f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Americans' willingness to adopt a COVID-19 tracking app: The role of app distributor

by Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer

Abstract

The COVID-19 global pandemic led governments, health agencies, and technology companies to work on solutions to minimize the spread of the disease. One such solution concerns contact-tracing apps whose utility is tied to widespread adoption. Using survey data collected a few weeks into lockdown measures in the United States, we explore Americans' willingness to install a COVID-19 tracking app. Specifically, we evaluate how the distributor of such an app (*e.g.*, government, health-protection agency, technology company) affects people's willingness to adopt the tool. While we find that 67 percent of respondents are willing to install an app from at least one of the eight providers included, the factors that predict one's willingness to adopt differ. Using Nissenbaum's theory of privacy as contextual integrity, we explore differences in responses across distributors and discuss why some distributors may be viewed as less appropriate than others in the context of providing health-related apps during a global pandemic. We conclude the paper by providing policy recommendations for wide-scale data collection that minimizes the likelihood that such tools violate the norms of appropriate information flows.

Contents

Introduction

In March 2020, the World Health Organization declared COVID-19 a global pandemic (World Health Organization, 2020). As infections increased globally, companies and governments rushed to develop technological solutions to trace infections and minimize the spread of the disease (*e.g.*, Centers for Disease Control and Prevention, 2020; eHealth Network, 2020). Most tools being developed focused on scaling contact-tracing and tracking efforts (hereafter referred to as "contact-tracing apps"), a method used for decades to reduce disease spread by notifying those who have been in contact with an infected individual (World Health Organization, 2017).

Contact-tracing apps use Bluetooth signals or GPS location data to identify phones that come in close proximity to the phone of an infected person (as determined by submission of COVID-19 test results) and notify the users of those "exposed" phones that they have come into contact with someone infected with COVID-19. While some countries and public health departments have chosen to build their own contact-tracing apps (Kelion, 2020), others are being built on

Google and Apple's "exposure notification system" (ENS) infrastructure (Google/Apple, 2020). The Google/Apple partnership is particularly noteworthy as the two companies are competitors that account for the vast majority of smartphone operating systems globally so a collaboration such as this is unusual. Additionally, they have made privacy a cornerstone of the technology (Nellis and Dave, 2020; Sherr, 2020).

As of this writing, use of most contact-tracing apps is voluntary; making app adoption voluntary rather than required is critical to protecting civil liberties (Díaz, 2020). There are many questions and unknowns about who may access the data, how long those data are stored, and for what purposes said data might be used in the future (Redmiles, 2020). The downside of a voluntary app is that it will not be an effective deterrent without widespread adoption, and recent polls suggest Americans are skeptical of the tools. A Pew survey in April 2020 found that most American adults (60 percent) did not think a tracking app would make a difference in stopping the spread of the disease (Anderson and Auxier, 2020). Likewise, an April 2020 University of Maryland-Washington Post poll found that nearly 60 percent of Americans are currently unwilling or unable (due to not owning a smartphone) to use an app to help track coronavirus spread (Timberg, *et al.*, 2020). The poll also found low trust in health insurance firms and technology companies like Google and Apple. This lack of trust might increase reticence to use an app, even one employing privacy-preserving strategies.

How to increase trust in and adoption of contact-tracing apps raises the following question: Does the distributor of the app affect one's likelihood to embrace the technology? In this paper, we answer this question by analyzing survey data from a sample of American adults collected in April 2020. We asked respondents whether they would install a contact-tracing app from various distributors. We examine what factors correlate with willingness to install an app from (1) any of the proposed distributors; (2) more than one distributor; and (3) each specific distributor. Some factors like age, Internet skills, and medical circumstances are consistently important to respondents' assessment, while others vary across app distributors.

We examine these findings through the lens of contextual integrity (Nissenbaum, 2010), a framework that moves beyond public-private dichotomies to account for numerous parameters within specific contexts when determining appropriate information flows. We focus on the role of the actor and transmission principle of the contextual integrity framework in identifying violations of contextual integrity, and the role of institutional trust in this process. We conclude the paper by discussing broader policy implications of this research for considering responses to crises and other large-scale events that require widespread data collection.

