When Those with Privacy Concerns Show Stronger In-group Favoritism: Using Personal Information from In-group and Out-group Members to Identify Terrorist Threats

Torsten Reimer
Nathanael Johnson

Follow this and additional works at: https://docs.lib.purdue.edu/fund

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact epubs@purdue.edu for additional information.
When Those With Privacy Concerns Show Stronger In-Group Favoritism: Using Personal Information From In-Group and Out-Group Members to Identify Terrorist Threats

Torsten Reimer and Nathanael Johnson

Abstract
Terrorist threats and attacks provide major risks and sources of public crises in the 21st century. New probabilistic computing technologies possess the capability of increasing the success of identifying terrorist threats and solving cybersecurity and encryption problems more efficiently. However, to identify terrorist threats, these technologies would require the use of a large amount of personal data, which cause potential concerns for privacy. We offer a social-identity explanation of public support for the detection of terrorist threats through the use of online personal data. A survey study (N = 1,204) revealed strong support for the provided social-identity explanation of public perceptions. As expected, respondents displayed in-group favoritism by more strongly supporting the use of private personal information from out-group members (non-U.S. citizens) than from in-group members (U.S. citizens). The observed in-group favoritism was most pronounced when respondents had both a strong national identity and a strong sense of general privacy concern. The observed differences were independent of respondents’ political orientation and age.

Keywords
Public opinions about counter-terrorism, adoption of new technologies, use of personal data, privacy concerns, social identity, in-group favoritism, national identities

Introduction
On August 1st, 2019, top diplomats from major world powers including the United States and China were meeting in Bangkok, Thailand, to discuss security in Southeast Asia (Wongcha-um & Thepgumpanat, 2019). Six bombs exploded around the city, wounding several people and causing significant damage. Thailand’s prime minister condemned the attack as destroying the peace and progress Thailand had worked for. He went on to urge the people of Thailand to cooperate fully with the authorities to seize the attackers.

A bombing such as this requires a coordinated effort by multiple individuals, which involves communication over the internet. Terrorist communication over the internet is known to happen in public and private spaces like email, chat rooms, and online games, all of which pass large amounts of information through them rapidly, causing difficulty tracking and identifying relevant information that may pertain to terrorist activity (Drozdova & Samoilov, 2010). However, the potential to identify information relevant to terrorist activity is being considerably heightened by probabilistic computing technologies, which are capable of tracking large amounts of online information rapidly (Behin-Aein et al., 2016; Camsari et al., 2017). Probabilistic computers replace stable magnets in standard computers that hold a bit of information as a constant zero or one with unstable magnets that fluctuate between ones and zeros (Behin-Aein et al., 2016). The processing power of these bits, known

1Purdue University, West Lafayette, IN, USA

Corresponding Author:
Torsten Reimer, Communication and Cognition Lab, Brian Lamb School of Communication, Purdue University, 100 North University Street, West Lafayette, IN 47907-2050, USA.
Email: treimer@purdue.edu

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 4.0 License (https://creativecommons.org/licenses/by/4.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
as p-bits, offers to increase the speed and ability of computers to concurrently process large datasets (Camsari et al., 2020). The use of probabilistic computing by government entities promises to limit attacks like the one described above by detecting communication about attacks earlier, giving greater opportunity to thwart the plans of terrorists.

To identify the planning of terrorist activity on the internet, the technology has to process large amounts of data: Along with the few pieces of information that are collected to combat terrorism, mass amounts of irrelevant information would be processed also, the personal information of innocent civilians. Thus, the adoption of such technology raises potential privacy concerns, similar to those raised in other applications of data mining, artificial intelligence, and machine learning that use large sets of online data (Sun & Huo, 2019). Surveillance for security reasons is known to enhance feelings of security and safety, but there is also widespread concern that such surveillance may be an invasion of privacy (van Heek et al., 2014). We sought to assess public concern for and acceptance of government use of probabilistic computing technologies to gather online information for the purpose to prevent terrorist attacks. Specifically, we tested four hypotheses derived from a social-identity framework (Tajfel & Turner, 1986) that describe the independent and combined effects of four factors on the acceptance of the use of personal information to prevent terrorist attacks: whether information is being gathered from members who belong to one’s own group (the in-group) or an out-group; whether the collected information is private or publicly available; and respondents’ national identity and overall sense of privacy regarding online information. The proposed hypotheses were supported in a recent study (see Reimer & Johnson, 2022) that used an MTurk (Amazon Mechanical Turk) sample of N = 1,023 participants and provided participants with a newspaper article describing a specific attack that was developed by Hinsz and Betts (2014). We aimed to extend on the study by Reimer and Johnson (2022) in the following ways: (1) test the hypotheses with a new sample of participants (N = 1,204); (2) use a variety of different possible terrorist attacks that have been described in the literature (see Liu et al., 2019); (3) focus on the observed in-group favoritism regarding the surveillance of private information and compare the effect more closely to other effects of in-group favoritism.

