AJPM FOCUS
INCLUSIVITY IN PEOPLE, METHODS, AND OUTCOMES
RESEARCH ARTICLE

Impact of Privacy Messaging on COVID-19 Exposure Notification App Downloads: Evidence From a Randomized Experiment

Laura A. Gibson, PhD,[1] Erica L. Dixon, PhD,[1] Marissa A. Sharif, PhD,[2] Anyara C. Rodriguez, BA,[1] Joseph N. Cappella, PhD[3]

Introduction: Digital contact-tracing smartphone apps have the potential to slow the spread of disease but are not widely used. We tested whether messages describing how a COVID-19 digital contact-tracing app protects users' privacy led to increased or decreased intentions to download the app by either calming privacy concerns or increasing their saliency.

Design: Randomized controlled trial.

Setting/participants: We recruited adult smartphone owners in the U.S. (oversampled for younger adults aged 18−34 years) in November 2020 through an online panel.

Intervention: Survey software randomly assigned 860 participants to 1 of 2 parallel messaging conditions (n=430 privacy assured, n=430 no privacy described).

Main outcome measures: 4-point scale of intention to use the app "if public health officials released a COVID Exposure Notification app in their state" that averaged likelihood to (1) download and install the app on their phone; (2) keep the app active on their phone; and (3) keep Bluetooth active on their phone (needed for the app to work).

Results: After removing incompletes, those who failed the manipulation checks, or those who had already downloaded a COVID-19 digital contact-tracing app, we analyzed 671 participants (n=330 privacy, n=341 no privacy) in 2021. There was no relationship between privacy condition and download intention ($mean_{privacy}$=2.69, $mean_{noprivacy}$=2.69, b=0.01, 95% CI= −0.13, 0.15, p=0.922) but also no evidence that describing the app's security increased context-dependent privacy concerns (measured 3 ways). Instead, we found increased endorsement of data security in the privacy condition using a scale of beliefs about the app keeping privacy secure ($mean_{privacy}$=2.74, $mean_{noprivacy}$=2.58, b=0.16, 95% CI=0.04, 0.28, p=0.009, small effect ω^2=0.009).

Conclusions: This study provides some evidence that people developing contact-tracing messaging campaigns do not need to worry that describing a digital contact-tracing app's privacy protections will backfire. Future mixed methods testing of messages about who has access to information—and for how long—may uncover new communication strategies to increase public trust in contact-tracing apps.

From the [1]Department of Medical Ethics and Health Policy, Perelman School of Medicine, University of Pennsylvania, Philadelphia, Pennsylvania; [2]Marketing Department, Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania; and [3]Annenberg School for Communication, University of Pennsylvania, Philadelphia, Pennsylvania

Address correspondence to: Laura A. Gibson, PhD, Department of Medical Ethics and Health Policy, Perelman School of Medicine, University of Pennsylvania, 1105B Blockley Hall, 423 Guardian Drive, Philadelphia PA 19104. E-mail: gibla@pennmedicine.upenn.edu.

2773-0654/$36.00
https://doi.org/10.1016/j.focus.2022.100059

Trial registration: This study is registered with AsPredicted#51826
AJPM Focus 2023;2(1):100059.

INTRODUCTION

Digital contact-tracing efforts implemented through smartphone apps have the potential to slow the spread of coronavirus disease 2019 (COVID-19) but have not been widely embraced by the public. These apps anonymously log and rapidly report to other app users when someone they have recently been in contact with is diagnosed with a disease to prevent further disease transmission. For diseases such as COVID-19 with high transmission rates and a high proportion of transmission from presymptomatic individuals, digital contact tracing may address the speed and labor constraints of manual contact tracing.[1−3] However, their success depends on widespread use (estimates range from 15% to at least 60% uptake)[1,3,4] and routine testing (at least 10% of the population).[5] In 2020, median penetration of voluntary apps was only 6% in non-U.S. countries (ranging from <1% in Mexico to 45% in Finland) and 5% in the U.S. (ranging from <1% in California to 56% in the District of Columbia).[6] Despite apps launching across the globe, some ascribe the lack of widespread adoption to privacy concerns.[7−11] Communicating an app's security through public-service announcements (PSAs) has the potential to alleviate those concerns.

COVID-19 digital contact-tracing apps vary in whether they are voluntary, disguise or anonymize user data for their privacy, include a pledge to stop tracking and destroy the data once COVID-19 is under control, or have limitations on how the data can be used.[6] All U.S. apps meet these conditions except a small minority whose policies are not as clear in data-use limitations (3 of 29 as logged by MIT's COVID-19 tracing tracker[6]). Worldwide, 43 digital contact-tracing apps are connected to the Google/Apple API, and nearly every U.S. COVID-19 digital contact-tracing app uses the Google/Apple API (25 of 29). Competitors Google and Apple took privacy concerns seriously when they joined forces to design their Exposure Notifications System for COVID-19 digital contact-tracing apps.[12] They use Bluetooth to sense when another phone with the app is close by (usually within 6 feet) for a period of time (usually 15 minutes), but that information is anonymous, does not include location information, and is only stored on the user's phone for 14 days. If a user tests positive, they actively choose to alert potential close contacts. This decentralization limits the app's effectiveness at assessing larger disease patterns but ensures privacy. A conjoint experiment conducted with 2,000 Americans found that decentralized data architecture (relative to centralized) increased intentions to download an exposure app and was the only significant predictor among 6 attributes.[13]