Related work

In this section, we summarize research regarding institutional trust, which may affect people's likelihood of using a contact-tracing app from a particular institutional distributor, as well as frameworks for thinking more broadly about privacy and disclosure in health contexts such as the COVID-19 pandemic.

Consumer trust in organizations and institutions

Institutional trust plays a significant role in the adoption and continuation of using products and services (Fukuyama, 1995). Trust generally refers to people's willingness to be vulnerable to other people or institutions (Pirson, *et al.*, 2019). Put another way, institutional trust can be understood as the "extent to which that partner is viewed as unlikely to exploit any vulnerabilities the other partner has," and includes perceptions of ability, benevolence, and integrity [1].

As noted by Ermisch and colleagues (2009), decisions about whether to trust another entity involve three components: (1) a consideration of the returns when trust expectations are fulfilled versus costs when they are not; (2) a probability calculation of the likelihood that the trustee (*e.g.*, an app distributor) will do as expected; and (3) an assessment of the risk of being exploited by the trustee. Trust can be personal — focused narrowly on an individual — or, more often, generalized toward a category of people or institutions (Rotter, *et al.*, 1972). Generalized trust toward popular online e-commerce companies, for example, can serve as a simple heuristic to help individuals decide whether or not to trust a Web site with their credit card information.

Trust serves as a social and economic lubricant in both interpersonal interactions and in facilitating transactions between people and institutions (Putnam, 2000). When considering public trust in institutions, Pirson and colleagues (2019) point to both individual and institution-based factors that play a role in decision-making. In their research,

public trust in an institution was positively influenced by people's previous experience with said institution and negatively affected by a person's age. Men were more likely to trust a company than women when controlling for other factors. Likewise, firms whose missions were connected to societal benefits were viewed as more trustworthy.

Historically, trust has been closely connected to economic outcomes (Fukuyama, 1995) and has provided a competitive advantage to institutions (Barney and Hansen, 1994). When trust in an institution decreases, people are more likely to turn to a competitor or alternate solution. However, research shows a steady decline of trust in recent decades across many domains (Cook and Schilke, 2010). For example, Imber (2008) details declining trust in doctors over the twentieth century. Findings from the Pew Research Center highlight decreased trust in the federal government following Edward Snowden's revelations of mass surveillance (Rainie and Duggan, 2016; Rainie, *et al.*, 2019).

Public trust in technology companies has been decreasing over the last decade following a number of security breaches and other violations of users' privacy expectations. For example, in a 2019 NBC/Wall Street Journal poll (Murray, 2019), nearly two-thirds of Americans said they do not trust Facebook to protect their data. This lack of trust in the company can be connected to the Cambridge Analytica scandal as well as media reports on their "emotional contagion" study (Selinger and Hartzog, 2016). However, these violations in trust have not slowed down the popularity of the platform, which has continued to grow in the months and years following these events.

During a crisis, trust becomes both more and less important. In the case of COVID-19, people need more trust in the institutions (*e.g.*, federal government, technology companies) that are working toward a solution. This is especially important when considering contact-tracing apps, which require significant buy-in to be successful. If people do not trust the entity creating and distributing an app — be it the government, public health institutions, businesses, or technology companies — they are probably less likely to use it. Those working toward solutions need to take steps associated with building trust to ensure buy-in, which could include transparency in terms of data being collected and data-minimization practices to limit both the amount of data being collected and how those data are being used.

Conversely, trust could be less important in the face of a global pandemic, when society might be more willing to acquiesce to things it would otherwise reject under regular conditions. Individuals may be more willing to accept government surveillance if it reduces the spread of a deadly disease, even in the absence of trustworthy actors or protections. Historically, during times of acute crisis (*e.g.*, riots, natural disasters), Americans have seen their rights restricted to protect citizens from different harms (Finkelman, 2003). In the case of COVID-19, some people — including a team of scientists at the forefront of tracking the pandemic — have argued for the oft-used tradeoff of giving up some personal privacy to benefit public health (Servick, 2020). From this perspective, people should be willing to provide institutions with sensitive personal information (*i.e.*, location data) because it reduces the spread of COVID-19.

