Current Psychology
https://doi.org/10.1007/s12144-022-02753-4

Public support for counterterrorism efforts using probabilistic computing technologies to decipher terrorist communication on the internet

Torsten Reimer[1] · **Nathanael Johnson**[1]

Accepted: 19 January 2022

Abstract
Advancements in big data analytics offer new avenues for the analysis and deciphering of suspicious activities on the internet. One promising new technology to increase the identification of terrorism threats is based on probabilistic computing. The technology promises to provide more efficient problem solutions in encryption and cybersecurity. Probabilistic computing technologies use large amounts of data, though, which raises potential privacy concerns. A study ($N = 1{,}023$) was conducted to survey public support for using probabilistic computing technologies to increase counterterrorism efforts. Overall, strong support was found for the use of publicly available personal information (e.g., personal websites). Regarding private personal information (e.g., online conversations), respondents perceived it to be more appropriate to use information from out-group members (non-American citizens) than from in-group members (American citizens). In line with a social-identity account, this form of in-group favoritism was strongest among respondents displaying a combination of strong national identities and strong privacy concerns.

Keywords Counterterrorism · Social identity theory · Ingroup favoritism · Privacy concerns

On Halloween Day of 2017, Sayfullo Saipov careened a pickup truck along a biking path by the Hudson river in New York City, striking pedestrians and finally crashing into a school bus back on the road. After the crash, he left his vehicle and ran around the highway with a pellet gun before being stopped by the police (Mueller et al., 2017). The attack killed eight people, injured eleven, and struck fear and panic into a countless number more. Government agencies determined that it was a terrorist attack that was planned in advance. Typically, the planning of terrorist attacks begins with communication among members of terrorist organizations (Schuurman et al., 2018). Terrorist communication is known to include hidden, encrypted, or disappearing messages online through venues like email, online gaming, texting, and chat rooms (Gill et al., 2017), which all contain very large amounts of information that is usually kept secret, as leaked information can prevent their plans. Due to the unavailability of timely and accurate information, it is difficult and challenging to predict and prevent terrorist threats (Drozdova & Samoilov, 2010).

New technologies, including probabilistic computing technologies, promise to considerably raise the standard on the amount of information that can be processed concurrently and, thus, are increasing the potential to identify suspicious communication on the internet (Camsari et al., 2017; Behin-Aein et al., 2016). While standard computers use stable magnets to hold their bits as stable ones or zeros, probabilistic computers replace the stable magnets with unstable magnets to allow their bits, known as p-bits, to fluctuate back and forth between ones and zeros (Camsari et al., 2020). This type of computing makes p-bits suitable for solving problems of probability, machine learning, and problems that have recently been addressed by quantum computing (Camsari et al., 2020). Advancements and applications of probabilistic computing technologies in deciphering and cybersecurity promise to increase the probability of detecting attacks like the described October 31st attack in advance and increase the chances for government agencies to thwart attempts and save lives.

✉ Torsten Reimer
treimer@purdue.edu

[1] Communication and Cognition Lab, Brian Lamb School of Communication, Purdue University, 100 North University Street, West Lafayette, IN 47907, USA

Published online: 02 March 2022

However, probabilistic and quantum computing technologies would use large amounts of data including personal information of many individuals. As a consequence, the adoption of these new technologies to decipher and identify terrorist threats on the internet raises potential privacy concerns. The use of large amounts of information is not unique to probabilistic computing, nor is big data's only use counterterrorism. Sun and Huo (2019) reviewed the most common research applications that use big data analytics, which included data mining, machine learning, data science and systems, artificial intelligence, and distributed computing and systems as the top five. As illustrated by the burgeoning research in privacy-preserving data mining (Agrawal & Srikant, 2000), these areas that use big data retain similar concerns of the trade-off between privacy and security as the use of probabilistic computing for counterterrorism efforts. Research has shown that other technologies such as surveillance equipment are acknowledged to have potential to bring with it a sense of security and safety, but they also are thought to bring a risk of privacy invasion (van Heek et al., 2014).

Our study was motivated by the development of probabilistic computing technologies. We set out to survey public support for the potential usage of personal information by government agencies using p-bits technologies. The conducted study, thus, framed the privacy and security discussion around probabilistic computing for the participants. Using a social-identity framework (Tajfel & Turner, 1986), we aimed to test a set of hypotheses that describe the independent and combined effects of four relevant factors on the public acceptance of the use of personal data to prevent terrorist attacks: Whether the processed personal information is private (e.g., conversations over the internet) or publicly available (e.g., personal websites); the general privacy concerns of respondents; the strength of respondents' national identity; and whether the processed personal information would be taken from in-group members (US citizens) or out-group members (non-US citizens). To explore if the proposed effects generalize across several situations, the proximity of potential victims of a terrorist attack and the location were varied following a procedure that was developed by Hinsz and Betts (2014). In addition, participants' age, economic status, education, and political orientation were measured.

We first introduce research on privacy and security concerns and advance the hypothesis that the acceptance of the use of personal information to identify suspicious internet activities depends on whether personal information is publicly available or not and on respondents' general privacy concerns. Next, we describe research that suggests that the support for the usage of personal information will differ depending on whether personal information is taken from in-group members (US citizens) or out-group members (non-US citizens). In a third step, we advance the hypothesis that in-group favoritism for private information (more support for the use of personal information from out-group than in-group members) is particularly pronounced among respondents who have strong national identities and hold high privacy concerns. Finally, we describe a study that tested the introduced hypotheses and conclude with a general discussion and future directions.

Privacy Concerns for Personal Information

As with other judgments and perceptions, research suggests that privacy concerns are a function of the situation and the person (situation x person; see Lewin, 1935): Most people have greater privacy concerns in certain situations (e.g., surveillance of private spaces) than in others (e.g., surveillance of public spaces; see van Heek et al., 2014), and individuals consistently vary in how much privacy concerns they have in general (e.g., see Crow et al., 2017; Newell, 2016). Moreover, as in other *situation x person* approaches (Lewin, 1935), these two dimensions can interact, as individuals' differences in privacy concerns vary across situations. For example, concerns for the use of surveillance technology in private spaces may be particularly concerning for people with high general privacy concerns and low trust in the organizations using the technology (see Pavone & Esposti, 2010).

Regarding differences across situations, studies on information sharing (Hayes et al., 2021; Phelps et al., 2001), scraping of information for marketing (Swani et al., 2021), the disclosure of sensitive information (Atienza et al., 2015; Dhagarra et al., 2020), and the acceptance of surveillance and security technologies (Larson & Ferrin, 2021; Pavone & Esposti, 2010) suggest that people's privacy concerns regarding their personal information vary across different types of information and depend on the purpose for which personal information is used and who is using it.

Privacy concerns are generally stronger for more sensitive information, which is information that can cause damage to the owner of the information when lost or stolen and used in an unintended or fraudulent way. For example, health information that is relatively routine, like blood pressure, is considered less risky to send over insecure channels than more sensitive information like a cancer diagnosis (Atienza et al., 2015), though these concerns can be alleviated for some people by government-enforced privacy policies (Hwang & Lin, 2020). People are generally willing to give simple demographic information or basic opinions and behaviors, but they are more resistant to allow others access to more sensitive information, like health and financial information (Dhagarra et al., 2020; Safaeimanesh et al., 2021).

The current study focuses on the use of probabilistic computing technologies by US government agencies. As publicly available websites and social media typically provide less

sensitive information and are made accessible to a broad audience by owners, we expected to find more support for the use of personal information that is publicly available than for the use of personal information that is only privately shared in online conversations and emails.

