washingtonpost.com/technology/2019/07/17/you-downloaded-faceapp-heres-what-youve-just-done-your-privacy/ (Accessed 23 September 2020).

Gabisch, J. A., & Milne, G. R. 2014. The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing,* 31(1): 136.

Gardner, W., Mulvey, E. P., & Shaw, E. C. 1995. Regression analyses of counts and rates: Poisson, overdispersed Poisson, and negative binomial models. *Psychological Bulletin,* 118(3): 392–404.

General Data Protection Regulation (GDPR) 2018. Intersoft Consulting § Article 4 – Definitions. https://gdpr-info.eu/art-4-gdpr/ (Accessed 17 March 2021).

Grothaus, M. 2019. Viral app hit FaceApp, which makes users look old, has privacy concerns. *Fast Company.* https://www.fastcompany.com/90377895/viral-app-hit-faceapp-which-makes-users-look-old-has-privacy-concerns (Accessed 17 March 2021).
Hartl, B., Kamleitner, B., & Holub, S. 2020. Take me on a ride: The role of environmentalist identity for carpooling. *Psychology & Marketing,* 37(5): 663–676.
Hayes, A. F. 2013. *Mediation, moderation, and conditional process analysis: A regression-based approach*. New York: Guilford.
Hofstede, G. 1980. Culture and organizations. *International Studies of Management & Organization,* 10(4): 15–41.
Hofstede, G. 2001. *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Thousand Oaks, CA: Sage Publications.
Hui, M. K., Au, K., & Fock, H. 2004. Empowerment effects across cultures. *Journal of International Business Studies,* 35(1): 46–60.
Ikeda, S. (2020). 75% of APAC consumers feel that personal data security is beyond their control; 96% prioritize convenience over security. *CPO Magazine.* https://www.cpomagazine.com/data-protection/75-of-apac-consumers-feel-that-personal-data-security-is-beyond-their-control-96-prioritize-convenience-over-security/ (Accessed 6 September 2021).
Janakiraman, R., Lim, J. H., & Rishika, R. 2018. The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing,* 82(2): 85–105.
Jarvenpaa, S. L., & Staples, D. S. 2001. Exploring perceptions of organizational ownership of information and expertise. *Journal of Management Information Systems,* 18(1): 151–183.
Jiang, Y., Colakoglu, S., Lepak, D. P., Blasi, J. R., & Kruse, D. L. 2015. Involvement work systems and operational effectiveness: Exploring the moderating effect of national power distance. *Journal of International Business Studies,* 46(3): 332–354.
Joinson, A. N., & Paine, C. B. 2007. Self-disclosure, privacy and the internet. In A. Joinson, K. McKenna, T. Postmes, & U. D. Reips (Eds.), *Oxford handbook of internet psychology*: 237–252. Oxford: Oxford University Press.
Kamleitner, B., & Mitchell, V. W. 2018. Can consumers experience ownership for their personal data? From issues of scope and invisibility to agents handling our digital blueprints. In J. Peck, & S. Shu (Eds.), *Psychological ownership and consumer behavior*: 91–118. Springer.
Kamleitner, B., & Mitchell, V. W. 2019. Your data is my data: a framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing,* 38(4): 433–450.
Kamleitner, B., Süssenbach, S., Thürridl, C., & Ruzeviciute, R. 2016. This brand is mine: Brand psychological ownership as a distinct construct and powerful driver of consumer behavior. *ACR North American Advances,* 44: 740–740.
Khatri, N. 2009. Consequences of power distance orientation in organisations. *Vision: the Journal of Business Perspective,* 13(1): 1–9.
Kirkman, B. L., Lowe, K. B., & Gibson, C. B. 2006. A quarter century of culture's consequences: A review of empirical research incorporating Hofstede's cultural values framework. *Journal of International Business Studies,* 37(3): 285–320.
Kobrin, S. J. 2001. Territoriality and the governance of Cyberspace. *Journal of International Business Studies,* 32(4): 687–704.
Königs, P. 2022. Government Surveillance, Privacy, and Legitimacy. *Philosophy & Technology,* 35(1): 1–22.
Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. 2009. Privacy concerns and identity in online social networks. *Identity in the Information Society,* 2(1): 39–63.