The trade-off between privacy and public benefit

The concept of privacy has been framed through a number of lenses, for example, Smith and colleagues (2011) describe how privacy can be viewed as a right — invoking Warren and Brandeis' (1890) early writing on privacy — or as a temporary state of "withdrawal of a person from the general society," as described by Westin [2]. The authors also note that privacy is often framed as a commodity, focusing on the economic nature of privacy whereby people exchange private information for some physical or informational good.

Privacy calculus (Culnan, 1993; Laufer and Wolfe, 1977) invokes privacy as a commodity. The theory describes a cost-benefit analysis for decision-making that includes disclosure of personal information, such as when one uses an e-commerce site or downloads a mobile app. Culnan and Bies (2003) argue that people are more likely to accept a loss in privacy when the benefits of the transaction outweigh the risks. Looking at e-commerce transactions, Dinev and Hart (2006) found that trust and Internet interests can overcome concerns about privacy risks associated with sharing sensitive data. For example, when deciding whether to make an online purchase, a person may compare potential risks (*e.g.*, if the site uses encryption, trust in the company) with potential benefits (*e.g.*, scarcity of desired product, speed of delivery). Such an approach would suggest that people may deprioritize privacy concerns in the context of a contact-tracing app given its potential health benefits.

Privacy calculus has high face validity; however, this framework has been criticized for being overly simplistic in accounting for the complexity of decision-making involved in trading private information for some benefit. For example, Turow and colleagues (2015) argue that Americans' increasing willingness to trade personal information for benefits cannot be explained by a rational assessment where they determine that the tradeoffs are fair. Instead, the researchers argue that Americans have become deeply resigned to sharing their data and that they lack the agency to

control or manage it. Other studies have highlighted a similar sense of resignation or apathy to explain why people disclose personal information on social media platforms and in other digital spaces (Hargittai and Marwick, 2016; Hoffmann, *et al.*, 2016). Such a perspective would suggest that when given an actual choice, people may opt against giving up their privacy.

Instead of looking at privacy attitudes and behaviors as an economic and context-neutral exchange, a more helpful way to account for the complexities of information flow is to focus on the contextual factors that affect the norms and appropriateness of those flows. In the next section, we unpack this idea more by describing Nissenbaum's (2010) framing of privacy as contextual integrity, and consider how the distributor of a contact-tracing app may affect a person's willingness to use that app.

Privacy as contextual integrity

As digital technologies become increasingly embedded in our everyday lives, they introduce new flows of information that frequently shift boundaries and challenge privacy norms. Such dynamism is central to the notion of networked privacy, which Marwick and boyd (2014) define as the "ongoing negotiation of contexts in a networked ecosystem in which contexts regularly blur and collapse" [3]. Such blurring and collapsing of contexts seem inevitable when we ask citizens to trust contact-tracing apps with their location and health data. Nissenbaum's (2010) theory of contextual integrity (CI) takes context as its starting point, making it a useful framework for considering the privacy implications of contact-tracing apps and the larger infrastructures that support them. Rejecting the public/private dichotomy that dominates most approaches to privacy, CI instead rests on the understanding that information flows occur within particular contexts, and the theory ties adequate privacy protection to respecting informational norms within those contexts.

Nissenbaum summarizes the fundamentals of CI via four theses. Thesis 1 asserts that privacy, to be a useful concept, must center on the appropriateness of flows of personal information, rather than categorizations of information (*e.g.*, as sensitive or secret). Thesis 2 argues that flows of personal information are only appropriate when they conform to informational norms "that describe, prescribe, proscribe, and establish expectations for characteristic contextual behaviors and practices" [4]. Such norms shape people's expectations about appropriate information flows within particular contexts.

Thesis 3 sets out three key parameters that define informational norms: actors, attributes, and transmission principles. *Actors* refer to the parties involved in a given interaction, including senders, receivers, and subjects of information. In the case of contact-tracing apps, actors include the app distributors and people asked to install said apps, and perhaps third parties such as health providers or insurance companies. *Attributes* describe the nature of the data that is flowing among the actors, and for contact-tracing apps this might include people's location, proximity to others, and health data. *Transmission principles* shape or constrain the flow of information, such as with doctor-patient confidentiality when disclosing health status. With contact-tracing apps, the principle of fiduciary most clearly delineates the relationship between users and the recipients of their data; this differs significantly from more traditional health disclosures between a doctor and patient, which are guided by the principle of confidentiality. Isolating these parameters yields a rich set of variables with which to characterize — and ultimately assess — the appropriateness of data flows within a given context.