Several studies on surveillance-oriented security technology, like cameras, suggest that security technology is seen as more appropriate in public areas than in private ones (e.g., Pavone & Esposti, 2010; van Heek et al., 2014). Van Heek et al. (2014) observed that security and safety were preferred over privacy in the context of already-public locations, but privacy was preferred in more private locations. The appropriateness of the use of personal data also depends on the perceived threat and severity of crimes. The threat of more serious crimes being repeated, such as from serial rapists, pedophiles, or terrorists, was seen as a just cause for increased surveillance, even in a more private sphere (Pavone & Esposti, 2010). Based on these considerations, we expected differences in the support of using public and private personal information to decipher terrorist communication on the internet.

Hypothesis 1: Respondents perceive it as more appropriate to use large amounts of publicly available personal information (e.g., personal websites) than to use private personal information (e.g., online conversations) to identify terrorist threats (*personal information)*.

Privacy concerns vary across different situations and types of information. As with other psychological constructs, there are also stable individual differences. For example, in a study on the use of police body cameras, Crow et al. (2017) observed that most people believed that the benefits of body cameras outweighed the risks and that they did not represent an invasion of privacy. However, those who were concerned about privacy invasion were less supportive of their usage. This can also include experts such as police officers who, at times, support more selective access to body camera footage because of privacy concerns (Newell, 2016). Similarly, in a large survey examining individual differences in online privacy concerns, Kim et al. (2018) found that females tended to be more concerned about online privacy than males and that wealthier and more educated people were more concerned than their counterparts.

We expected that respondents who have high general privacy and security concerns regarding their activities on the internet would be less supportive of the use of large amounts of personal information to decipher terrorist threats compared to respondents who have fewer general concerns. Respondents with high privacy concerns were expected to be particularly concerned about the usage of private personal information.

Hypothesis 2: (a) Compared to respondents with low privacy concerns, respondents who have high privacy concerns find it less appropriate to use personal information for counterterrorism purposes (*privacy concerns*). (b) This difference is larger for private than for publicly available personal information (*privacy concerns x personal information*).

In-Group Favoritism in the Use of Personal Information

When it comes to the use of large amounts of personal information and the prevention of crimes and terrorist threats, there is a tension between different goals; the goals are to both be safe and protected from attacks and to also have control over personal information and prevent the use of fraudulent usage of one's own personal information. We aimed to test for a social-identity account of privacy concerns. Specifically, we sought to find out if concerns regarding the usage of personal information for counter-terrorism efforts depend on whether personal information is taken from US citizens (in-group) or non-US citizens (out-group).

Hinsz and Betts (2014) conducted two studies in which they asked their participants to express their support for counterterrorism activities following a hypothetical terrorist attack. Specifically, Hinsz and Betts tested the hypothesis that respondents reveal in-group favoritism by supporting counterterrorism efforts more when American citizens are the victims of an attack than non-citizens and when the attack occurs in the US and not outside the country. The authors reasoned that in-group favoritism would be stronger among those respondents who display strong national identities and would be independent of negative attitudes toward out-groups (Allport, 1954; Brewer, 1999). In-group favoritism refers to the observation that in-group members are treated more favorably than out-group members. It occurs when group membership is salient and when members of one's own group are affected. It does not require that one is personally familiar with these members (Brewer, 1999).

Hinsz and Betts (2014) did not find support for the proposed hypotheses in their studies. We aimed to build on and extend their approach by exploring if respondents reveal in-group favoritism when asked if they would support the usage of personal information as a measure of a counter-attack. While Hinsz and Betts (2014) varied where an attack occurred, the potential costs and risks of a counter-attack were not differentiated as costs that occur for in-group or out-group members. Building on their approach, we aimed to differentiate between the support of using personal information from in-group versus out-group members. We expected that respondents would be more supportive of the idea of using personal information from out-group members

(non-US citizens) than from in-group members (US citizens), thus, reducing privacy risks for their own group. Moreover, we also expected that the salience of one's own group would trigger feelings of commitment to one's own group and in-group favoritism in particular in situations, in which respondents have high privacy concerns—that is, for personal information that is private and among respondents who have high general privacy concerns.

> ***Hypothesis 3:*** (a) To prevent a counterterrorism attack, respondents perceive it as more appropriate to use information from out-group members (non-US citizens) than from in-group members (US citizens) and display in-group favoritism (*citizenship of source*). (b) In-group favoritism is stronger for private than for public personal information (*citizenship x personal information*). (c) In-group favoritism for private information is particularly pronounced for respondents who have strong privacy concerns (*citizenship* x *personal information x privacy concerns*).

Typically, in-group favoritism is particularly strong among individuals who strongly identify with their group. In the case of counterterrorism efforts, previous research suggests that respondents who strongly identify with their nation are more in favor of counterterrorism efforts than respondents who display weaker national identity. In Hinsz and Betts' study (2014), nationalism strongly correlated with general and situation-specific support of counterterrorism measures. In a similar vein, Williamson (2019) observed in a survey study that Australians who identified more strongly with their country more strongly supported counterterrorism measures. Accordingly, we expected that respondents who display strong national identification would be more supportive of the use of personal information to identify terrorist threats than respondents who display weaker national identification and that national identity would interact with respondents' privacy concerns, the type of information (private vs public), and the citizenship of the source of information (US citizens vs non-US citizens).

> ***Hypothesis 4***: (a) Respondents who display a strong national identity perceive it as more appropriate to use personal information to identify and prevent terrorist attacks than respondents displaying a weak national identity (*national identity*). (b) In-group favoritism for private information is particularly pronounced for respondents who have strong privacy concerns and national identities (*citizenship* x *privacy concerns x personal information x national identity*).

The scope of the hypotheses and their intended applications (Balzer et al., 1989) refer to a situation in which potential terrorist threats clearly have a connection to a country and in which the access to personal information is intended to be used by one's own government. However, the terrorist attack does not necessarily have to be conducted in one's own country, nor are the victims necessarily citizens of one's own country. We pursued the hypotheses by analyzing respondents' reactions to a scenario description of a terrorist attack. Participants read about an attack that targeted either an in-group (US citizens) or an out-group (non-US citizens). They then responded to questions about support for counterterrorism efforts. To test if the proposed effects are limited to certain threats, the proximity of the victim and location was varied (see Hinsz & Betts, 2014). However, in all cases, the attacks had a clear relationship to the US where the study was conducted. As the main dependent variable, respondents were asked how appropriate it would be to use probabilistic computing technologies to collect and process large amounts of personal information in order to prevent attacks similar to the one described in the article.

Method

To test the proposed hypotheses, we conducted a study using Qualtrics and utilized Amazon's Mechanical Turk (MTurk) to recruit and compensate participants. We aimed to follow best practices that have been described in the scientific literature for the recruitment (e.g., approval rates), payment (e.g., ethical compensation), and collection of data (e.g., attention check) to maximize the quality of the collected data.

Amazon's Mechanical Turk (MTurk)

Participants recruited from Amazon Mechanical Turk (MTurk) have been previously shown to be more representative than in-person convenience samples (Buhrmester et al., 2016) and garner similar levels of validity in comparison to college student samples, other similar online samples, and pools drawn from social media (Berinsky et al., 2012; Casler et al., 2013; Clifford et al., 2015). Similarly, research has also indicated that MTurk participants perform better on attention checks and follow instructions better than college student samples (Hauser & Schwarz, 2016). Thomas and Clifford (2017) noted that although insufficient attention is a potential problem in MTurk studies, there is no evidence that inattention is a bigger problem for MTurk samples than for other commonly used convenience samples.