For contact-tracing apps (such as the Google/Apple API) that bake in privacy through decentralization, what beliefs about the apps will convince people to use them? There are no labels in U.S. generic app stores indicating which apps protect privacy effectively. Would marketing an app's privacy protections reduce that uncertainty and allay concerns or just increase the saliency of privacy as an issue? Because privacy preferences are malleable and context dependent,[14] it is possible that PSAs describing a particular app's privacy protections could reduce privacy concerns, increase feelings of safety, and potentially lead to more downloads. This would support the idea of privacy calculus: download decisions are influenced by weighing the costs of losing privacy and the benefits of the app.[15] A few studies have shown that contextually dependent perceptions of privacy increase intentions to download apps to some extent.[16−19] Conversely, messages about an app's privacy protections might backfire by making privacy concerns about the app more salient, thereby increasing privacy concerns, reducing feelings of safety, and reducing downloads.

Some think that privacy calculus is too simplistic of an explanation and instead suggest that most people are actually apathetic or resigned to losing privacy to apps.[20−22] In this case, PSAs meant to influence privacy concerns or perceptions of app safety by describing the app's privacy protections would have no impact on app downloads. One previous study using 2-minute educational videos to inform German participants about the privacy of a COVID-19 contact-tracing app did not show differences in downloads on the basis of seeing the video or in generic privacy concerns.[11] However, it did not measure context-dependent privacy concerns, and participants were recruited from a panel who had already agreed to have passive tracking on their phones, so findings might not generalize.

We explored whether and how messages about privacy influence intentions to download a contact-tracing app. First, to support the development of future PSAs,

we examined descriptive analyses about (1) general COVID-19 digital contact-tracing app concerns and (2) the entities that people are most concerned about having access to their personal data in this context. Next, we compared people's responses to a message that explained how the app keeps information private with their responses to a message that did not. Research Question (RQ) 1 asked whether privacy messages impact download intentions. RQ2 asked whether privacy messages increase or decrease privacy concerns (RQ2a) and perceptions of data security (RQ2b) (which are inversely related to one another) and, if so, whether those perceptions are associated with download intentions.

In addition, we examined how the framing of the message might interact with the presence versus the absence of privacy information (RQ3). In particular, we varied whether the message was framed in terms of gains, losses, or neither. Previous research found that people's decisions are often influenced by how they are framed.[23,24] People will avoid risks when considering the potential gains but take risks when considering the potential losses. If privacy information affects perceptions of app safety and thus the potential risk of downloading the app, the framing of the message may interact with the presence of this information in influencing downloads.

METHODS

Study Sample

The survey-sampling company, Dynata, recruited 860 U.S. participants who reported having a smartphone through nonprobability opt-in web panels from November 10 to 12, 2020. They completed an online survey through Qualtrics and were compensated with Dynata's usual panel incentives, which can be redeemed for a range of non-cash options (e.g., gift cards, charitable contributions, other options). This study was preregistered through AsPredicted.org (Appendix A, available online). Power analyses using the average intentions to download the app from a previous study with Delaware residents calculated that 600 participants were needed (300 per condition) to detect a quarter-point increase in that intention (on a 4-point scale) with 0.80 power and a 2-tailed alpha of 0.05. We oversampled young adults (aged 18−34 years) to be half of the sample so that there would be enough cases to conduct analyses within age category subgroups. Twenty participants (equally distributed between the 2 groups) were excluded because they did not complete the survey. We used attention checks specified in the preregistration to exclude participants if they did not know what month it was or if they completed the task too quickly (faster than a quarter of the median length). After removing those who failed the month check (n=57 [7%]; privacy n=30, no privacy n=27), no participants completed the task too quickly. Although not preregistered, we also dropped participants who reported that they already downloaded a COVID-19 exposure notification app (n=112 [13%]; privacy n=60, no privacy n=52) because their responses are not a good test of how effective a message will be at changing people's intentions, leaving a final sample of 671 (Appendix B, available online, for the full CONSORT diagram). The University of Pennsylvania IRB determined that this study was exempt, and the Delaware Department of Health and Social Services Human Subjects Review Board determined that it did not need a formal board review.

Intervention

For the privacy factor, Qualtrics randomly assigned participants to see either a message containing a description of how their information is kept private with COVID-19 Exposure Notification apps (n=430, analysis n=330) or a message with that privacy information removed (n=430, analysis n=341). Specifically, the privacy condition message included "[The app] protects your privacy and keeps your data safe and secure. How does it work? Bluetooth senses when you are in close contact with someone else with the app and stores that information only on your phone, without locations or names, for 14 days. If you test positive for coronavirus, you decide what to do with this information." For the framing factor, privacy was crossed with 3 levels of framing (gain, loss, or no gain/loss frame) (for the full set of messages, see Appendix C, available online).