Contextual integrity's fourth thesis provides the means for assessing the impact of a new technology or practice that disrupts a parameter by conflicting with existing contextual informational norms: "A practice violates a privacy norm if resulting flows fail to map onto expected values for the parameters" [5]. To determine what, if anything, should be done to address the violation, CI calls for a wider examination of the moral and political implications of the new practice and how it might affect the prevailing values, goals, and ends of the context in question. For example, while an update to a fitness tracking app to enable tracking one's body temperature and sharing that data with health authorities might constitute a disruption of the contextual integrity of health information flows between a user and a technology developer, this disruption of CI would need to be balanced against the public health benefit of using contact-tracing apps during a global health pandemic.

At first glance, contextual integrity provides an easy way to explain the strong negative reaction by many to reports of governments seeking to track citizens' locations directly via their smartphones in order to enforce social distancing and engage in contact tracing (Newton, 2020; Tau, 2020). While individuals might be comfortable sharing their location with Google or Garmin to receive services like navigation and fitness tracking, having that data flow to government officials for long-term monitoring of citizen movements — a change in both the actor and transmission principles — may be deemed an inappropriate new information flow. Yet, as the COVID-19 global pandemic continues, there is

increasing pressure to embrace contact tracing, and trust the technology developers and government agencies to balance individual privacy with the need to ensure public health adequately. Contextual integrity provides a helpful theoretical framework for considering these tensions and evaluating what the public considers appropriate information flows during a health crisis. In the context of contact-tracing apps, one way this manifests itself concerns the distributor of said apps.

Research questions

The adoption and use of contact-tracing apps amid the COVID-19 global pandemic depends greatly on people's trust in the actors involved, as well as whether such a solution preserves the contextual integrity of data flows by maintaining appropriate transmission principles. For example, do Americans feel differently about apps developed and distributed by medical groups versus the government? Are they willing to adopt apps distributed by tech companies that already collect significant personal information? To gain an understanding of the factors associated with willingness to use a contact-tracing app distributed by these entities, we ask the following research questions:

RQ1: Who is willing to install a COVID-19 tracking app regardless of the distributor?
RQ1a: Who is willing to install a COVID-19 tracking app from more than one distributor?

RQ2: How does the distributor of a COVID-19 tracking app relate to people's willingness to adopt it?
RQ2a: How does willingness to install from a particular distributor relate to a willingness to install from other distributors?
RQ2b: How do sociodemographic factors, political leaning, Internet skills, medical factors related to COVID-19, and institutional trust vary across people's willingness to install a COVID-19 tracking app from specific distributors?

Methods

Data collection

We collected survey data from American adults ages 18 and over during 4–8 April 2020. We contracted with the Cint online survey firm to reach a diverse sample. Cint's respondent pool includes over 15 million people gathered through a double opt-in procedure, participants are compensated for their time. We quota sampled on age, gender, education, and region to match U.S. Census figures. Those sociodemographic factors are often related to Internet use and so we wanted to make sure our sample varied on those characteristics (Robinson, *et al.*, 2015). Respondents come from all 50 U.S. states plus Washington, D.C. At the beginning of our data collection, the U.S. had 307,876 confirmed COVID-19 cases and there had been 8,359 COVID-19 deaths (Wikipedia, 2020).

We implemented attention-verification questions and removed cases that failed more than one, which constituted 4.6 percent of the 1,441 original respondents (Berinsky, *et al.*, 2014) resulting in 1,374 valid cases. In this paper, we restrict our analysis to the 1,254 respondents who reported having a mobile phone at home with Internet access given that the question is most realistically applicable to them.