We took several precautions to ensure that the collected data are of high quality. Specifically, participants had to meet a high approval rating (at least 95%) and, following the recommendations of Thomas and Clifford (2017), we included an attention check that was unique to this survey. The attention check item blended in with the survey content in an unobtrusive way.

Although the vast majority of participants do not use MTurk as their main source of income (Pew Research Center, 2016), participants on MTurk are primarily motivated by money in taking surveys (Litman et al., 2015; Pew Research Center, 2016). There has been concern that paying too high or too low of wages may impact data quality, but Rouse (2015) and Litman et al. (2015) demonstrated reliability across wages that were below, at, or above minimum wage. Although a meta-analysis has shown that average hourly wage has been as low as $2 for MTurk studies, at least minimum wages should be paid as compensations for ethical reasons (Silberman et al., 2018). Therefore, we piloted the length of the surveys to estimate what a fair wage would be, based on the time it took to complete the survey.

Participants

As a second selection criterion beyond the MTurk approval rate, respondents had to be American citizens to be able to participate in the study. Of the 1,023 participants, 19 respondents indicated that they were not residing in the US, and 18 respondents did not answer the attention-check item correctly. The following analyses were conducted with the remaining 986 respondents. Table 1 provides descriptives for the gender, age, race, education, and income of the studied sample along with US census data for comparison purposes.

Procedure and Design

Participants were presented with a survey that contained one of four different newspaper articles adapted from Hinsz and Betts (2014). Each article provided a short, hypothetical news story about a bombing of an embassy (see Appendix for an example). Participants were asked to imagine they awoke to the news of a suicide attack in which a truck filled with explosives was detonated outside an embassy after being stopped by security personnel. The general storyline of each article was identical and each of the articles had a reference to the US. As in the study by Hinsz and Betts (2014), the articles differed in the nationality of the victims (US citizen vs. Thai citizen) and the location of the attack (US embassy in Thailand or Thai embassy in the US). In two articles, the attack supposedly occurred at the Royal Thai Embassy in Washington, D.C., and in the other two articles the attack supposedly occurred at the United States Embassy in Thailand. Within each location, the articles also differed in whether the victims were American or Thai citizens.

Each participant read one of the four articles representing four different conditions, to which participants were randomly assigned. After reading the article, the survey described the potential of probabilistic computing technologies helping the US government to analyze and decipher online data with the goal to identify terrorist threats earlier than in the past and increase the chance of possibly preventing more terrorist attacks like the one described in the article (see Appendix for details).

Subsequently, participants were provided a number of possible actions and were asked to evaluate how appropriate each of these counterterrorism efforts would be from their perspective. The following section measured participants' general privacy concerns, national identity, and political

Table 1 Age, Gender, Education, and Race of Participants in the Study

	Sample		US Census Data
Demographic	*n*	%	%
Age			
18–20	14	1.4	4.7
21–44	747	75.9	41.3
45–64	191	19.3	32.9
65 +	33	3.4	21.1
Gender			
Male	597	60.5	49.0
Female	373	37.9	51.0
Non-binary / third gender	9	0.9	-
Prefer not to say	7	0.7	-
Education			
Some schooling, but no diploma or degree	2	0.2	10.0
High school diploma or GED	59	6.0	29.0
Some college	154	15.7	17.6
Bachelor's or Associate degree	516	52.6	29.8
Some grad school	22	2.2	-
Graduate degree	228	23.2	13.7
Income			
Under $25,000	133	13.5	18.1
$25,001—$50,000	259	26.3	19.7
$50,001—$80,000 (U.S. Census 50–75)	312	31.6	16.5
$80,001—$130,000 (U.S. Census 75–150)	182	18.5	27.5
$130,000 + (U.S. Census 150 +)	74	7.5	18.3
Prefer not to say	26	2.6	-
Race			
White	743	75.4	61.6
Black or African-American	103	10.4	12.4
American Indian or Alaska Native	41	4.2	1.1
Asian	111	11.3	6.0
Hawaiian or Pacific Islander	5	0.5	0.2
Other	19	1.9	8.4

Notes: US Census data was not always divided exactly the same way as our sample, as noted. Age is divided into age groups in accordance with the divisions found on the US Census. Where dashes are listed in the US Census data, the Census did not have those answers as options

orientation. The survey concluded with the measure of demographic variables. The main measurements and instructions are provided in the Appendix.

Measurements

Counterterrorism Efforts Three different measures of counterterrorism efforts were used: Participants' agreement for the use of personal information by the US government to identify terrorist threats and Hinsz and Bett's (2014) regional and general measures of counterterrorism efforts.

Support for the Use of Personal Information The first scale contained sixteen items and specifically asked about the article each participant read. Each item on this scale was rated on a seven-point Likert scale (1, strongly disagree, to 7, strongly agree; see Appendix). Each item started with the statement, "Probabilistic computing is analyzing very large amounts of information to decipher and identify suspicious activities." Participants then evaluated sixteen items that systematically varied the underlined part of the following claim: "It would be appropriate to include private online conversations of US citizens living in the US to prevent terrorist attacks like the one described in the article."

Four different types of information were included. Two items referred to private information: "to include private online conversations" and "to include emails and other personal electronic information;" two items referred to public information: "to examine publicly available websites" and "to examine publicly available social media information." The two private information items were adapted from Williamson (2019), and the public information items were created new. Furthermore, each of these four types of information was broken into four groups of targeted individuals: "of US citizens living in the US," "of US citizens living outside the US," "of non-US citizens living in the US," and "of non-US citizens living outside the US." Responses to the two items relating to private information correlated highly with each other as did the responses to the two items relating to public information and were aggregated within each condition (pairwise *r*s varied between 0.73 and 0.84). Thus, for each respondent, eight measures of their support for the use of personal information were obtained, following a $2 \times 2 \times 2$ design based on the factors of *personal information* (private vs public), *citizenship* (US citizen vs non-US citizen), and *residence* (US vs. abroad).

Regional Counterterrorism Efforts The second scale contained five items taken from Hinsz and Betts (2014) to measure attitudes toward counterterrorism efforts in the region of the attack (US vs Thailand; e.g., "More money should be spent on efforts geared toward preventing terrorism in the region of the attack").

General Counterterrorism Efforts The third scale asked respondents to express their agreement with each of the five items of counterterrorism efforts in general (e.g., "I support the development and implementation of new technology that aids counterterrorism efforts in general").

Privacy Concerns Participants' general perceptions and concerns about privacy, in particular concerns about the misuse of private information on the internet, were measured with six items using a seven-point Likert scale, with higher scores indicating stronger privacy concerns. After forming a composite score, respondents were rank-ordered according to their privacy concerns and split into three equal-sized groups of individuals who had high ($M = 6.32$; $SD = 0.51$; $N = 332$), moderate ($M = 4.44$; $SD = 0.59$; $N = 338$), and low ($M = 2.42$; $SD = 0.67$; $N = 316$) privacy concerns. The three groups significantly differed from each other in their general privacy concerns ($F(2,983) = 3509.87$; $p < 0.01$).

National Identity National identification was measured through six items that were used to form a composite measure of national identity (e.g., "How important is being American to you?"). Subsequently, a median split was performed, forming two groups of respondents who systematically differed in the strength of their national identity (strong identity: $M = 6.07$; $SD = 0.69$; weak identity: $M = 3.28$; $SD = 0.94$; $t(984) = 53.22$; $p < 0.01$).