In the remainder, we begin by introducing basic tenets of social identity theory and the concept of in-group favoritism, which refers to the tendency to favor members of one’s in-group over members of out-groups. Next, we introduce a specific form of in-group favoritism that is related to privacy concerns. We reasoned that privacy concerns would be generally lower for out-group members than for in-group members. Accordingly, we expected that U.S. citizens will support the use of personal information from out-group members, or non-U.S. citizens, more than from in-group members. Next, we discuss several conditions that were expected to qualify the predicted in-group favoritism. First, we anticipated that the level of in-group favoritism would be increased for private information, compared to publicly available information. Likewise, we reasoned that the extent of in-group favoritism regarding privacy concerns depends on the level of national identification an individual holds and on general privacy concerns. We expected that this would be shown as stronger in-group favoritism for those with both a strong national identity and high concerns for privacy. Next, we report a study in which we tested the described hypotheses, concluding with a discussion of the results, implications, and future research.

### Social Identity Theory: The Use of Personal Information from In-Group and Out-Group Members

Social identity theory posits that membership in social groups is integral to an individual’s self-concept (Tajfel & Turner, 1986). The identification with a group and comparison of this group with relevant other groups lead to the formation of in-group favoritism. People strive to be members of superior groups that are more positively evaluated than relevant comparison groups. To gain and maintain a positive self-concept, people favor their own group over out-groups. Positive self-esteem can be achieved by positively differentiating one’s in-group from a relevant out-group (Aronson et al., 2018; Tajfel & Turner, 1986).

Many studies have documented the wide nature of in-group favoritism, which occurs in many situations and can involve the evaluation of others, the allocation of resources, the determination of punishments, and the willingness to interact and cooperate with others (Balliet et al., 2014; Guo et al., 2022; Hogg & Ridgeway, 2003; Hornsey, 2008; Krahé & Reimer, 1998; Mullen et al., 1992).

In-group favoritism has also been demonstrated in the context of terrorism and anti-terrorism (e.g., Levy & Rozmann, 2022) and has been linked to institutional out-group discrimination and support for anti-immigration policies (Doosje et al., 2009). Like Reimer and Johnson (2022), we started out to explore another possible form of in-group favoritism that is concerned with the use of personal information that raises potential privacy concerns. The literature on social identity suggests that individuals trust in-group members more than out-group members (Cruwys et al., 2020), and they are less concerned sharing information with in-group than with out-group members (Bingley et al., 2022). People feel a sense
of belonging together when they have access to the same information (Bingley et al., 2022), and a sense of belonging and shared group membership leads to more effective communication (Greenaway et al., 2015). Bingley et al. (2022) offer a model that highlights situations in which it is functional to extend privacy to others (e.g., in online support groups). According to Bingley et al. (2022), however, maintaining personal privacy can have benefits in the face of external threats. Accordingly, Reimer and Johnson’s (2022) study aimed to test the idea that people may care more about reducing privacy threats and maintaining privacy for members of one’s own group than for members of out-groups.

There is a significant tension between safety from crime and control over one’s own private information. The use of online personal information to stop crime or terrorist activity also invades private information, bringing with it the potential of fraudulent use of that information. This raises concerns about who has access to personal information and whether those people are trustworthy. In democratic societies, citizens have typically more trust in their government than in foreign governments. However, do people show in-group favoritism in terms of the information that is used?

Hinsz and Betts (2014) hypothesized that American citizens would be more favorable toward counter-terrorism efforts to counteract attacks on fellow Americans, in comparison to an attack occurring elsewhere, against people that are not U.S. citizens. They reasoned that citizenship in a country would be sufficient to trigger in-group favoritism for increased effort to protect the in-group. This proposed favoritism is not necessarily based on negative views of an out-group (Allport, 1954; Brewer, 1999), acting independently of, though not precluding, any negative biases. Hinsz and Betts’s (2014) hypothesis was not supported in two studies with undergraduate students and did not find support in a follow-up study with an MTurk sample (see Reimer & Johnson, 2022). In all three studies, similar support was observed for counter-terrorism efforts for both in-groups and out-groups. Hinsz and Betts’s (2014) studies did not include a measure of potential costs or risks of counter-terrorism efforts. We extended on their approach by exploring support for using people’s online personal information for counter-terrorism, proposing that efforts for counter-terrorism that induce a particular cost may reveal in-group favoritism whereas measures without costs do not. We expected that the use of out-group members’ personal information (non-U.S. citizens) would be perceived more favorably than using in-group members’ personal information (U.S. citizens).