Measures

The preregistered primary outcome (used for RQ1 and RQ3) was a scale of intention to use the app "if public health officials released a COVID-19 Exposure Notification app in their state" that averaged the likelihood to (1) download and install the app on their phone, (2) keep the app active on their phone, and (3) keep Bluetooth active on their phone (needed for the app to work) (1=*definitely will not*, 4=*definitely will*).

We assessed whether message condition predicted context-dependent privacy concerns (RQ2a) using 3 items. One was a Likert scale: the amount of concern about using the app (1=*not at all concerned*, 4=*very concerned*). Among those who reported anything more than *not at all concerned* about using the app, one free-response question asked them to describe their concerns. One rater inductively read through a subset of open-ended responses to generate the 16 categories (one of which was privacy) that 2 independent raters used to categorize the full data set. The 2 raters resolved disagreements by consensus. After the free-response question, participants answered a closed-ended question about what concerned them the most (e.g., privacy and security, battery drain, etc.). Both the free-response and closed-ended privacy responses were transformed into binary variables, coded 1 if concerned about privacy, or 0 if they were not. For participants with closed-ended responses indicating that they were most concerned about privacy, we also asked who they were most concerned about having access to their information.

We assessed whether message condition predicted the perceptions of context-dependent data security (RQ2b) with 2 measures: a privacy belief scale and whether they wanted to learn more about how the app keeps data secure and private (1=*yes*, 0=*no*, where 0 indicates more perceptions of security). The privacy belief scale averaged responses to (1) their information will be kept

secure, (2) they will be the only one who can upload their data to the health department, and (3) it will not store location information, if they download and install a COVID-19 Exposure Notification app recommended by public health officials in the next 2 weeks (1= *strongly disagree*, 4= *strongly agree*). In contrast to the privacy-related beliefs, we expected that the intervention would have less impact on a pro-app belief scale, which averaged 7 beliefs supporting downloading the app (and unrelated to privacy) on a 1−4 scale.

Participants reported standard demographics: their age, gender, race, ethnicity, the number of people in their household (including whether they live with children or a partner), their highest education level attained, and their political identification. We also measured COVID-19–specific covariates: frequency of engaging in 3 COVID-19 prevention health behaviors in the past 7 days (e.g., masking, social distancing) and how worried they were about someone they know getting COVID-19 (including themselves). We also included 3 categorical items: whether they work some or most days in close contact with people from outside their home, whether they know anyone who is at high risk for complications from COVID-19, and whether they know anyone who had a mild or severe case of COVID-19.

We assessed reactance to the message, perceptions of message effectiveness, a manipulation check, and the amount of exposure to the message. Messages did not differ on these characteristics, so they are not discussed further (Appendix D, available online). The full questionnaire is available in Appendix F (available online).

Statistical Analysis

Our initial analyses summarized the sample and univariate outcomes by condition using means and SDs for continuous and ordinal variables and proportions and frequencies for categorical outcomes. We tested for sample differences between the privacy and no-privacy groups using linear regression for continuous and ordinal variables and chi-square for categorical variables. We then descriptively summarized privacy concerns.

Next, the primary analyses used linear regressions to predict the intention scale from an indicator for privacy condition (1) or not (0) and 2 dummy variables for framing condition (gain [1] versus none [0]; loss [1] versus none [0]) in 3 steps. First, we assessed the individual main effects for privacy (RQ1) in separate linear regressions. Second, we assessed whether the framing condition changed the impact of the privacy condition with an *F*-test of the null hypothesis that the coefficients for the 2 interactions (RQ3, gain framing x privacy and loss framing x privacy) was 0. Third, depending on the outcome of the interaction analyses, we planned to conduct moderation analyses by age category, either examining the main effects for privacy or the interaction, interacting age category with each condition variable. We also used linear and logistic regressions to predict whether exposure to privacy messaging predicted privacy concerns (RQ2a, 1 continuous and 2 binary items), data security (RQ2b, 1 continuous and 1 binary item), or pro-app beliefs unrelated to privacy (discriminant validity test, 1 continuous item). We used chi-square tests to assess the null hypothesis that the condition coefficient predicting pro-app beliefs was the same as any condition coefficient significantly predicting privacy concerns or data security beliefs. Follow-up observational analyses tested whether any significantly predicted beliefs were associated with increased intentions to download the app.

We assessed the univariate associations of each potential confounder and each outcome variable in preliminary analyses (Appendix E, available online). As described in the preregistration, we included potential confounders as covariates if they were associated with any outcome variable (primary or secondary) at $p<0.25$. Analyses were conducted in 2021 using Stata 16.1.

RESULTS

The national sample (N=671) ranged from age 18 to 83 years and was majority female and White (Table 1). The younger age group (18−34 years) had a smaller proportion of White participants, more participants identifying most with Democrats, and more participants with lower education than the older age group. They were also more likely to live with other people (including children) and work in close contact with other people on some or most days.