Leotti, L. A., Iyengar, S. S., & Ochsner, K. N. 2010. Born to choose: The origins and value of the need for control. *Trends in Cognitive Sciences,* 14(10): 457–463.
Lian, H., Ferris, D. L., & Brown, D. J. 2012. Does power distance exacerbate or mitigate the effects of abusive supervision? It depends on the outcome. *Journal of Applied Psychology,* 97(1): 107.
Lin, X., Chen, Z. X., Herman, H. M., Wei, W., & Ma, C. 2019. Why and when employees like to speak up more under humble leaders? The roles of personal sense of power and power distance. *Journal of Business Ethics,* 158(4): 937–950.
Madan, S., Basu, S., Ng, S., & Ching Lim, E. A. 2018. Impact of culture on the pursuit of beauty: Evidence from five countries. *Journal of International Marketing,* 26(4): 54–68.
Magnusson, P., Peterson, R., & Westjohn, S. A. 2014. The influence of national cultural values on the use of rewards alignment to improve sales collaboration. *International Marketing Review,* 31(1): 30–50.
Malhotra, A., & Malhotra, C. K. 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research,* 14(1): 44–59.
Maronick, T. J. 2014. Do consumers read terms of service agreements when installing software? A two-study empirical analysis. *International Journal of Business and Social Research,* 4(6): 137–145.
Martin, K. D., Borah, A., & Palmatier, R. W. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing,* 81(1): 36–58.
Martin, K., & Murphy, P. E. 2017. The role of data privacy in marketing. *Journal of the Academy of Marketing Science,* 45(2): 135–155.
Menard, P., Warkentin, M., & Lowry, P. B. 2018. The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security,* 75: 147–166.
Merrill, J., & Goldhill, O. 2020. Cambridge Analytica used these 5 political ads to target voters. https://qz.com/1782348/cambridge-analytica-used-these-5-political-ads-to-target-voters/ (Accessed 23 September 2020).
Milberg, S. J., Smith, H. J., & Burke, S. J. 2000. Information privacy: Corporate management and national regulation. *Organization Science,* 11(1): 35–57.
Möller, J., & Eisend, M. 2010. A global investigation into the cultural and individual antecedents of banner advertising effectiveness. *Journal of International Marketing,* 18(2): 80–98.
Morewedge, C. K., Monga, A., Palmatier, R. W., Shu, S. B., & Small, D. A. 2021. Evolution of consumption: A psychological ownership framework. *Journal of Marketing,* 85(1): 196–218.
Muncaster, P. 2019. Global breach costs set to top $5 trillion by 2024. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/breach-costs-trillion/ (Accessed 21 September 2020).
Murciano-Goroff, R. 2019. Do Data Breach Disclosure Laws Increase Firms' Investment in Securing Their Digital Infrastructure? In *Workshop on the Economics of Information Security*. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_33.pdf (Accessed 15 June 2021).
Olavario, D. 2019. FaceApp: Are security concerns around viral app founded?: *#TheCube*. https://www.euronews.com/2019/07/17/faceapp-are-security-concerns-around-viral-app-founded-thecube (Accessed 21 September 2020).
Osborne, C. 2020. The biggest hacks, data breaches of 2020. *ZD Net*. https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/ (Accessed 17 March 2021).
Oyserman, D. 2006. High power, low power, and equality: Culture beyond individualism and collectivism. *Journal of Consumer Psychology,* 16(4): 352–356.
PCIPal. 2020. Online shoppers more concerned about deliveries than personal security, according to PCI Pal Survey. https://www.pcipal.com/en-us/knowledge-centre/resource/online-shoppers-more-concerned-about-deliveries-than-personal-security-according-to-pci-pal-survey/ (Accessed 18 March 2021).
Peck, J., Kirk, C. P., Luangrath, A. W., & Shu, S. B. 2020. Caring for the commons: Using psychological ownership to enhance stewardship behavior for public goods. *Journal of Marketing,* 85(2): 33–49.