Hypothesis 1: To prevent a counter-terrorism attack, respondents perceive it as more appropriate to use personal information from out-group members (non-U.S. citizens) than from in-group members (U.S. citizens) and display in-group favoritism (citizenship of source).

Generally, in-group favoritism becomes more pronounced when a person identifies with their group more strongly (Aronson et al., 2018; Jiang & Christian, 2022). Individuals are particularly likely to display in-group favoritism when the in-group is central to their self-concept, and when the given comparison is particularly relevant, or the outcome is contestable (Tajfel & Turner, 1986). Previous literature has suggested that stronger identification with one’s own country leads to higher favorability toward counter-terrorism, in comparison to people with weaker national identity (Williamson, 2019). Hinsz and Betts (2014) found nationalism and support for counter-terrorism measures to be strongly correlated with one another. Similarly, Williamson (2019) observed an effect of national identity on support for counter-terrorism measures in Australia. Based on these previous studies (also see Doosje et al., 2009; Reimer & Johnson, 2022), we expected that stronger national identity would lead to more support for the use of personal information to combat terrorism, combined with an effect of in-group favoritism, where participants who have strong national identities show stronger in-group favoritism than participants who have weak national identities.

Hypothesis 2: Respondents who display a strong national identity (a) perceive it as more appropriate to use personal information to identify and prevent terrorist attacks than respondents displaying a weak national identity (national identity) and (b) display stronger in-group favoritism (interaction of national identity × citizenship).

Privacy Concerns for Personal Information and In-Group Favoritism

Research indicates that concerns about privacy vary across both people and situations, similar to other judgments and perceptions that reveal a situation × person interaction (see Lewin, 1935). Situationally, individuals tend to distinguish between private spaces and public spaces, being more opposed to surveillance in areas they deem private (see van Heek et al., 2014), and personally, some individuals have higher levels of general concern for privacy than others do (Crow et al., 2017; Newell, 2016). Consistent with other situation × person approaches (Lewin, 1935), individual differences can be expected to vary across situations. Specifically, some research suggests that individual differences regarding
privacy concerns are heightened in private spaces and are mitigated in public spaces (Pavone & Esposti, 2010).

In general, privacy concerns are particularly strong for sensitive information. People tend to be more hesitant to share sensitive information, like health information relating to a cancer diagnosis or financial information, compared to less sensitive information like blood pressure or demographic data and opinions (Dhagarra et al., 2020; Safaeimanesh et al., 2021). Swani et al. (2022) found similar concerns for online information being scraped for marketing purposes.

Online information can be more or less sensitive, depending on where it is posted and shared. Information that is made to be public, such as information placed on websites or social media, is generally less sensitive than personal information sent in more private channels, such as through email or other personal online conversations. Knowing that people are more protective of more sensitive information, we expected that there would be higher support for the use of publicly available information, compared to private information. Similar trends have been seen in the context of camera surveillance, where people were generally in favor of the security that cameras bring in public areas but were more resistant to their use in private spaces (van Heek et al., 2014). This effect was qualified by the level of threat, though, where areas that were more threatened, even if also more private, were seen as better areas for camera surveillance (Pavone & Esposti, 2010). The latter finding suggests that some individuals may well be in favor of surveillance of even private online information under the significant threat of a terrorist attack. Considering these previous studies, we expected that support for using public online information from individual persons to analyze internet-based terrorist activity would differ overall from support for using private personal information (Hypothesis 3) and that there will be individual differences in the support for the usage of private personal information (Hypothesis 4).

Hypothesis 3: 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).

Although there is variance in privacy concerns across different types of information and situations, there are also stable individual differences. For example, Crow et al. (2017) observed a relationship between privacy concerns and support for police body cameras, though the majority of people believed that these cameras were not an invasion of privacy and were worth potential risks. At times, experts, such as police officers, have expressed concern for privacy issues with body cameras (Newell, 2016). Research also indicates that females are often more cautious about online privacy than their male counterparts, and people who are wealthier and more educated show higher concern for online privacy (Y. Kim et al., 2018). Personality traits have been shown to be related to privacy concerns also: Agreeableness and conscientiousness were both associated with increased concerns for online privacy in areas such as online banking, online shopping, and social media (Y. Kim et al., 2018).

To the extent that participants’ general and internet-related privacy concerns also apply to the use of personal information that is collected to identify terrorist threats, it can be expected that respondents who are more concerned about privacy online, compared to those with fewer concerns, will be less supportive of the use of personal information for deciphering terrorist activities. As a function of information type, we also expected that these differences in privacy concerns will be stronger for private online information, as opposed to public online information, describing a situation \( \times \) person interaction.

Hypothesis 4: (a) Compared to respondents with low privacy concerns, respondents who have high privacy concerns find it less appropriate to use personal information for counter-terrorism purposes (privacy concerns). (b) This difference is larger for private than for publicly available information (privacy concerns \( \times \) personal information).