Descriptive Results: Privacy Concerns

In terms of context-dependent privacy concerns, people reported moderate amounts of concern about the app (mean=2.57, SD=1.05 between those who were a little concerned and those who were somewhat concerned) (Table 2). When asked to describe their concerns about the app in a free-response format, respondents' top concern was privacy (43%, *n*=247), but their second most popular response was having no concerns (35%, *n*=204). Fewer respondents were concerned about the accuracy of app notifications (9%), distrusting the government (7%), or distrusting the app (7%). In closed-ended reports of what they were most concerned about, participants were again most concerned about privacy and security (52%, *n*=351), and the second largest proportion of respondents said that they were not at all concerned (20%, *n*=134). Among the 351 people who reported privacy and security as their top concern in the closed-ended item, most were concerned about the federal government (44%, *n*=156), followed by local government (19%, *n*=67) and Apple/Google (the tech developers) (17%, *n*=60).

Main Analyses

The scale for the main outcome, intention to download the COVID-19 Alert Notification app, hung together well with an alpha of 0.93. Across all conditions, on average, participants were just over the mid-point (2.5) of the likelihood scale on intention to download the app (mean=2.67, SD=1.02) (Table 2). The primary analysis set out in the preregistration (RQ1) showed no significant relationship between privacy condition and download intention ($mean_{privacy}$=2.69, $mean_{noprivacy}$=2.69, b=0.01, 95% CI= −0.13, 0.15, p=0.922) (Table 3). In addition, the set of framing conditions showed no

Table 1. Sample Description by Condition

Characteristics	No privacy (*n*=341)		Privacy (*n*=330)	
	Mean (SD) or proportion	Freq.	Mean (SD) or proportion	Freq.
Age	42.65 (18.26)		41.97 (17.54)	
Female	0.59	201	0.58	189
Race: 4 mutually exclusive categories				
White	0.79	270	0.74	243
Black	0.06	21	0.11	36
Asian	0.08	26	0.10	32
Other/multiple	0.07	24	0.06	19
Hispanic	0.08	28	0.08	26
The political party identified with the most				
Democrat	0.36	123	0.38	124
Republican	0.32	109	0.30	100
Independent/other/none	0.32	108	0.32	106
Highest education				
High school or less	0.28	94	0.27	88
Some college	0.31	107	0.27	89
College degree	0.41	140	0.46	152
Number of people in the household				
1	0.21	71	0.22	73
2	0.35	120	0.32	106
3	0.16	56	0.24	78
4 or more	0.28	94	0.22	72
Work in close contact on some/most days	0.43	147	0.38	124
Live with a partner	0.56	191	0.54	176
At least one child in the household	0.31	105	0.30	99
Did COVID-19–preventive activities (0–3)	2.81 (0.54)		2.80 (0.56)	
Mean past 7-day frequency in engaging in activities: 1=*never*, 4=*every time*	3.26 (0.76)		3.26 (0.82)	
COVID-19 test result[a]				
At least 1 positive (detected) test	0.12	10	0.15	15
All negative (not detected) test(s)	0.87	73	0.84	81
Not sure of the result	0.01	1	0.01	1
High-risk COVID-19 complications				
Do not know anyone at high risk	0.53	181	0.58	192
Only know friends/family at high risk	0.29	100	0.22	72
Self is at high risk	0.18	60	0.20	66
Know COVID-19 cases				
Do not know a case	0.76	259	0.77	253
Had/know only mild cases	0.15	50	0.12	40
Had/know a severe case	0.09	32	0.11	37

Note: There were no significant differences in demographics between the 2 conditions ($p<0.05$).
[a]COVID-19 test results were only reported among those who had been tested (no privacy *n*=84, privacy *n*=97).
Freq., frequency.

significant main effect ($F[2,624]=0.45$, $p=0.64$) or interaction ($F[2,621]=1.14$, $p=0.32$) with the privacy condition (Table 4). Age category did not moderate the main effects of privacy either ($mean_{privacyx18–34}=2.77$, $mean_{privacyx35+}=2.63$, $mean_{noprivacyx18–34}=2.72$, $mean_{noprivacyx35+}=2.66$, b=0.08, 95% CI= −0.20, 0.36, $p=0.59$) (Table 5).