Political Orientation Four items were used to assess political orientation (e.g., "I am politically more liberal than conservative") on a seven-point Likert scale, with high scores indicating a more liberal and less conservative political orientation than low scores.

Demographics In addition to their age and gender, participants were asked in which state they live and to provide basic information about their education, their religious orientation, and their annual income in the previous year.

Results

Data were analyzed in the following steps: We first looked into potential effects of the nationality of the victims and the location of the attack that were varied across the newspaper articles on the reported support for counter-terrorism efforts, replicating the study of Hinsz and Betts (2014). In a second step, we looked at the overall correlations among the main variables of the study including the ascertained demographic variables. In a third step, we tested the hypotheses on the predicted support for the use of personal information for counter-terrorism measures using probabilistic computing technologies.

Support for Regional and General Counterterrorism Efforts: Replication of Hinsz and Betts (2014)

In general, there was substantial support for counterterrorism efforts in this sample. The mean value on the seven-point response scale measuring participants' support for counterterrorism efforts in the region that was described in the article was $M = 5.56$, matching the reported perception of Hinsz and Betts (2014) in a student sample. Similar to Hinsz and Betts (2014), we did not observe any substantial differences in the support of regional or general counterterrorism efforts due to the victims' citizenship (US citizen vs non-citizen) or the location of the attack that was described in the newspaper article (US vs Thailand) (all Fs < 1). Likewise, no substantial differences among the four conditions in the support for regional counter-terrorist measures were observed in an analysis of covariance in which differences in the support of general counterterrorism measures were controlled (partialled out) (all Fs < 1.1). The four conditions also did not trigger substantially different support for the usage of personal information to identify terrorist threats, neither for private personal information, nor for public personal information (all Fs < 1.88; $p > 0.40$). In the following analyses, we aggregated across responses to the four newspaper articles.

Correlations among Main Measures and Demographic Variables

Table 2 displays the overall means, standard deviations, and correlations among the main measures of the study and participants' age. Whereas support for regional and general counterterrorism were highly correlated (0.81), the correlation with the supported use of personal information was smaller (0.47 and 0.52) suggesting that respondents differentiated between their general support for counterterrorism efforts and their support of the use of personal information to identify terrorist threats and prevent attacks. Support for the use of personal information correlated negatively with respondents' privacy concerns (-0.54) and positively with their national identity (0.34). Respondents' expressed privacy concerns only weakly correlated with the remaining variables (< ±0.20), suggesting that privacy concerns were only weakly related to respondents' age, national identity, political orientation, and general support for counterterrorism measures. Female respondents ($M = 4.52$; $SD = 1.66$) tended to reveal stronger privacy concerns than male respondents ($M = 4.32$; $SD = 1.70$; $t(968) = 1.88$; $p = 0.06$), but were slightly more supportive of the use of personal information for counterterrorism efforts ($M = 4.89$; $SD = 1.29$) than male respondents ($M = 4.68$; $SD = 1.39$; $t(968) = 2.39$; $p < 0.05$). The variables listed in Table 2 were not strongly correlated with participants' level of education or self-reported income (all correlations < ±0.20; the correlation between participants' level of education and income was $r = 0.24$; $p < 0.01$).

Support for the Use of Personal Information to Prevent Terrorist Attacks: Test of Hypotheses

In line with the findings by Hinsz and Betts (2014), the study did not reveal in-group favoritism related to the support of regional counterterrorism efforts. As expected, though, it revealed strong in-group favoritism for the usage of personal information to prevent terrorist attacks. To test the proposed hypotheses, a MANOVA was conducted on the perceived appropriateness to use personal information with the following factors: The factors *personal information* (public vs private), *citizenship* (US citizen vs non-US citizen), and *residence* (US vs. abroad) were included as within-subjects factors. The factors *privacy concerns* (high/moderate/low) and *national identity* (strong/weak) were added as between-subjects factors.

All four hypotheses were supported. Figure 1 shows participants' support for using either US citizens' or non-US citizens' personal information for counterterrorism efforts, separately for public and private information and different levels of general concern for privacy. In line with Hypothesis 1, respondents perceived it as more appropriate to use large amounts of publicly available personal information

Table 2 Intercorrelations, Means, and Standard Deviations of Main Variables

Variable	*M*	*SD*	1	2	3	4	5	6
1. Use of Personal Information	4.75	1.36	-					
2. Privacy Concern	4.42	1.69	-.54**	-				
3. National Identity	4.71	1.62	.34**	-.14**	-			
4. Political Orientation	4.58	1.72	-.04	-.08*	-.35**	-		
5. Regional Counter Measures	5.56	1.14	.47**	-.13**	.30**	-.01	-	
6. General Counter Measures	5.52	1.18	.52**	-.18**	.32**	.00	.81**	-
7. Age	37.38	11.47	.06*	.19**	.14**	-.05	.13**	.13**

**p < .01 *p < .05

Notes: This table displays the correlations among the main variables of the study, including participants' support of counterterrorism activities, general privacy concerns, national identification and political orientation, and age. *Use of Personal Information* refers to participants' overall support to use personal information for the prevention of terrorist attacks through probabilistic computing technologies

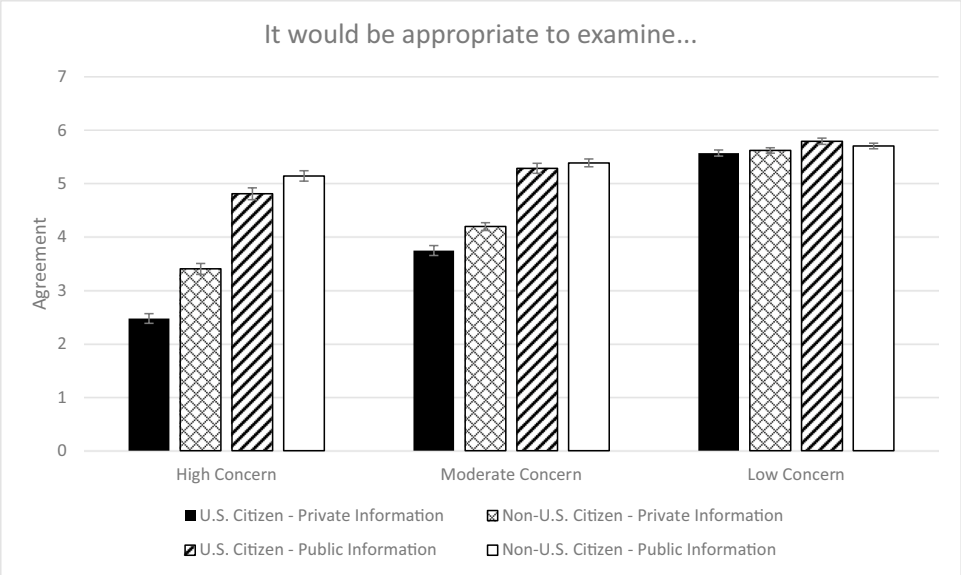

Fig. 1 Support for the Usage of Personal Information Separately for Different Levels of Privacy Concerns (High, Moderate, Low), Type of Personal Information (Private, Public), and Group Membership of Information Source (US Citizen/Non-US Citizen). *Notes:* This figure shows support for using either US citizens' or non-US citizens' personal information for counterterrorism efforts, separate for public or private information and different levels of general concern for privacy. Bars represent mean agreement across participants. Standard errors are added to each bar

($M = 5.35$; $SD = 1.36$) than to use private personal information ($M = 4.15$; $SD = 1.81$) to identify terrorist threats (main effect *personal information*, $F(1,980) = 625.27$; $p < 0.01$). In agreement with Hypothesis 2a, respondents who revealed high privacy concerns showed less support ($M = 3.96$; $SD = 1.40$) than respondents who had moderate ($M = 4.66$; $SD = 1.19$) or low concerns ($M = 5.67$; $SD = 0.83$; main effect *privacy concerns*, $F(2,980) = 176.87$; $p < 0.01$). As is evident in Fig. 1 and Table 3 and as predicted by Hypothesis 2b, the observed differences due to respondents' privacy concerns were larger for private than for public information (interaction *personal information x privacy concerns*, $F(2,980) = 131.39$; $p < 0.01$).