We expected that participants will show an overall effect of in-group favoritism (Hypothesis 1), and that this effect will be stronger for individuals with a strong national identity (Hypothesis 2). To the extent that participants are more concerned about private than public personal information, in-group favoritism was expected to be stronger for private personal information than for publicly available personal information. Respondents were anticipated to show more concern for private than for public personal information (Hypothesis 3), in particular individuals with high privacy concerns (Hypothesis 4). Following the introduced social-identity account, Reimer and Johnson (2022) expected and found that the factors that are involved in the first four hypotheses, interact with each other in that a specific combination of conditions increases ingroup favoritism regarding personal information. Past research suggests that the centrality of a group for one’s identity as well as the perceived relevance of the evaluative dimension on which groups are compared affect ingroup favoritism (Aronson et al., 2018; Tajfel & Turner, 1986). Accordingly, Reimer and Johnson (2022) expected and found stronger ingroup favoritism when private personal information was being used and people had high general privacy.
concerns, compared to situations where privacy concerns were relatively low. Moreover, participants who were particularly concerned about their privacy displayed especially high in-group favoritism if they showed strong national identities.

These considerations provided the rationale for Hypothesis 5, which we aimed to replicate.

Hypothesis 5: (a) In-group favoritism is stronger for private than for public personal information (citizenship × personal information). (b) In-group favoritism for private information is particularly pronounced for respondents who have strong privacy concerns (citizenship × personal information × privacy concerns). (c) The in-group favoritism for private information is particularly strong for respondents who have strong privacy concerns and national identities (citizenship × personal information × privacy concerns × national identity).

Method
To test the proposed hypotheses, participants were provided with descriptions of several different possible terrorist attacks. Participants were asked to describe their view of the appropriateness of using probabilistic computing technologies to prevent attacks similar to each one described by way of analyzing personal information. Although probabilistic computing was the context of interest and the motivation for the study, the actual measures used in the study to assess participant opinions did not require understanding the technology itself. Participants needed to understand that the new technology increases the probability to identify terrorist threats and that online information was under consideration for using to stop terrorism. In addition, we took a measure of the age, income, education level, and political orientation for each participant. The instructions and measurements were based on the study by Reimer and Johnson (2022). Different from Reimer and Johnson (2022), who used only one scenario of a possible terrorist attack, participants were provided with five different scenarios that were adapted from Liu et al. (2019).

Participants
To test the proposed hypotheses, we used Amazon’s Mechanical Turk (MTurk) to recruit participants to a study conducted on Qualtrics. All participants of the study were U.S. citizens who signed up for this specific study only. Participants received a compensation of 1.25 USD for their participation. The median completion time of the study was 11.5 min. We followed practices described in the scientific literature in order to achieve high quality data. Analyses of participants from MTurk have shown samples from MTurk to be more representative than common convenience samples (Buhrmeister et al., 2016) and produce as high of validity as college samples, social media samples, or other online sources (Berinsky et al., 2012; Casler et al., 2013; Clifford et al., 2015). Similarly, Hauser and Schwarz (2016) showed that MTurk participants passed attention checks better than college students and followed instructions more accurately. Although insufficient attention to the task or survey is a problem in any data collection scenario, Thomas and Clifford (2017) found no evidence that inattention is a bigger problem for MTurk, compared to other convenience sampling techniques.

We took two specific measures to obtain high quality data. First, participants had to have at least a 95% previous approval rating to qualify for the study. Second, we included a unique, unobtrusive attention check, following the recommendation of Thomas and Clifford (2017) (see also B. Kim & Schuldt, 2018).

Of the 1,204 participants, seven participants were not living in the United States, and six failed the attention check item. The analyses were conducted after excluding those 13 participants, leaving 1,191 usable responses. Participant demographics are presented in Table 1, along with data from the U.S. census for comparison purposes (United States Census Bureau). Of the 1,191 participants, 719 (60.4%) were male. Participants were between 18 and 79 years old (M = 37.23; SD = 12.10). When asked for their highest degree and education, 55.8% (665) of participants included a unique, unobtrusive attention check, following the recommendation of Thomas and Clifford (2017) (see also B. Kim & Schuldt, 2018).

Of the 1,204 participants, seven participants were not living in the United States, and six failed the attention check item. The analyses were conducted after excluding those 13 participants, leaving 1,191 usable responses. Participant demographics are presented in Table 1, along with data from the U.S. census for comparison purposes (United States Census Bureau). Of the 1,191 participants, 719 (60.4%) were male. Participants were between 18 and 79 years old (M = 37.23; SD = 12.10). When asked for their highest degree and education, 55.8% (665) of participants included a unique, unobtrusive attention check, following the recommendation of Thomas and Clifford (2017) (see also B. Kim & Schuldt, 2018).