Turning to the secondary outcomes, none of the measures of privacy concerns were predicted by experimental exposure to the privacy message (Table 3 for results and Table 6 for raw correlations). In contrast, for perceptions of security, the privacy belief scale (with a reliable alpha of 0.85) was predicted by experimental exposure to the privacy message ($mean_{privacy}=2.74$, $mean_{noprivacy}=2.58$, b=0.16, 95% CI=0.04, 0.28, $p=0.009$). This corresponds to an ω^2 of 0.009 or a small effect. The discriminant validity test showed that the impact of the

Table 2. Univariate Outcomes by Condition

Outcomes	No privacy (*n*=341)		Privacy (*n*=330)	
	Mean (SD) or proportion	Freq.	Mean (SD) or proportion	Freq.
Main outcome				
Intention to download the app scale (1=*very unlikely,* 4=*very likely*)	2.67 (0.99)		2.68 (1.07)	
Secondary outcomes				
Amount of concern about the app (1=*not at all concerned,* 4=*very concerned)*	2.59 (1.00)		2.55 (1.10)	
Free response: what concerns about app[a]				
Privacy	0.42	126	0.43	121
No concerns	0.32	96	0.38	108
Accuracy of app notifications	0.10	29	0.08	22
Bad government	0.07	22	0.06	18
Distrust the app	0.06	19	0.07	19
Have technical issues	0.03	10	0.02	5
Do not know enough about the app	0.03	9	0.01	3
Don't know (what concerns them)	0.02	7	0.01	4
Distrust all apps	0.02	7	0.01	4
Not enough people will download the app for it to work	0.01	2	0.02	6
Do not need it/COVID-19 is fake	0.02	5	0.01	2
Fear of having COVID-19 if tested	0.01	3	0.01	2
Closed-ended most concerned about				
Privacy and security	0.52	177	0.53	174
Not at all concerned	0.18	60	0.22	74
Not enough people will download the app for it to work	0.19	63	0.16	52
Battery drain	0.09	31	0.07	23
Other	0.03	9	0.02	7
Concerned about whom[b]				
Federal government	0.44	78	0.45	78
Local government	0.19	33	0.20	34
Apple/Google (the tech developers)	0.21	37	0.13	23
Other	0.10	18	0.13	23
Everyone/anyone/all the above		9		16
Hackers		4		2
(Irrelevant)		1		2
Not sure		2		1
Nothing		1		1
Government		0		1
App makers		1		0
Your employer	0.05	9	0.07	13
Your school	0.01	2	0.02	3
Privacy belief scale (1=*strongly disagree*, 4=*strongly agree*)	2.57 (0.85)		2.74 (0.90)	
Want to learn about app privacy	0.43	147	0.39	130
Pro-app belief scale — mean of 7 beliefs (1=*strongly disagree*, 4=*strongly agree*)	2.85 (0.79)		2.93 (0.80)	

[a]N=578 (no privacy *n*=297 and privacy *n*=281) because 93 free responses were set to missing (*n*=71 [no privacy=36, privacy=35] were uninterpretable: nonwords, irrelevant comment, or too generic to categorize; *n*=21 [no privacy=7, privacy=14] did not give a free response; *n*=1 [no privacy=1] did not answer on the amount of concern about the app). Sixty-eight people (no privacy=35, privacy=33) described >1 concern.
[b]No privacy *n*=177 and privacy *n*=174 because it was only asked of people who reported that they were worried about privacy in closed-ended responses.
Freq., frequency.

Table 3. Effects of Privacy Condition on Primary and Secondary Outcomes

Outcomes	Privacy marginal mean	No privacy marginal mean	Adj b	Adj OR	95% CI	ω^2
Intention to download	2.69	2.69	0.01	–	−0.13, 0.15	−0.002
App concern	2.56	2.59	−0.03	–	−0.19, 0.13	−0.001
Free: concern about privacy[a]	0.43	0.42	–	1.05	0.74, 1.49	–
Closed: concern about privacy	0.52	0.52	–	1.02	0.74, 1.41	–
Privacy scale	2.74	2.58	**0.16***	–	0.04, 0.28	0.009
Want to learn about app privacy	0.40	0.43	–	0.84	0.60, 1.18	–
Pro-app beliefs	2.95	2.86	0.09	–	−0.02, 0.19	0.002

Note: Boldface indicates statistical significance (*$p<0.01$).
N=649 (no privacy *n*=334, privacy *n*=315). All models compare participants in the privacy condition with those in the no-privacy condition (ref category) and adjust for age; gender; race/ethnicity; the number of people in their household (including whether or not they live with children or a partner); their highest education level attained, their political identification; frequency of engaging in 3 COVID-19 prevention health behaviors in the past 7 days (e.g., masking, social distancing); how worried they were about someone they know getting COVID-19 (including themselves); and 3 categorical items: whether they work some or most days in close contact with people from outside their home, whether they know anyone who is at high risk for complications from COVID-19, and whether they know anyone who had a mild or severe case of COVID-19.
[a]N=560 (no privacy *n*=291 and privacy *n*=269).
Adj, adjusted

privacy messaging was unique to the privacy belief scale and did not significantly affect pro-app beliefs in general ($mean_{privacy}$=2.95, $mean_{noprivacy}$=2.86, b=0.09, 95% CI= −0.02, 0.19, p=0.115). The chi-square test that those condition coefficients were effectively the same showed that they were not (chi-square(1)=2.93, p=0.087). In addition, in follow-up observational analyses, privacy beliefs were associated with download intent, even after adjusting for covariates (b=0.65, 95% CI=0.57, 0.72, $p<0.001$).