Measures: Dependent variable

Whenever possible, we relied on previous work for our questions. Given the novelty of the situation, this was not possible with questions specifically about the pandemic so we did extensive pretesting of those. After pretesting the instrument in our research group, we conducted in-depth pilot tests with seventy respondents on Amazon Mechanical Turk as a way to conduct cognitive interviews at scale. We asked multiple open-ended questions about our pandemic-

specific items, probing respondents' difficulty with answering the questions, interpretation of specific terms in the questions, and overall comprehension of the questions. We iteratively refined and tested survey wording until respondents consistently and correctly understood our items. This is how we arrived at the following question to assess people's willingness to install a COVID-19 tracking app, which does not assume agreement, rather, explicitly asks whether people would agree to installing an app:

> If there was a tracking app that could help slow the spread of the Coronavirus in your community and reduce the lockdown period, would you agree to install it on your phone knowing that it would collect your location data and information about your health status?

This question was then followed by several options and respondents were asked to check all that apply:

> Yes, if a not-for-profit organization verified by a public authority distributes the app
> Yes, if the federal government distributes the app
> Yes, if my local government distributes the app
> Yes, if a health protection agency (such as CDC, FDA) distributes the app
> Yes, if my health insurance provider distributes the app
> Yes, if an international organization distributes the app
> Yes, if a technology company distributes the app
> Yes, if the main public university in my state distributes the app
> No, I would not agree to install it in any of the above cases

For our measure of whether someone is amenable to installing such an app (*RQ1*), we created a variable that indicates having chosen any of the Yes options versus having chosen the No option. (Respondents who chose both a Yes and the No option were coded as missing for this question and are excluded from the analyses; there were five such cases.) We also examined who would be willing to install apps from multiple providers and for this we created a summary variable of Yes responses. To address *RQ2* and *RQ2a*, we created separate dummy variables for each of the Yes responses.

Measures: Independent variables

Sociodemographics. We measured age by asking for respondents' birth year and subtracted that from 2020. Gender options were male, female, and other, which we recoded into a female gender category (1 vs. 0 for all others). We measured education level by asking for respondents' highest level of school completed with six options, which we recoded into three: high school degree or less, some college, and college degree or more. We asked about household income through 13 categories ranging from less than US$10,000 to US$200,000 or more, which we then recoded to midpoint values to create a continuous variable. We use a logged version of this in the regression models. To assess people's metropolitan status, the answer options were: a big city, the suburbs or outskirts of a big city, a town or a small city, or a rural area, and recoded this into a binary variable reflecting urban residence (value of 1 for those who live in a big or small city) versus other (0).

To determine people's political ideology, we used the American National Election Studies (2020) question: "Generally speaking, do you usually think of yourself as a Republican, a Democrat, an Independent, or what?" The choices were those three, plus "No preference." Independents and no-preference respondents were asked a follow-up: "Do you think of yourself as closer to the Republican or Democratic Party." We use information from these two questions to create a dummy variable for Republican-leaning political ideology versus other.

Internet skills. Understanding the Internet better may influence people's attitudes toward app installation so we wanted to control for Internet skills. We use the established six-item Web-use skills scale (Hargittai and Hsieh, 2012) to do this by averaging the six values.

Medical factors related to COVID-19. People who belong to the medically high-risk category for COVID-19, those who live in a household with medical workers, and those who know others with the disease (or who themselves have been diagnosed with it) may approach tracking apps differently so we wanted to account for this in our models. We asked people whether they have various medical conditions (*e.g.*, high blood pressure, cardiovascular disease, cancer) that constitute high-risk and created a dummy variable for this. We also asked: "Do you or anyone in your household

currently work at a healthcare facility, or visit a healthcare facility for work reasons, where Coronavirus (COVID-19) patients are cared for?" and created a dummy for those who answered yes (=1). We also wanted to account for whether people know of others who have tested positive and asked: "Do you know any people who have been diagnosed with Coronavirus (COVID-19)?" creating another dummy variable (1 for knowing someone).

Trust in institutions. A willingness to install a COVID-tracing app may be related to people's trust in the types of institutions that are distributing such apps. To account for this, we asked: "Below are some institutions in this country. As far as the people running these institutions are concerned, would you say you have a great deal of confidence, only some confidence, or hardly any confidence at all in them in *addressing the Coronavirus pandemic*?" The institutions included: "medical system," "federal government," "state/local government," "business leaders" with three answer options: a great deal of confidence (value of 3), only some confidence (2), hardly any confidence (1).