Procedure and Design
Participants were provided a survey that described five different hypothetical terrorist attacks, such as an armed attack or an explosion of a bomb. The descriptions of the attacks were adapted from Liu et al. (2019). In addition to varying the type of attack, the location of the attack was varied, such that participants responded to each attack based on whether the hypothetical attack was planned inside the U.S. or outside the U.S. The attack type and location were varied within subjects; thus, all participants responded to all ten unique attack situations (see Table 2 for an example). For each attack, participants were asked to assess how appropriate it would be to examine different information sources as a countermeasure to prevent the described attack.

The survey began with a description of probabilistic computing technologies and their potential to help the U.S. government identify and prevent terrorist threats by analyzing online data. The survey then briefly explained...
the nature of online terrorist communication as hidden or disappearing messages through email, texting, chat rooms, or online gaming, all of which run enough data through at once, making the communication difficult to track. Next, participants were given a number of possible actions that could be taken to track online terrorist communication and were asked to give their opinion on how appropriate this tracking would be to prevent each of the ten described terrorist attacks. Specifically, for each of the ten scenarios, the survey measured participants’ support for the usage of private and public personal information from U.S. citizens and non-U.S. citizens who either live in the U.S. or abroad, resulting in eight questions per scenario (see Table 2).

In a next step, participants were asked for their general support for counter-terrorism measures, their general and internet-specific privacy concerns, national identity, and political orientation. Subsequently, participants were categorized based on their reported general privacy concerns (high, moderate, low) and national identity (strong, weak; see details below). The underlying design involved the following factors: Type of attack (biological weapon, armed attack on civilian or military personnel, explosion of a bomb at a public place, airline attack similar to 9/11); location of attack (U.S. or abroad); used personal information (private vs. public); citizenship of information source (U.S. citizen vs non-U.S. citizen), and residence of information source (U.S. vs. abroad), yielding a $5 \times 2 \times 2 \times 2 \times 2$ design. These factors were varied within participants. Overall, each participant made 80 judgments (see Table 2 for an example). In addition, participants’ national identity (strong, weak) and privacy concerns (high, moderate, low) were included in the analyses and test of hypotheses as between-subjects factors.

### Measurements

#### Counter-Terrorism Efforts

Two measures of counter-terrorism efforts were used. First, participants indicated their level of agreement for using personal information by the U.S. government to identify terrorist threats. Second, we used a measure from Hinsz and Betts (2014) on the support of general counter-terrorism efforts. Whereas the first measure asked participants to evaluate the appropriateness of using each of the eight different types of personal information to prevent each of the ten described terrorist threats, the second measure consisted of five items that ascertained participants’ general attitudes toward counter-terrorism efforts.

#### Use of Personal Information

The first scale measured support for the use of eight different types of personal information with the goal to prevent each of ten different terrorist attacks, rated on a seven-point, Likert scale (1, strongly disagree, to 7, strongly agree). Each item began with, “Probabilistic computing is analyzing very large amounts of information to decipher and identify suspicious activities.” The ten scenarios differed in the underlined part of the following question: “How appropriate would the following actions be to stop the following threat from happening in the U.S.: A cyber-attack on the
nation’s power grid?’’ The five unique attacks were adapted from Liu et al. (2019) and included (1) an attack with a biological weapon, (2) an armed attack on civilian or military personnel, (3) an explosion of a bomb at a public place, and (4) an airline attack similar to 9/11. Each of these five hypothetical attacks was situated as either “in the U.S.” or “outside the U.S.” for a total of ten scenarios. The ten scenarios were presented to each participant in the same order.

For each of the ten scenarios, respondents were presented eight different types of personal information (see Table 2). For each of the eight types of personal information, respondents were asked to indicate their agreement (1, strongly disagree, to 7, strongly agree) with how appropriate it would be to use that information. An example item read, “It would be appropriate to examine publicly available websites and social media of U.S. citizens living in the U.S.” Four of the eight items addressed private information: “to examine email and other private online conversations,” and four items addressed public information: “to examine publicly available websites and social media.” The private information item was adapted from Williamson (2019), and the public information item was taken from Reimer and Johnson (2022). These two types of information were further broken into four different owners of the information: “of U.S. citizens living in the U.S.,” “of U.S. citizens living outside the U.S.,” “of non-U.S. citizens living in the U.S.,” and “of non-U.S. citizens living outside the U.S.” Thus, each participant responded to a total of eight items that measured their support for using personal information. This followed a $2 \times 2 \times 2$ design, including the factors personal information (private vs. public), citizenship (U.S. citizen vs. non-U.S. citizen), and residence (U.S. vs. abroad). Each of these eight items was completed for each of the ten hypothetical attacks, for a total of 80 responses.