DISCUSSION

Very few studies have examined whether describing an app's privacy encourages or discourages downloads. In line with Munzert and colleagues,[11] this study showed no difference in intentions to download on the basis of privacy messaging and did not depend on whether the framing of the message was gain or loss. Encouragingly though, privacy messaging describing how the app keeps individuals' data safe and secure only increased the

Table 4. Effects of Framing Conditions on Primary Outcome and Moderating the Privacy Condition

	Model 1			Model 2			
Predictors of intention to download the app	Marginal mean	Adj b	95% CI	Privacy marginal mean	No Privacy marginal mean	Adj b	95% CI
Framing		$F(2,624)=0.45$, p=0.64				$F(2,621)=0.36$, p=0.70	
No frame (ref)	2.74	–	–	–	–	–	–
Gain	2.68	−0.05	(−0.22,0.12)	–	–	−0.08	(−0.32,0.15)
Loss	2.66	−0.08	(−0.25,0.09)	–	–	0.01	(−0.23,0.24)
Privacy	–	–	–	–	–	0.05	(−0.20,0.29)
Framing x privacy						$F(2,621)=1.14$, p=0.32	
No frame (ref) x Privacy	–	–	–	2.76	2.71	–	–
Gain x privacy	–	–	–	2.74	2.63	0.06	(−0.28,0.40)
Loss x privacy	–	–	–	2.59	2.72	−0.18	(−0.52,0.16)

N=649 (no privacy *n*=334, privacy *n*=315). All models compare the download intentions among participants in the gain and loss framing conditions with those in the no-framing condition (ref category) and adjust for age; gender; race/ethnicity; the number of people in their household (including whether or not they live with children or a partner); their highest education level attained; their political identification; frequency of engaging in 3 COVID-19 prevention health behaviors in the past 7 days (e.g., masking, social distancing); how worried they were about someone they know getting COVID-19 (including themselves); and 3 categorical items: whether they work some or most days in close contact with people from outside their home, whether they know anyone who is at high risk for complications from COVID-19, and whether they know anyone who had a mild or severe case of COVID-19. Model 2 adds the privacy condition and the interaction of the privacy and gain/loss conditions as predictors.
Adj, adjusted.

Table 5. Effects of Privacy Condition on Primary Outcome Moderated by Age Category

Predictors of intention to download the app	Privacy marginal means	No privacy marginal means	Adj b	95% CI	ω^2
Privacy	–	–	−0.02	−0.21, 0.16	−0.002
Age category	–	–	0.06	−0.24, 0.37	−0.001
Privacy x age category					
≥35 years	2.63	2.66	–	–	–
18−34 years	2.77	2.72	0.08	−0.20, 0.35	−0.001

N=649 (no privacy *n*=334, privacy *n*=315). Measures assessed among U.S. adults in November 2020. The model compares the download intentions among participants in the privacy condition with those in the no-privacy condition (ref category), the 18−34 to 35+ age group categories, and the interaction of privacy and age category. The model adjusts for age; gender; race/ethnicity; the number of people in their household (including whether or not they live with children or a partner); their highest education level attained; their political identification; frequency of engaging in 3 COVID-19 prevention health behaviors in the past 7 days (e.g., masking, social distancing); how worried they were about someone they know getting COVID-19 (including themselves); and 3 categorical items: whether they work some or most days in close contact with people from outside their home, whether they know anyone who is at high risk for complications from COVID-19, and whether they know anyone who had a mild or severe case of COVID-19.
Adj, adjusted.

perceptions of data security; it did not increase privacy concerns. These context-dependent perceptions of security (i.e., *my info will be kept secure*, *I control who sees my info*, and *location information is not stored*) were associated with increased intentions to download the app in posthoc observational analyses adjusting for potential confounders, but this change was not large enough to detect overall differences by condition on intentions.

Given that this study was sufficiently powered to detect a change of a quarter of a scale point, we consider 2 other alternative explanations for why there were no differences in intentions by condition. It could be that (1) participants were resigned to losing their privacy to the app, so privacy messaging had no impact, or (2) the privacy messaging was not persuasive enough to change participants' privacy calculus about downloading the app. Neither this study nor the previous one by Munzert et al.[11] can distinguish between these alternatives. Although Munzert and colleagues[11] conclude that financial incentives do a better job at increasing app downloads than persuasive messaging about the app's security, their sample was recruited from a population of people who were already willing to undergo data surveillance, so it is possible that their sample had no room to move on persuasion about privacy. Furthermore, they may be motivated by incentives different from those that motivate the general population.