The sample

Table 1 presents sample characteristics. Ages range from 18–82 with a median of 43, mean of 44.7. Just over half (53.6 percent) of respondents identify as female. Just under half (46.2 percent) live in big cities or smaller cities and towns. About half have no more than a high school education and less than a third have a college degree or more. The average household income is US$60,000. There is a close-to equal split of Democrat-leaning (54 percent) and Republican-leaning respondents. Over a third (37 percent) of respondents belong to a medically high-risk category for COVID-19 and eighteen percent know someone who has been infected.

Table 1: Sample descriptives.
Note: (*N*=1,254).

	Percent	Mean	Standard deviation
Age		44.7	15.4
Female	53.6		
Education: High school or less	48.3		
Education: Some college	21.1		
Education: Bachelor's or above	30.5		
Household income		US$60,401	S$51,687
Urban	46.2		
Political leaning: Democrat	54.1		
Political leaning: Republican	45.1		
High risk for infection	37.0		
Medical staff in household	12.4		
Knows someone infected	17.7		
Internet skills		3.4	1.1
Confidence in Medical System (1–3) Hardly any		2.6	0.6
Confidence in Federal Government (1–3) Hardly any		2.1	0.7
Confidence in Local Government (1–3) Hardly any		2.3	0.7
Confidence in Business Leaders			

Hardly any		2.0	0.7

Analysis

We start by sharing basic descriptives about willingness to install a COVID-19 tracking app. Then, to examine who is most amenable to installing a COVID-19 tracking app, we construct two binomial logistic regression models with (1) whether the respondent was willing to install a coronavirus app from at least one provider as the dependent variable; and (2) whether the respondent was willing to install a COVID-19 app from just one provider versus more than one. In both cases, we include sociodemographics, Internet skills, political ideology, and COVID-19 experiences as the independent variables. To understand which distributors were most popular, we used X^2 proportion tests to compare the proportion of respondents who preferred each provider. We correct for multiple testing effects using Bonferroni-Holm (BH) correction where appropriate. Additionally, to explore differences in which respondents were willing to install apps from different distributors, we constructed binomial logistic regression models for willingness to install an app from each of the distributors. We did not construct models for apps distributed by public universities or international organizations because fewer than 200 respondents (<16 percent) of our sample reported being willing to install an app from either of these distributors, and 200 cases is the threshold for robust regression modeling (King and Zeng, 2001).

Results

Willingness to install a COVID-19 tracking app

RQ1 asked about people's willingness to install a COVID-19 tracking app at all, and *RQ1a* asked about who would be willing to do so from multiple distributors. Overall, two-thirds (66.9 percent) of respondents would be willing to install a COVID-19 tracking app from at least one of the distributors we asked about. Half (50.5 percent) were only willing to install an app from one of the listed distributors, 15.9 percent from two distributors, 13.8 percent from up to three distributors, and the remaining 12.2 percent from 4–8 distributors (see Figure 1).