Table 2. Measure of Acceptance of Use of Personal Information.

<table>
<thead>
<tr>
<th></th>
<th>Strongly agree</th>
<th>Moderately agree</th>
<th>Slightly agree</th>
<th>Neither agree nor disagree</th>
<th>Slightly disagree</th>
<th>Moderately disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>to examine publicly available websites and social media of U.S. citizens living in the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine publicly available websites and social media of U.S. citizens living outside the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine publicly available websites and social media of non-U.S. citizens living in the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine publicly available websites and social media of non-U.S. citizens living outside the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine email and other private online conversations of U.S. citizens living in the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine email and other private online conversations of U.S. citizens living outside the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine email and other private online conversations of non-U.S. citizens living in the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>to examine email and other private online conversations of non-U.S. citizens living outside the U.S.</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

Counter-Terrorism Efforts. The second counter-terrorism support measure contained five items, adapted from Hinsz and Betts (2014), to measure attitudes toward counter-terrorism efforts. All items were on the same seven-point Likert scale as before. The five actions were “I support the development and implementation of new technology that aids counter-terrorism efforts,” “More should be done to acquire information that aids counter-terrorism efforts,” “More money should be spent on efforts geared toward preventing terrorism,” “More skilled workers that are involved in counter-terrorism
efforts should be hired.” “Relaxed counter-terrorism policies should be reviewed more carefully.” Unlike the first measure of participants’ perceptions of counter-terrorism efforts that referred to the use of personal information, the second, general measure, was administered only once as the following measures on privacy, national identity, and political orientation.

Privacy Concerns. This section assessed general privacy concerns, focused on the security risk of putting private information online. The same seven-point Likert scale was used as before. Two items were adapted from Misis et al. (2017): “I do not mind giving up my right to privacy” and “I do not mind giving up my protection against unreasonable search and seizure.” In addition, four items were adapted 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,” and “Overall, the internet is a safe place to transmit sensitive information.”

Responses were reverse coded and integrated into one measure of privacy concerns by averaging each participant’s responses (Cronbach’s $\alpha = .91$). Values in this composite measure can vary between 1 and 7, with a 7 indicating strong privacy concerns. Subsequently, responses were ordered according to levels of concern for online privacy and divided into three equally sized groups: high ($M = 6.37; SD = 0.45; N = 390$), moderate ($M = 4.64; SD = 0.51; N = 384$), or low ($M = 2.64; SD = 0.73; N = 417$) privacy concerns. The three groups significantly differed from each other in their privacy concerns ($F(2,1198) = 56.51; p < .01$).

National Identity. Six items taken from Huddy and Khatib (2007) were used to measure national identification: “How important is being American to you?” (1, not at all important, to 7, extremely important). “To what extent do you see yourself as a typical American?” (1, not at all, to 7, completely), “How well does the term American describe you?” (1, not at all well, to 7, extremely good), “When talking about Americans, how often do you say ‘we’ instead of ‘they’?” (1, never, to 7, always), “How good does it make you feel when you see the American flag flying?” (1, not at all good, to 7, extremely good), “How good does it make you feel when you hear the national anthem?” (1, not at all good, to 7, extremely good). Responses to the six items correlated highly with each other and were integrated into one composite measure of national identity (Cronbach’s $\alpha = .93$). Participants’ responses were then split into two groups using a median split, resulting in a group with strong national identity ($M = 5.98; SD = 0.75$) and a group with weak national identity ($M = 3.22; SD = 0.93; t(1189) = 56.51; p < .01$).

Political Orientation. To measure political orientation, four items were borrowed from Mehrabian (1996): “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.” All four items were measured on the same seven-point Likert scale (1, strongly disagree, to 7, strongly agree) (Cronbach’s $= .85$).

Demographics. For demographic information, participants were asked to indicate their age and gender, which state they live in, and basic education and household income information.

Results

Table 3 provides the overall means, standard deviations, and correlations for the main measures, along with participants’ age, and Table 4 presents the means and
standard deviations of participants’ expressed support to use personal information separately for the main conditions of the study. As expected, the study demonstrated significant in-group favoritism when considering using personal online information for counter-terrorism efforts. The proposed hypotheses on the perceived appropriateness of using online information from individuals were tested using a MANOVA, with citizenship (U.S. citizen vs. non-U.S. citizen), personal information (public vs. private), and residence (U.S. vs. abroad) included as within-subjects factors and national identification (strong/weak) and privacy concerns (high/moderate/low) as between-subjects factors. Thereby, within each of the eight conditions of citizenship \times personal information \times residence, participants’ responses were aggregated across the ten different scenarios.