Future studies could address these possible explanations by increasing the potency of the privacy messaging manipulation. Switching from a description of what data will be collected and how it will be stored to who will have access to it and how long it will be stored could be more persuasive. In a study of Americans' beliefs about digital contact tracing in April 2020, Hargittai et al.[20] found that the players involved matter. Participants were most willing to download a COVID-19 contact-tracing app from a health protection agency, as opposed

Table 6. Raw Correlations Between the Outcomes and the Privacy Messaging Intervention

		1	2	3	4	5	6	7	8
	Outcomes/Intervention								
1	Intention to download	1.00							
2	App concern	**−0.18**	1.00						
3	Free: concern about privacy[a]	**−0.09**	**0.41**	1.00					
4	Closed: concern about privacy	**−0.15**	**0.40**	**0.60**	1.00				
5	Privacy scale	**0.67**	**−0.16**	**−0.18**	**−0.21**	1.00			
6	Want to learn about app privacy	**0.46**	−0.02	0.05	−0.06	**0.33**	1.00		
7	Pro-app beliefs	**0.73**	**−0.10**	−0.04	**−0.11**	**0.78**	**0.38**	1.00	
	Intervention								
8	Privacy condition	0.00	−0.02	0.01	0.01	**0.09**	−0.04	0.05	1.00

Note: Boldface indicates statistical significance ($p<0.05$).
N=671 (no privacy *n*=341, privacy *n*=330).
[a]N=578 (No Privacy *n*=297 and Privacy *n*=281).

to downloading an app from a government agency or a technology company. Participants were also more concerned about how long the data would be kept and any limitations on its use than on what data would be collected. Lewandowsky and colleagues[25] also showed that people's concerns about downloading an app are allayed by knowing who will see the data and for how long it will be stored. By changing the privacy messaging in this way, perceptions of safety might increase enough to see increases in intentions to download the app relative to a no-messaging condition. In addition, when there is no difference between conditions, a mixed method approach using qualitative interviews would allow researchers to ask more in-depth questions to distinguish between privacy apathy and messages that are not persuasive enough.

This study reduces concerns that PSAs describing how data are stored might increase worry about privacy, leading to fewer downloads. None of the responses to measures of concern increased in the privacy messaging condition relative to those in the no-privacy messaging condition.

Limitations

Although we strengthened this study by randomly assigning participants to message conditions within a large national sample, there were several limitations. At the time of the study, not every state had an app to download, so for some participants, the messaging was about a hypothetical future app, whereas others may have already thought about and decided whether to download their state's contact-tracing app. To use the same questions for residents of every state, the survey referred to a generic COVID-19 Exposure Notification app (to match the Apple/Google interface labeled Exposure Notification) instead of the state-specific app names. Tailoring the app name to a participant's state of residence may have led to responses more predictive of real life, although they would have also captured more of the variance in participants' responses to individual app features and the way each app was rolled out. Finally, this study used intentions to download the app scale as the primary outcome. Garrett et al.[26] found a large gap between intentions to download a contact-tracing app and actual uptake in Australia. Still, a 2006 meta-analysis of experimental evidence showed that a moderate change in intentions typically leads to at least small changes in behavior.[27]

CONCLUSIONS

Because a contact-tracing app's effectiveness increases as most of the population use the app, app developers must be equipped with strategies to curb challenges to mass acceptance, such as privacy concerns. Although this study found no direct differences in download intentions between the privacy and no-privacy messaging conditions, there was also no evidence that describing the app's privacy increased concerns about the app. Rather, describing the security measures taken to protect participants' privacy increased perceptions of security. These findings suggest that marketing an app's privacy protections is more likely to allay privacy concerns than increase the saliency of privacy as an issue. Future mixed-methods message testing about who has access to information—and for how long—may uncover new communication strategies for increasing public trust in contact-tracing and other apps.

ACKNOWLEDGMENTS

The authors are grateful to Allison Buttenheim, Robert Hornik, and Kevin Volpp for their feedback on the study design and paper drafts. We are grateful for support from the Delaware Department of Health and Social Services through the CARES Act.

The funder provided feedback on the study materials and design but had no role in the collection, analysis, or interpretation of data; writing of the report; or the decision to submit the report for publication.

This study was supported by Delaware's Department of Health and Social Services through the CARES Act.

Article content has not been previously presented elsewhere.

Declarations of interest: none.

CREDIT AUTHOR STATEMENT

Laura A. Gibson: Conceptualization, Methodology, Software, Formal analysis, Data curation, Funding acquisition, Project administration, Writing — original draft. **Erica L. Dixon**: Conceptualization, Project administration, Writing — review and editing. **Marissa A. Sharif**: Conceptualization, Writing — review and editing. **Anyara C. Rodriguez**: Writing — original draft. **Joseph N. Cappella**: Conceptualization, Writing — review and editing.

SUPPLEMENTARY MATERIALS

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.focus.2022.100059.

REFERENCES

1. Ferretti L, Wymant C, Kendall M, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*. 2020;368(6491):eabb6936. https://doi.org/10.1126/science.abb6936.
2. Aleta A, Martín-Corral D, Pastore Y Piontti A, et al. Modelling the impact of testing, contact tracing and household quarantine on second waves of COVID-19. *Nat Hum Behav*. 2020;4(9):964–971. https://doi.org/10.1038/s41562-020-0931-9.