In support of Hypothesis 3a, respondents' support for private information revealed in-group favoritism in that respondents were more hesitant to support the use of personal information from US citizens ($M = 4.60$; $SD = 1.48$) than from non-US citizens ($M = 4.90$; $SD = 1.44$) (main effect *citizenship*, $F(2,980) = 86.13$; $p < 0.01$). Supporting Hypothesis 3b and 3c, in-group favoritism was particularly evident for private information (interaction *citizenship x personal information*, $F(1,980) = 109.76$; $p < 0.01$) within the group of respondents that showed high privacy concerns (interaction *citizenship x personal information x privacy concerns*, $F(2,980) = 14.35$; $p < 0.01$) (see Table 4).

These differences were further qualified by respondents' national identity supporting Hypothesis 4 (see Table 5 and Fig. 2). Respondents with strong national identities were more supportive of using personal information ($M = 5.11$; $SD = 1.30$) than respondents who expressed weaker national identities ($M = 4.36$; $SD = 1.32$) (main effect *national identity*, $F(1,980) = 78.79$; $p < 0.01$). The analysis revealed that in-group favoritism was strongest for private information

Table 3 Support for the Usage of Personal Information Separately for Different Levels of Privacy Concerns (High, Moderate, Low), and Type of Personal Information (Private, Public) (Hypothesis 2)

Information Source	High Privacy Concern	Moderate Privacy Concern	Low Privacy Concern
Private Information			
M	2.94	3.97	5.60
SD	1.66	1.60	0.96
Public Information			
M	5.00	5.34	5.75
SD	1.70	1.26	0.85
N	332	338	316

Table 4 Support for the Usage of Personal Information Separately for Different Levels of Privacy Concerns (High, Moderate, Low), Type of Personal Information (Private, Public), and Group Membership of Information Source (US Citizen/Non-US Citizen) (Hypothesis 3)

Information Source	High Privacy Concern	Moderate Privacy Concern	Low Privacy Concern
Private Information US Citizen			
M	2.48	3.75	5.57
SD	1.65	1.71	1.02
Private Information Non-US Citizen			
M	3.40	4.20	5.62
SD	2.02	1.73	1.04
Public Information US Citizen			
M	4.81	5.29	5.79
SD	1.87	1.34	0.91
Public Information Non-US Citizen			
M	5.15	5.39	5.71
SD	1.78	1.35	0.93
N	332	338	316

among those respondents who had strong privacy concerns (interaction *national identity x citizenship x personal information x privacy concerns*, $F(2,980) = 3.04$; $p < 0.05$). The four-way interaction was not qualified by the residence of the source (US vs abroad; $F < 1$).

Discussion

Probabilistic computing technologies promise to contribute to more efficient problem solutions in encryption and cybersecurity, increasing the probability to identify terrorist threats through deciphering communication on the internet. Probabilistic computing technologies use large amounts of data, though, which raises potential privacy concerns. The conducted survey study aimed to describe public support for the use of personal data and revealed several results. Overall, respondents showed strong support for using publicly available personal information such as personal websites or personal information on social media to increase counterterrorism efforts. The average agreement for the use of large amounts of public personal information was 5.35 on a scale from 1 (strongly disagree) to 7 (strongly agree). Regarding private personal information in online and email conversations, responses varied substantially depending on whether information would be taken from US citizens or non-US citizens and respondents' general privacy concerns and strength of national identity. Respondents perceived it to be more appropriate to use information from out-group members (non-American citizens) than from in-group members (American

Table 5 Support for the Usage of Personal Information Separately for Different Levels of National Identity (Low, High), Privacy Concerns (High, Moderate, Low), Type of Personal Information (Private, Public), and Group Membership of Information Source (US Citizen/Non-US Citizen) (Hypothesis 4)

	Low National Identity		
Information Source	High Privacy Concern	Moderate Privacy Concern	Low Privacy Concern
Private Information US Citizen			
M	2.08	3.35	5.28
SD	1.44	1.58	0.98
Private Information Non-US Citizen			
M	2.73	3.71	5.34
SD	1.82	1.61	0.95
Public Information US Citizen			
M	4.62	5.13	5.56
SD	1.92	1.40	0.83
Public Information Non-US Citizen			
M	4.85	5.18	5.44
SD	1.79	1.36	0.86
N	171	176	134
	High National Identity		
	High Privacy Concern	Moderate Privacy Concern	Low Privacy Concern
Private Information US Citizen			
M	2.89	4.18	5.79
SD	1.76	1.73	1.00
Private Information Non-US Citizen			
M	4.12	4.72	5.83
SD	1.98	1.69	1.05
Public Information US Citizen			
M	5.02	5.46	5.97
SD	1.79	1.26	0.93
Public Information Non-US Citizen			
M	5.46	5.61	5.90
SD	1.72	1.30	0.94
N	161	162	182

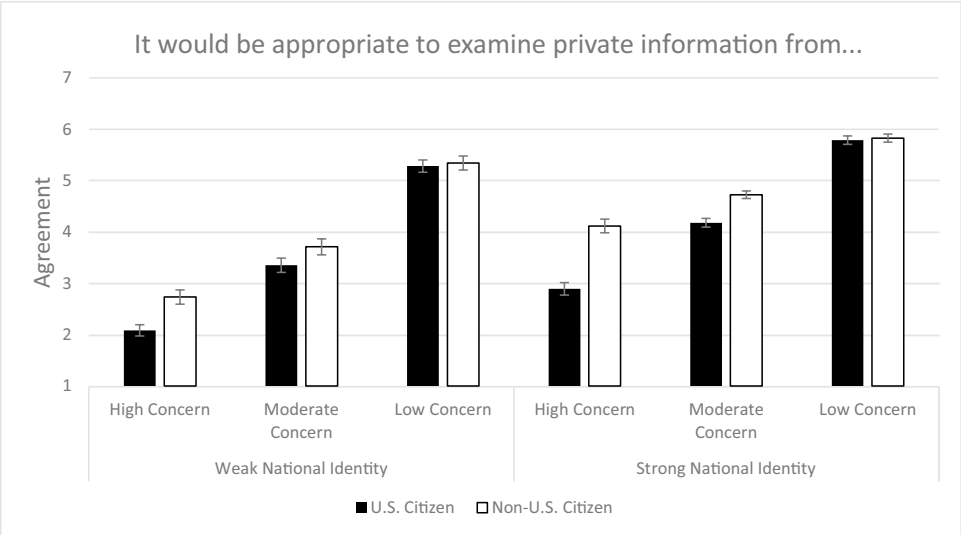

Fig. 2 Support for the Usage of Private Personal Information by Respondents Varying in their General Privacy Concerns and National Identification. *Notes:* This figure shows support for using either US citizens' or non-US citizens' private information for counterterrorism efforts, based on the general levels of concern for privacy and identification as an American. Bars represent mean agreement across participants. Standard errors are added to each bar

citizens) displaying in-group favoritism. In line with a social-identity account, this form of in-group favoritism was strongest among respondents who were showing a combination of strong national identities and strong privacy concerns.