All five hypotheses were supported. Figures 1 and 2 show levels of participant support for using personal information based on the individual’s location as in or out of the U.S., on the type of information as public or private, and on general level of privacy concern. In support of Hypothesis 1, respondents showed lower support for using U.S. citizens’ personal information ($M = 4.83; SD = 1.29$) compared to non-U.S. citizens ($M = 5.11; SD = 1.27$) (main effect citizenship, $F(1,1184) = 159.32; p < .01$). In support of Hypothesis 2a, respondents displayed more support for the use of personal information when they had a strong national identity ($M = 5.31; SD = 1.21$), compared to those who expressed weaker national identity ($M = 4.63; SD = 1.23$) (main effect national identity, $F(1,1184) = 97.47; p < .01$). Moreover, respondents with strong national identity showed
Figure 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 (U.S. citizen/Non-U.S. citizen).

Note. This figure shows support for using either U.S. citizens’ or non-U.S. citizens’ personal information for counter-terrorism efforts, separately 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.

Figure 2. Support for the usage of private personal information by respondents varying in their general privacy concerns and national identification.

Note. This figure shows support for using either U.S. citizens’ or non-U.S. citizens’ private information for counter-terrorism 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.
stronger in-group favoritism than those with weak national identity, supporting Hypothesis 2b (see Table 4; interaction national identity × citizenship, \( F(1,1184) = 36.09; p < .01 \)).

In line with the third hypothesis, respondents were more favorable toward using publicly available personal information (\( M = 5.63; SD = 1.29 \)), rather than private personal information (\( M = 4.31; SD = 1.69 \)) for terrorist threat identification (main effect personal information, \( F(1,1184) = 825.10; p < .01 \)). In support of Hypothesis 4a, respondents who were highly concerned about privacy were less supportive of the overall use of personal information for counter-terrorism (\( M = 4.52; SD = 1.75 \)) than respondents who were moderately concerned (\( M = 4.96; SD = 1.50 \)) or had low concerns (\( M = 5.39; SD = 1.17 \); main effect privacy concerns, \( F(2,1184) = 55.77; p < .01 \)). As predicted by Hypothesis 4b, there was an interaction between type of personal information and concern for privacy indicating that the difference in support for the use of personal information due to privacy concerns was larger for private information than for publicly available information (interaction personal information × privacy concerns, \( F(2,1184) = 129.62; p < .01 \)). This is shown in Figure 1 and Table 4.

Supporting Hypotheses 5a and 5b, in-group favoritism for the use of personal information was particularly pronounced (interaction citizenship × personal information, \( F(1,1184) = 158.75; p < .01 \)) for participants high in concern for privacy (interaction citizenship × personal information × privacy concerns, \( F(2,1184) = 23.16; p < .01 \)).

In support of Hypothesis 5c, the strongest in-group favoritism occurred for private information among respondents with high national identity and strong privacy concerns (interaction citizenship × personal information × privacy concerns × national identity, \( F(2,1184) = 6.20; p < .01 \)). The residence of the source of this information (U.S. vs. abroad) did not qualify this four-way interaction (\( F < 1 \)).

**Discussion**

In 2016, the U.S. government took Apple to the Federal court to try and force Apple to allow them into the private phone of an attacker in the mass shooting at San Bernardino, California (Perlroth, 2019). Apple refused to fulfill the request, being concerned about this concession opening up a door of opportunity for the government to begin more and more invasive surveillance. The New York Times (Perlroth, 2019) reports this long-lasting power struggle as an ongoing battle between big tech companies and the U.S. government. This raises an important question for the prevention of terrorist attacks. How much of their right to privacy are people willing to give up in order to counteract terrorist activities?

The conducted study revealed several findings regarding public support for counter-terrorism efforts by monitoring online personal data. Overall, respondents were significantly in favor of using personal websites or social media to increase the detection of terrorist activity. As expected, respondents showed in-group favoritism toward U.S. citizens, agreeing more to use out-group member information (non-U.S. citizens) than in-group member information (U.S. citizens). Support for the use of private online information from email conversations and other private conversations varied significantly based on whose information it was and on individual differences of national identity and privacy concerns. The study builds on the findings of Reimer and Johnson (2022) by replicating the observed in-group favoritism in a new sample of participants and by demonstrating that the observed effect is not limited to a specific terrorist attack but holds across a variety of terrorist attacks (see Liu et al., 2019). The observed in-group favoritism regarding the surveillance of private information describes a new form of in-group favoritism and adds to our understanding of public assessments of the use of private information and the role of privacy concerns in the use of surveillance technologies.