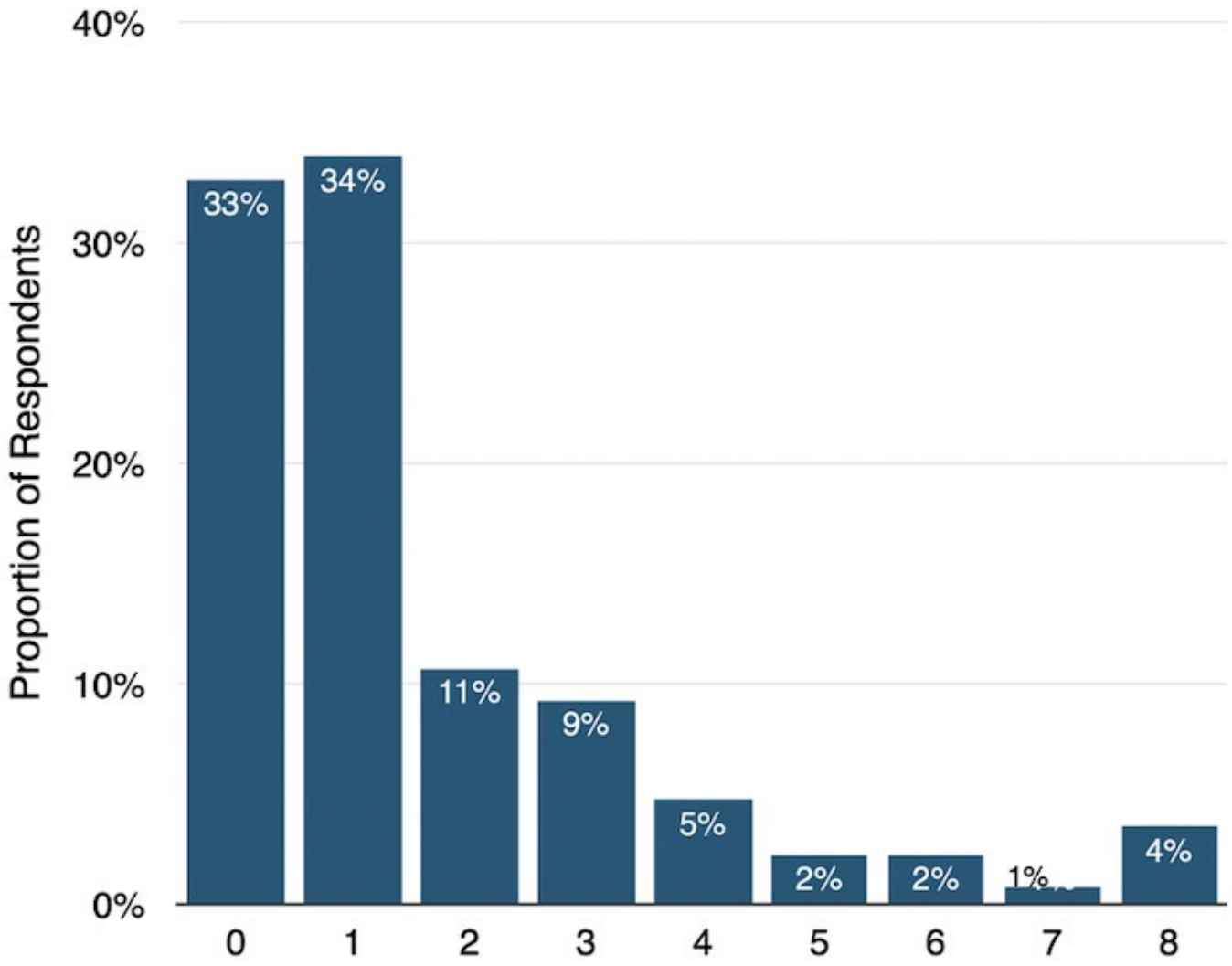

Figure 1: Number of distributors from which respondents who were willing to install COVID-19 apps were willing to install.

To determine whether background factors relate to people's willingness to install a COVID-19 tracking app, we ran binary logistic regression models on willingness to install at all and willingness to install from more than one distributor compared to one. For the first, we coded those who selected at least one of the providers as "1" while those who selected "No, I would not agree to install it in any of the above cases" as "0". The first model looks at how sociodemographics, political ideology, personal COVID-19 experiences and Internet skills relate to willingness to install a COVID-19 tracking app. The results (see Table 2) suggest that older adults are somewhat less willing to install such an app, while those more educated are considerably more willing. Being at a high risk of COVID-19 or knowing someone who has COVID-19 is associated with a higher willingness to install an app, as is having higher Internet skills. Next, we added four variables measuring confidence in various institutional actors addressing the pandemic (*i.e.*, medical system, federal government, local/state government, and business leaders), to assess whether trust in these institutions affected people's willingness to download. While age became a stronger predictor of willingness to install an app and education less strong, the other findings from the earlier model remained robust. Additionally, those who have a higher confidence in the medical system were more willing to install a COVID-19 tracking app. Confidence in other institutional actors plays no role when considering all institutional confidence together. We do not find that willingness to install apps differs by political leaning. Specifically, 68.8 percent of

Democrats and Democrat-leaning respondents were willing to install a COVID-19 tracking app, while 64.7 percent of Republicans and Republican-leaning respondents were willing to install. At the time of our study, early April 2020, measures to mitigate COVID-19 were nearly-equally supported by Democrats and Republicans (Van Green and Tyson, 2020).