According to social identity theory (Tajfel & Turner, 1986), individuals respond differently when their group identity becomes salient to them. This holds in particular for group members who strongly identify with their group. Generally, in-group favoritism refers to the tendency to have more favorable opinions of and responses toward one's own group than toward an out-group (Tajfel & Turner, 1986). As documented in many studies, in-group favoritism occurs in a wide range of situations (Mullen et al., 1992).

Only few studies have taken a social-scientific approach to describe and analyze public support for counterterrorism efforts (Hinsz & Betts, 2014; Lum & Kennedy, 2012). To our knowledge, this is the first study that connected privacy concerns with in-group favoritism regarding the use of personal information. The observed differences in the support for the use of personal information to prevent terrorist attacks were very strong. The strongest support was observed for respondents who had strong national identities and low general privacy concerns. As can be seen in Fig. 2 and Table 5, their average support was 5.83 on a seven-point scale. Conversely, the lowest support was found among those who had strong privacy concerns but low national identities, which was 2.08 and, thus, almost 4 points lower on the seven-point scale. Whereas in-group favoritism was strongest for respondents who scored high on the national identity and privacy concerns, the lowest support for the use of private information was found among those who had high privacy, but low national identity scores.

The observed differences are remarkably strong. Notably, even though questions regarding the use of computer and information technology to prevent terrorist attacks have important political dimensions, the current study showed that public support cannot be reduced to political partisanship and also not to mere national identification. Respondents' general privacy concerns only showed a low correlation with their political orientation and their national identification. Likewise, respondents' age was not strongly correlated with their support for the use of personal information, nor was it strongly related to respondents' privacy concerns or national identification.

These results suggest a couple of possible implications for governmental policy. Given the high level of overall support for using public information for counterterrorism efforts, this study suggests it may be acceptable for the government to use probabilistic computing and similar technologies to monitor personal information that is already publicly available. However, the study also suggests that people may be much more resistant toward policies that would ask them to give up their private information, especially for those who are more concerned about privacy and those who have a weaker national identity.

The observed privacy and group membership effects held across different demographic variables including participants' age, education, and income, which showed only low correlations with the observed support of the use of personal information. There are additional variables that have not been measured in the current study that may moderate the observed differences. For example, we did not measure how often participants engage in online conversations and how much personal information they convey about themselves on publicly available websites. Future studies may explore if the link between privacy concerns and in-group favoritism generalizes across consumers that differ in their internet and social media use.

Although MTurk has been shown to be more representative of the population than college samples and some other convenience sample techniques (Berinsky et al., 2012; Buhrmester et al., 2016), it does have systematic differences in its population as compared to the US population. Specifically, Berinsky et al. (2012) reported that the MTurk population is slightly more educated and contains a higher proportion of females,

Democrats, and whites, as compared to the US census. As indicated in Table 1, most of these trends were also seen in our sample, though, we did end up with a higher proportion of males (61%). It is not clear if the higher proportion of males is related to the topic of the current study or may be an artifact of the particular sample or a result of demographic shifts on MTurk during the COVID-19 pandemic, as studies on the demographic shifts on MTurk show consistency in gender but some changes in political orientation and race (Arechar & Rand, 2021; Moss et al., 2020). Future studies may test how robust the observed results are and if they can be generalized using other measurements and samples of participants.

The scope of the hypotheses and their intended applications (Balzer et al., 1989) referred to a situation in which potential terrorist threats clearly have a connection to a country and in which the access to personal information is intended to be used by one's own government. Building on Hinsz and Betts' studies (2014), we varied in the used news stories the proximity of the victim and location. Like Hinsz and Betts (2014), we did not find substantial differences between these scenarios in respondents' support for general or regional counterterrorism efforts. One explanation of these findings may be that all four scenarios had a connection to the US, be it geographically or in terms of the imagined victims or the proximity of an American embassy abroad. These cues may have been sufficient to trigger the salience of respondents' in-group and national identities. Future studies may extend this approach by looking at regions and locations that are not tied to the US and at countries that vary in their international relationships with the US (e.g., Germany, Iran, Russia, and China). Support for counterterrorism efforts and the use of personal information may depend on perceptions and trust towards the agency using the technology and perceptions of the beneficiary of the efforts. Likewise, the study stressed that the US government may use probabilistic computer technologies and access personal information. Future studies may explore if public support would be different if other stakeholders including private domestic and international companies and governments of foreign countries would have agency over the technology.

This study focused on probabilistic computing technologies that use large amounts of personal information to identify terrorism threats and prevent terrorist attacks. It would be interesting to explore in future research if public support may look different for other uses of the p-bits technology (e.g., for financial services or supply chain management).

Surveillance technology in private spaces is seen as more appropriate when it is used to prevent serious crimes including terrorist attacks than in situations in which minor crimes are prevented (Pavone & Esposti, 2010). Thus, it may well be that the observed support for the use of the p-bits technology would be smaller if it were used for other purposes and in other contexts (e.g., for marketing purposes). A central contribution of the current study is the predicted and observed link between privacy concerns and in-group favoritism. As can be seen in Fig. 1, privacy concerns mainly affected the use of private personal information but had only small effects on the use of publicly available personal information. Future studies may explore if the privacy and in-group favoritism link can also be found for other technologies such as surveillance technologies and in other contexts (e.g., health contexts) that trigger privacy concerns as well as societal threats (e.g., information relevant to the spread of infectious diseases).

Appendix – Survey Questionnaire

(Instructions that were provided to participants are written in italics.)

Imagine that you awoke to news of a suicide attack in which a truck filled with explosives was detonated outside an embassy after being stopped by security personnel. This is the article where you read the story.

The Daily N

Embassy bombing kills 7

Bangkok, Thailand. Seven American citizens were killed in a bombing outside the Embassy of the United States in Bangkok this morning.

A truck containing explosives detonated alongside a van containing American visitors to the embassy. Embassy security personnel report that the suspect waited at a nearby construction site until gates to the embassy opened for the visitors. The suspect then attempted to drive the truck through the gates. Confronted by security personnel, the suspect detonated the explosives.

The dead include six American civilians, and one American embassy security worker. The embassy building remained undamaged and no Thai were hurt by the blast.

As of yet, no group or individual has claimed responsibility for organizing the attack. A Thai police officer speaking under conditions of anonymity reported that the Thailand National Police Department has suspects, but refused additional comment because of the ongoing investigation.

Note: This article provides an example of one of four conditions, as described in the Methods section. The newspaper articles have been adapted from Hinsz and Betts (2014). Each participant read one of the four articles, which were randomly assigned.

More terrorist attacks like the one described in the article could possibly be prevented if the United States implemented probabilistic computing technologies to analyze online data for terrorist plans and activities. This new form of computing technology can be used to analyze large amounts of data quickly to help identify terrorist threats earlier and increase the chance of stopping them.

Terrorist communication is known to occur in hidden, encrypted, or disappearing messages online through venues like email, online gaming, texting, and chat rooms, which all contain very large amounts of information that previously could not be processed quickly enough to be useful for tracking terrorist activity. But with probabilistic computing, this could now be possible. However, in order for this to become a reality, the United States government would have to access large amounts of information, including personal information from many individuals.