Social identity theory posits that responses to a stimulus can differ based on the salience of an individual’s group identity (Tajfel & Turner, 1986), particularly when the person’s group identity is strong (Aronson et al., 2018). Generally, in-group favoritism is shown when individuals have more favorable opinions and responses toward their own group than toward an out-group (Tajfel & Turner, 1986). In-group favoritism has been demonstrated across a wide array of groups and behaviors including the willingness to cooperate with others and to share information (Balliet et al., 2014; Guo et al., 2022; Hogg & Ridgeway, 2003; Hornsey, 2008). The current study adds to the literature on in-group favoritism in that it links in-group favoritism to privacy concerns and the perceived appropriateness to use personal data. The description and analysis of public support for counterterrorism support has only been done from a social-scientific approach by a few studies (Hinsz & Betts, 2014; Lum & Kennedy, 2012; Reimer & Johnson, 2022). This is one of the first studies that demonstrates the impact of privacy concerns on in-group favoritism.

The strongest support for the use of private data was observed for respondents who simultaneously identified strongly with the U.S. nationally and were less concerned about online privacy. As shown in Figure 2 and Table 4, their average support was 5.54 (SD = 1.41) on a seven-point scale, while the lowest support was more than 2.5 points lower on the same scale, found among those
with strong concerns for privacy and weak national identities. Actual in-group favoritism was most strongly seen for participants with high levels of both national identity and privacy concern, while the lowest level was found among those that, while high in privacy concerns, only weakly identified with the U.S.

The observed differences between experimental conditions and groups of participants are quite strong. Although there are political dimensions related to computer and information technologies, the results of the presented study suggest that public support for using probabilistic computer technologies for counter-terrorism cannot be reduced to political partisanship or national identity. Respondents’ political orientation was only mildly correlated with both national identity and general privacy concerns, and age was not strongly related to the use of personal information, concerns for privacy, or national identification (see Table 3).

The scope of the tested hypotheses and their intended applications (Balzer et al., 1989) concerns scenarios where potential terrorist threats unambiguously connect to a country and where the access to personal information is clearly referring to one’s own government doing the accessing. Support for counter-terrorism efforts by collecting personal information with probabilistic computing may also depend on the level of trust an individual has toward both the agent that is collecting the data and those who are benefiting from the efforts. This study suggests that American citizens may find the use of probabilistic computer technologies to access personal online information by the U.S. government acceptable overall. However, future studies could examine other agents that may be more or less trusted, like other countries’ governments or non-government organizations like private corporations, to examine whether those agents would also be trusted with collecting similar data (also see Reimer & Johnson, 2022).

The presented study has several limitations. First, participants were asked how they would behave to prevent hypothetical scenarios in which probabilistic computing technologies would be used to identify and thwart terrorist threats. Future research may delineate if support for the use of personal information varies depending on the salience of possible terrorist threats. As research on surveillance suggests (van Heek et al., 2014), support for the use of personal information may be higher in situations in which people perceive the risk of a terrorist attack to be very high. Another limitation consists in the use of an MTurk sample that is not representative of the total population. We tested the observed differences regarding privacy and in-group favoritism across several demographic characteristics including income, education, and age, and the effect was not qualified by these differences, nor were any of these demographic characteristics strongly correlated with support for the use of personal online information. Future studies may test the robustness of the reported results across different measurements and samples of participants to determine the generalizability of the results. The observed differences matched the results of Hinsz and Betts (2014) and Reimer and Johnson (2022), where participants read about a fictitious terrorist attack in a newspaper article and responded to similar counter-terrorism measures. In the current study, each participant provided judgments on ten different scenarios, whereas the study by Reimer and Johnson (2022) used a between-subjects design in which each participant read only about one scenario. Both studies found strong support for the proposed in-group favoritism on the use of personal information. Thus, the current study adds to the expected reliability and robustness of the observed in-group favoritism and speaks to the generalizability across several scenarios and descriptions of terrorist threats.

This study focused on probabilistic computer technology that offers potential to identify and prevent terrorist attacks by monitoring large amounts of personal online information. Future research may test if public support differs in situations in which the p-bits technology is used for other purposes. It may be that the overall support for the use of personal information would be smaller when used for financial or marketing purposes. At the same time, the reported ingroup favoritism related to the access of personal information may well hold across areas in which society can benefit from processing personal information including public health and societal risks beyond the threats of terrorism.

Acknowledgments
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. We thank Verlin Hinsz and Kevin Betts for sharing their study materials, instructions, and measurements with us.

Declaration of Conflicting Interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study was funded through a Purdue 2.0 Big Challenge award by Purdue University.

Ethics Statement
All study materials and procedures and the informed consent form of the study were approved by Purdue University’s Institutional Review Board.
ORCID iDs
Torsten Reimer https://orcid.org/0000-0002-7419-0076
Nathanael Johnson https://orcid.org/0000-0003-2466-5165

References

Levy, I., & Rozmann, N. (2022). Differences in attitudes toward terrorists: Type of terrorist act, terrorist ethnicity, and
observer gender and cultural background. Group Processes and Intergroup Relations, 26(2), 476–492.