Pierce, J. L., Kostova, T., & Dirks, K. T. 2003. The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology,* 7(1): 84–107.
PwC. 2018. Consumer intelligence series: Protect.me. https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html (accessed 18 March 2021).
Qiu, T. 2014. Product diversification and market value of large international firms: A macroenvironmental perspective. *Journal of International Marketing,* 22(4): 86–107.
Ralston, D. A., Holt, D. H., Terpstra, R. H., & Kai-Cheng, Y. 1997. The impact of natural culture and economic ideology on managerial work values: a study of the United States, Russia, Japan, and China. *Journal of International Business Studies,* 28(1): 177–207.
Richardson, V. J., Smith, R. E., & Watson, M. W. 2019. Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems,* 33(3): 227–265.
Rigby, K. 1982. A concise scale for the assessment of attitudes towards institutional authority. *Australian Journal of Psychology,* 34(2): 195–204.
Rigby, K. 1987. An authority behavior inventory. *Journal of Personality Assessment,* 51(4): 615–625.
Risk Based Security. 2021. New research: No. of records Exposed Increased 141% in 2020. https://www.riskbasedsecurity.com/2021/01/21/new-research-no-of-records-exposed-increased-141-in-2020/ (accessed 17 March 2021).
Samiee, S. 1984. Transnational data flow constraints: A new challenge for multinational corporations. *Journal of International Business Studies,* 15(1): 141–150.
Sivakumar, K., & Nakata, C. 2001. The stampede toward Hofstede's framework: Avoiding the sample design pit in cross-cultural research. *Journal of International Business Studies,* 32(3): 555–574.
Skinner, E. A. 1996. A guide to constructs of control. *Journal of Personality and Social Psychology,* 71(3): 549.
Smith, A., & Hume, E. 2005. Linking culture and ethics: A comparison of accountants' ethical belief systems in the individualism/collectivism and power distance contexts. *Journal of Business Ethics,* 62(3): 209–220.
Spiekermann, S., & Korunovska, J. 2017. Towards a value theory for personal data. *Journal of Information Technology,* 32(1): 62–84.
Spiekermann, S., Korunovska, J., & Bauer, C. 2012. Psychology of ownership and asset defense: Why people value their personal information beyond privacy. *Available at SSRN 2148886*.
TraceTogether (2021). TraceTogether, Safer Together. https://www.tracetogether.gov.sg/ (accessed 30 September 2021).
United Nations Conference on Trade and Development (UNCTAD). 2020. Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
Winterich, K. P., & Zhang, Y. 2014. Accepting inequality deters responsibility: How power distance decreases charitable behavior. *Journal of Consumer Research,* 41(2): 274–293.
Wong, J. C. 2019. The Cambridge Analytica scandal changed the world. But it didn't change Facebook. *The Guardian*. https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (accessed 21 September 2020).
Xu, H., Dinev, T., Smith, J., & Hart, P. 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems,* 12(12): 1.
Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. 2009. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems,* 26(3): 135–174.
Yaveroglu, I. S., & Donthu, N. 2002. Cultural influences on the diffusion of new products. *Journal of International Consumer Marketing,* 14(4): 49–63.
Yoo, B., Donthu, N., & Lenartowicz, T. 2011. Measuring Hofstede's five dimensions of cultural values at the individual level: Development and validation of CVSCALE. *Journal of International Consumer Marketing,* 23(3–4): 193–210.
Yu, E. 2020. APAC consumers believe onus on businesses, governments to safeguard their data. *ZD Net.* https://www.zdnet.com/article/apac-consumers-believe-onus-on-businesses-governments-to-safeguard-their-data/ (Accessed 17 March 2021)

ABOUT THE AUTHORS

Shilpa Madan is Assistant Professor of Marketing at Virginia Tech. She aspires to use consumer behavior research to help people live better, more fulfilling, and more sustainable lives. She is keenly interested in consumers' naïve (lay) theories about the world and cultural differences to enhance individual and societal well-being. Her work has implications for public policy, sustainable living, and consumer welfare.

Krishna Savani is a Professor of Management at the Hong Kong Polytechnic University. This work was conducted when he was the Provost's Chair in Business at Nanyang Technological University. He conducts research on culture, decision-making, diversity, and morality, and has an emerging program of research on using machine learning to generate hypotheses in the social and organizational sciences.

Constantine S. Katsikeas is the Arnold Ziff Research Chair and Professor of Marketing and International Management, and the Founder and Director of the Global and Strategic Marketing Research Center at the University of Leeds. His interests are global marketing and exporting, sales management, cross-border relationships, and strategic alliances. He is an AIB Fellow and currently serves as Editor for *Journal of International Business Studies* and Area Editor for *Journal of the Academy of Marketing Science*.

Accepted by Keith Brouthers, Guest Editor, 22 February 2022. This article has been with the authors for four revisions.