In the following questions, we provide a number of possible actions. Please evaluate how appropriate each of these responses would be to attempt to identify and prevent terrorist attacks like the one described in the article.

Each of the scales below (except the *National Identity* index) was measured using a seven-point Likert scale (1-strongly disagree; 2-moderately disagree; 3-slightly disagree; 4-neither agree nor disagree; 5-slightly agree; 6-moderately agree; 7-strongly agree).

Counter Terrorism Efforts

Support for the Use of Personal Information

Two items related to private personal information, which were adapted from Williamson (2019). The two items referred to *private online conversations* and *emails and other personal electronic information*. Two items related to public personal information and referred to *publicly available websites* and *publicly available social media information*. Responses to the two items relating to private information correlated highly with each other as did the responses to the two items relating to public information and were subsequently aggregated within each condition (pairwise *r*s varied between 0.73 and 0.84).

- Probabilistic computing is analyzing very large amounts of information to decipher and identify suspicious activities. It would be appropriate _____ to prevent terrorist attacks like the one described in the article.
  - to examine publicly available websites of U.S. citizens living in the U.S.
  - to examine publicly available websites of U.S. citizens living outside the U.S.
  - to examine publicly available websites of non-U.S. citizens living in the U.S.
  - to examine publicly available websites of non-U.S. citizens living outside the U.S.
  - to monitor publicly available social media information from U.S. citizens living in the U.S.
  - to monitor publicly available social media information from U.S. citizens living outside the U.S.
  - to monitor publicly available social media information from non-U.S. citizens living in the U.S.
  - to monitor publicly available social media information from non-U.S. citizens living outside the U.S.
  - to include private online conversations of U.S. citizens living in the U.S.
  - to include private online conversations of U.S. citizens living outside the U.S.
  - to include private online conversations of non-U.S. citizens living in the U.S.
  - to include private online conversations of non-U.S. citizens living outside the U.S.
  - to include emails and other personal electronic information from U.S. citizens living in the U.S.
  - to include emails and other personal electronic information from U.S. citizens living outside the U.S.
  - to include emails and other personal electronic information from non-U.S. citizens living in the U.S.
  - to include emails and other personal electronic information from non-U.S. citizens living outside the U.S.

Support for Regional Counterterrorism Efforts (from Hinsz & Betts, 2014) (Cronbach's α = 0.88)

In the following questions, additional counter-terrorism efforts are described. Please evaluate the appropriateness of these efforts to prevent ***attacks like the one described in the article.***

- I support the development and implementation of new technology that aids counterterrorism efforts in the region of the attack.
- More should be done to acquire information that aids counterterrorism efforts in the region of the attack.
- More money should be spent on efforts geared toward preventing terrorism in the region of the attack.
- More skilled workers that are involved in counterterrorism efforts in the region of the attack should be hired.
- Relaxed counterterrorism policies in the region of the attack should be reviewed more carefully.

Support for General Counterterrorism Efforts (from Hinsz & Betts, 2014) (Cronbach's α = 0.89)

In the following questions, additional counter-terrorism efforts are described. Please evaluate the appropriateness of these efforts to prevent ***terrorist attacks in general.***

- I support the development and implementation of new technology that aids counterterrorism efforts in general.
- More should be done to acquire information that aids counterterrorism efforts in general.
- More money should be spent on efforts geared toward preventing terrorism in general.
- More skilled workers that are involved in counterterrorism efforts in general should be hired.
- Relaxed counterterrorism policies in general should be reviewed more carefully.

Privacy, Government, and Politics

In this section, we will ask you for your personal opinions on privacy, government, and politics. The following questions ***do not refer to the article you read*** *in the beginning of the survey. We are interested in your personal opinions. There are no right or wrong answers.*

Privacy Concerns (all items were reverse coded) (Cronbach's α = 0.92)

From Misis et al. (2017)

- I do not mind giving up my right to privacy.
- I do not mind giving up my protection against unreasonable search and seizure.

From Salisbury et al. (2001)

- I feel secure sending sensitive information across the internet.
- The internet is a secure means through which to send sensitive information.
- I feel totally safe providing sensitive information about myself over the internet.
- Overall, the internet is a safe place to transmit sensitive information.

National Identity (from Huddy & Khatib, 2007) (Cronbach's = 0.93)

- How important is being American to you?
  1-Not at all important; 2-Just a little important; 3-Somewhat important; 4-Moderately important; 5-Quite important; 6-Very important; 7-Extremely important;
- To what extent do you see yourself as a typical American?
  1-Not at all; 2-Just a little; 3-Somewhat; 4-Moderately; 5-Quite a bit; 6-Very much; 7-Completely;
- How well does the term *American* describe you?
  1-Not at all well; 2-Just a little well; 3-Somewhat well; 4-Moderately well; 5-Quite well; 6-Very well; 7-Extremely well;
- When talking about Americans, how often do you say "we" instead of "they"?
  1-Never; 2-Almost never; 3-Some of the time; 4-Half of the time; 5-Most of the time; 6-Almost always; 7-Always
- How good does it make you feel when you see the American flag flying?
  1-Not at all good; 2-Just a little good; 3-Somewhat good; 4-Moderately good; 5-Quite good; 6-Very good; 7-Extremely good;
- How good does it make you feel when you hear the national anthem?
  1-Not at all good; 2-Just a little good; 3-Somewhat good; 4-Moderately good; 5-Quite good; 6-Very good; 7-Extremely good;

Political Orientation (from Mehrabian, 1997) (Cronbach's = 0.83)

- I am politically more liberal than conservative.
- In any election, given a choice between a Republican and a Democratic candidate, I will select the Republican over the Democrat. (*reverse coded*)
- I cannot see myself ever voting to elect conservative candidates.
- On balance, I lean politically more to the left than to the right.

Acknowledgements This study was funded as part of a Purdue 2.0 Big Challenge award. We are grateful to Joerg Appenzeller, Supriyo Datta, and Peter Bermel for educating us about probabilistic computing technologies using p-Bits and to Purdue Discovery Park for supporting our study.

Data Availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of Interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Agrawal, R. & Srikant, R. (2000). Privacy-preserving data mining. In M. Durham, J. F. Naughton, W. Chen, & N. Koudas (Eds.), *Proceedings of the 2000 ACM SIGMOD international conference on management of data* (pp. 439–450). Dallas, Texas.

Allport, G. W. (1954). *The nature of prejudice*. Addison-Wesley.

Arechar, A. A., & Rand, D. G. (2021). Turking in the time of COVID. *Behavior Research Methods, 53*, 2591–2595.

Atienza, A. A., Zaracadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W. S., & Pritts, J. (2015). Consumer attitudes and perceptions on mHealth privacy and security: Findings from a mixed-methods study. *Journal of Health Communication, 20*(6), 673–679.

Balzer, W., Moulines, C. U., & Sneed, J. D. (1989). *The architectonic for science: The structuralist program*. D. Reidel Publishing Company.

Behin-Aein, B., Diep, V., & Datta, S. (2016). A building block for hardware belief networks. *Scientific Reports, 6*, 29893.

Berinsky, A., Huber, G., & Lenz, G. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis, 20*(3), 351–368.

Brewer, M. B. (1999). The psychology of prejudice: Ingroup love or outgroup hate? *Journal of Social Issues, 55*, 429–444.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2016). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality data? In A. E. Khazdin (Ed.), *Methodological issues and strategies in clinical research* (pp. 133–139). American Psychological Association.