3. Rodríguez P, Graña S, Alvarez-León EE, et al. A population-based controlled experiment assessing the epidemiological impact of digital contact tracing. *Nat Commun.* 2021;12(1):587. https://doi.org/10.1038/s41467-020-20817-6.
4. Abueg M, Hinch R, Wu N, et al. Modeling the effect of exposure notification and non-pharmaceutical interventions on COVID-19 transmission in Washington state. *NPJ Digit Med.* 2021;4(1):49. https://doi.org/10.1038/s41746-021-00422-7.
5. Cebrian M. The past, present and future of digital contact tracing. *Nat Electron.* 2021;4(1):2–4. https://doi.org/10.1038/s41928-020-00535-z.
6. Johnson B. The Covid Tracing Tracker: what's happening in coronavirus apps around the world. *MIT Technology Review.* December 16, 2020 https://www.technologyreview.com/2020/12/16/1014878/covid-tracing-tracker/.
7. O'Callaghan ME, Buckley J, Fitzgerald B, et al. A national survey of attitudes to COVID-19 digital contact tracing in the Republic of Ireland. *Ir J Med Sci.* 2021;190(3):863–887. https://doi.org/10.1007/s11845-020-02389-y.
8. Williams SN, Armitage C, Tampe T, Dienes K. Public attitudes towards COVID-19 contact tracing apps: a UK-based focus group study. *Health Expect.* 2021;24(2):377–385. https://doi.org/10.1111/hex.13179.
9. Chan EY, Saqib NU. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Comput Human Behav.* 2021;119:106718. https://doi.org/10.1016/j.chb.2021.106718.
10. Ramos LSC, Bhattacharya D. COVID-19: privacy and confidentiality issues with contact tracing apps. In: Proceedings of the 54th Hawaii International Conference on System Sciences; 2021. http://hdl.handle.net/10125/70859. Accessed February 9, 2021.
11. Munzert S, Selb P, Gohdes A, Stoetzer LF, Lowe W. Tracking and promoting the usage of a COVID-19 contact tracing app. *Nat Hum Behav.* 2021;5(2):247–255. https://doi.org/10.1038/s41562-020-01044-x.
12. Exposure notifications: helping fight COVID-19: Google COVID-19 information & resources. Google. https://www.google.com/covid19/exposurenotifications/. Updated September 9, 2020. Accessed February 8, 2021.
13. Zhang B, Kreps S, McMurry N, McCain RM. Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *PLoS One.* 2020;15(12):e0242652. https://doi.org/10.1371/journal.pone.0242652.
14. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. *Science.* 2015;347(6221):509–514. https://doi.org/10.1126/science.aaa1465.
15. Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. *Inf Syst Res.* 2006;17(1):61–80. https://doi.org/10.1287/isre.1060.0080.
16. Harris MA, Brookshire R, Chin AG. Identifying factors influencing consumers' intent to install mobile applications. *Int J Inf Manag.* 2016;36(3):441–450. https://doi.org/10.1016/j.ijinfomgt.2016.02.004.
17. Chin AG, Harris MA, Brookshire R. A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *Int J Inf Manag.* 2018;39:49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010.
18. Gu J, Xu Y, Xu H, Zhang C, Ling H. Privacy concerns for mobile app download: an elaboration likelihood model perspective. *Decis Support Syst.* 2017;94:19–28. https://doi.org/10.1016/j.dss.2016.10.002.
19. Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model. *Inf Syst Res.* 2004;15(4):336–355. https://doi.org/10.1287/isre.1040.0032.
20. Hargittai E, Redmiles EM, Vitak J, Zimmer M. Americans' willingness to adopt a COVID-19 tracking app: the role of app distributor. *First Monday.* 2020;25(11). https://doi.org/10.5210/fm.v25i11.11095.
21. Marwick A, Hargittai E. Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Inf Commun Soc.* 2019;22(12):1697–1713. https://doi.org/10.1080/1369118X.2018.1450432.
22. Draper NA, Turow J. The corporate cultivation of digital resignation. *New Media Soc.* 2019;21(8):1824–1839. https://doi.org/10.1177/1461444819833331.
23. Tversky A, Kahneman D. The framing of decisions and the psychology of choice. *Science.* 1981;211(4481):453–458. https://doi.org/10.1126/science.7455683.
24. Rothman AJ, Bartels RD, Wlaschin J, Salovey P. The strategic use of gain- and loss-framed messages to promote healthy behavior: how theory can inform practice. *J Commun.* 2006;56(s1):S202–S220. https://doi.org/10.1111/j.1460-2466.2006.00290.x.
25. Lewandowsky S, Dennis S, Perfors A, et al. Public acceptance of privacy-encroaching policies to address the COVID-19 pandemic in the United Kingdom. *PLoS One.* 2021;16(1):e0245740. https://doi.org/10.1371/journal.pone.0245740.
26. Garrett PM, White JP, Lewandowsky S, et al. The acceptability and uptake of smartphone tracking for COVID-19 in Australia. *PLoS One.* 2021;16(1):e0244827. https://doi.org/10.1371/journal.pone.0244827.
27. Webb TL, Sheeran P. Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychol Bull.* 2006;132(2):249–268. https://doi.org/10.1037/0033-2909.132.2.249.