Camsari, K. Y., Debashis, P., Ostwal, V., Pervaiz, A. Z., Shen, T., Chen, Z., Datta, S., & Appenzeller, J. (2020). From charge to spin and spin to charge: Stochastic magnets for probabilistic computing. *Proceedings of the IEEE, 108*(8), 1322–1337.

Camsari, K. Y., Faria, R., Sutton, B. M., & Dutta, S. (2017). Stochastic bits of invertible logic. *Physical Review, X 7 (3)*, 031014.

Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's Mturk, social media, and face-to-face behavioral testing. *Computers in Human Behavior, 29*(6), 2156–2160.

Clifford, S., Jewell, R. M., & Waggoner, P. D. (2015). Are samples drawn from Mechanical Turk valid for research on political ideology? *Research & Politics, 2*(4).

Crow, M. S., Snyder, J. A., Crichlow, V. J., & Smykla, J. O. (2017). Community perceptions of police body-worn cameras: The impact of views on fairness, fear, performance, and privacy. *Criminal Justice and Behavior, 44*(4), 589–610.

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *International Journal of Medical Informatics, 141,* 104164.

Drozdova, K., & Samoilov, M. (2010). Predictive analysis of concealed social network activities based on communication technology choices: Early-warning detection of attack signals from terrorist organizations. *Computational and Mathematical Organization Theory, 16*, 61–88.

Hayes, J. L., Brinson, N. H., Bott, G. J., & Moeller, C. M. (2021). The influence of consumer–brand relationship on the personalized advertising privacy calculus in social media. *Journal of Interactive Marketing, 55*, 16–30.

Hauser, D. J., & Schwarz, N. (2016). Attentive Turkers: Mturk participants perform better on online attention checks than do subject pool participants. *Behavior Research Methods, 48*, 400–407.

Hinsz, V., & Betts, K. R. (2014). Public support for counterterrorism efforts: The role of ingroup bias, individual differences, and proximity to terrorist attacks. In J. M. Ramirez, C. Morrison, & A. J. Kendall (Eds.), *Conflict, terrorism, and their prevention* (pp. 131–149). Cambridge Scholars Publishing.

Huddy, L., & Khatib, N. (2007). American patriotism, national identity, and political involvement. *American Journal of Political Science, 51*(1), 63–77.

Hwang, H., & Lin, Y. (2020). Evaluating people's concern about their health information privacy based on power-responsibility equilibrium mode: A case of Taiwan. *Journal of Medical Systems, 44*, 112.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers. *Criminology & Public Policy, 16*(1), 99–117.

Kim, Y., Choi, B., & Jung, Y. (2018). Individual differences in online privacy concern. *Asia Pacific Journal of Information Systems, 28*(4), 274–289.

Larson, R. B., & Ferrin, B. G. (2021). Shopper attitudes about privacy and the likelihood of disabling an RFID tag. *International Journal of Logistics Systems and Management, 38*(3), 325–342.

Lewin, K. (1935). *A dynamic theory of personality*. McGraw-Hill.

Litman, L., Robinson, J., & Rosenzweig, C. (2015). The relationship between motivation, monetary compensation, and data quality among US- and India-based workers on Mechanical Turk. *Behavior Research Methods, 47*, 519–528.

Lum, C., & Kennedy, L. W. (2012). Evidence-based counterterrorism policy. In C. Lum & L. W. Kennedy (Eds.), *Evidence-based counterterrorism policy* (pp. 3–9). Springer, New York, NY.

Misis, M. L., Bush, M. D., & Hendrix, N. (2017). An examination of college students' fears about terrorism and the likelihood of a terrorist attack. *Behavioral Sciences of Terrorism and Political Aggression, 9*(2), 125–138.

Moss, A. J., Rosenzweig, C., Robinson, J., & Litman, L. (2020). Demographic stability on Mechanical Turk despite COVID-19. *Trends in Cognitive Sciences, 24*(9), 678–680.

Mueller, B., Rashbaum, W. K., & Baker, A. (2017, October 31). Terror attack kills 8 and injures 11 in Manhattan. *The New York Times*. https://www.nytimes.com/2017/10/31/nyregion/police-shooting-lower-manhattan.html

Mullen, B., Brown, R., & Smith, C. (1992). Ingroup bias as a function of salience, relevance, and status: An integration. *European Journal of Social Psychology, 22*(2), 103–122.

Newell, B. C. (2016). Collateral visibility: A socio-legal study of police body-camera adoption, privacy, and public disclosure in Washington State. *Ind. LJ, 92*, 1329–1399.

Pavone, V., & Esposti, S. D. (2010). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science, 21*(5), 556–572.

Pew Research Center. (2016). Turkers in this canvassing: Young, well-educated and frequent users. https://www.pewresearch.org/internet/2016/07/11/turkers-in-this-canvassing-young-well-educated-and-frequent-users/

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2–17.

Rouse, S. V. (2015). A reliability analysis of Mechanical Turk data. *Computers in Human Behavior, 43*, 304–307.

Safaeimanesh, F., Kılıç, H., Alipour, H., & Safaeimanesh, S. (2021). Self-service technologies (SST) – The next frontier in service excellence: Implications for tourism industry. *Sustainability, 13*(5), 2604.

Salisbury, W. D., Pearson, R. A., Pearson, A. W., & Miller, D. W. (2001). Perceived security and World Wide Web purchase intention. *Industrial Management & Data Systems, 101*(4), 165–176.

Schuurman, B., Bakker, E., Gill, P., & Bouhana, N. (2018). Long actor terrorist attack planning and preparation: A data-driven analysis. *Journal of Forensic Sciences, 63*(4), 1191–1200.

Shanaah, S. (2019). Alienation or cooperation? British Muslims' attitudes to and engagement in counterterrorism and counter-extremism. *Terrorism and Political Violence*, 1–22.

Silberman, M. S., Tomlinson, B., LaPlante, R., Ross, J., Irani, L., & Zaldivar, A. (2018). Responsible research with crowds: Pay crowdworkers at least minimum wage. *Communications of the ACM, 61*(3), 39–41.

Sun, Z., & Huo, Y. (2019). The spectrum of big data. *Journal of Computer Information Systems, 61*(2), 154–162.

Swani, K., Milne, G. R., & Slepchuk, A. N. (2021). Revisiting trust and privacy concern in consumers' perceptions of marketing information management practices: Replication and extension. *Journal of Interactive Marketing, 56,* 137-158.

Tajfel, H., & Turner, J. C. (1986). The social identity theory of intergroup behavior. In S. Worchel & W. Austin (Eds.), *Psychology of intergroup relations* (pp. 7–24). Nelson Hall.

Thomas, K. A., & Clifford, S. (2017). Validity and Mechanical Turk: An assessment of exclusion methods and interactive experiments. *Computers in Human Behavior, 77*, 184–197.

United States Census Bureau. (n.d.). *Census.* https://www.census.gov/en.html

van Heek, J., Arning, K., & Ziefle, M. (2014). Safety and privacy perceptions in public spaces: An empirical study on user requirements for city mobility. In R. Giaffreda, D. Cag, Y. Ki, R. Riggio, & A. Voisard (Eds.), *International internet of things summit* (pp. 97–103). Springer International Publishing.

Williamson, H. (2019). Pride and prejudice: Exploring how identity processes shape public attitudes towards Australian counterterrorism measures. *Australian and New Zealand Journal of Criminology, 52*(4), 558–577.