	Willing to install app				Willing to install app from more than one distributor			
	Model 1		Model 2		Model 3		Model 4	
	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval
Female	0.858	[0.667, 1.104]	0.862	[0.668, 1.111]	1.086	[0.817, 1.445]	1.066	[0.8, 1.422]
Age	0.990 *	[0.982, 0.999]	0.987 ***	[0.978, 0.996]	0.998	[0.988, 1.008]	0.997	[0.987, 1.007]
Urban	1.035	[0.807, 1.328]	1.026	[0.798, 1.321]	0.794	[0.599, 1.051]	0.781	[0.588, 1.037]
Education: some college	1.352	[0.98, 1.873]	1.307	[0.944, 1.818]	0.804	[0.556, 1.161]	0.809	[0.559, 1.169]
Education: college or more	1.579 ***	[1.14, 2.193]	1.518 *	[1.091, 2.118]	1.020	[0.706, 1.473]	1.015	[0.7, 1.47]
Household income (logged)	1.086	[0.943, 1.251]	1.083	[0.939, 1.25]	1.109	[0.938, 1.314]	1.109	[0.937, 1.315]
Republican political leaning	0.857	[0.669, 1.099]	0.851	[0.65, 1.113]	1.034	[0.779, 1.372]	1.022	[0.756, 1.383]
High risk for Covid-19	1.520 ***	[1.162, 1.997]	1.533 ***	[1.167, 2.02]	1.061	[0.79, 1.426]	1.051	[0.781, 1.414]
Medical staff in household	1.839 ***	[1.214, 2.853]	1.845 ***	[1.213, 2.875]	0.772	[0.514, 1.156]	0.776	[0.516, 1.163]
Knows someone with Covid-19	0.977	[0.702, 1.37]	0.971	[0.695, 1.366]	1.429	[0.991, 2.069]	1.447	[1.001, 2.099]
Internet skills	1.286 ***	[1.149, 1.44]	1.257 ***	[1.121, 1.41]	1.271 ***	[1.105, 1.464]	1.254 ***	[1.089, 1.446]
Trust in medical system			1.576 ***	[1.235, 2.014]			1.097	[0.819, 1.47]
Trust in federal gov			0.953	[0.768, 1.183]			0.995	[0.787, 1.259]
Trust in local gov			1.037	[0.822, 1.307]			1.132	[0.884, 1.452]
Trust in business leaders			1.136	[0.919, 1.405]			1.055	[0.834, 1.334]
Intercept	0.439	[0.095, 2.05]	0.143 *	[0.028, 0.736]	0.163	[0.025, 1.033	0.098 *	[0.013, 0.713]
N	1231		1228		828		827	
X^2	75.51		95.00		26.35		28.61	
Pseudo-R^2 (Cragg-Uhler)	0.08		0.10		0.04		0.05	

Table 2: Binary logistic regression predicting willingness to adopt a COVID-19 tracking app from a set of eight distributors.

To examine willingness to download apps from multiple providers, we conducted a binary logistic regression with the dependent variable being whether a person was willing to download from just one of the potential distributors (coded as "0") or from more than one of the distributors (coded as "1"). The second set of models on Table 2 shows the results. We again first excluded the confidence-in-institutions measures and in the second model included those as well. In both models, the only factor that explains the willingness to adopt more than one app is Internet skills, which shows a positive association.

The relationship between distributor and willingness to install a COVID-19 tracking app

Respondents were divided on the distributors from which they would be willing to install a COVID-19 tracking app. As shown in Figure 2, over one-third of respondents (37 percent) indicated their willingness to install a coronavirus tracking app distributed by a Health Protection Agency (HPA) like the Centers for Disease Control and Prevention (CDC) or the Food and Drug Administration (FDA), with 13 percent indicating they would only be comfortable with that type of distributor. Significantly fewer (BH corrected X^2 proportion test, $p<0.05$) respondents were willing to install an app distributed by their health insurance provider (22 percent), the federal government (20 percent), local government (20 percent), or a technology company (19 percent). The least acceptable distributors (BH corrected X^2 proportion test, $p<0.05$) were a public university (12 percent) or an international organization (11 percent).

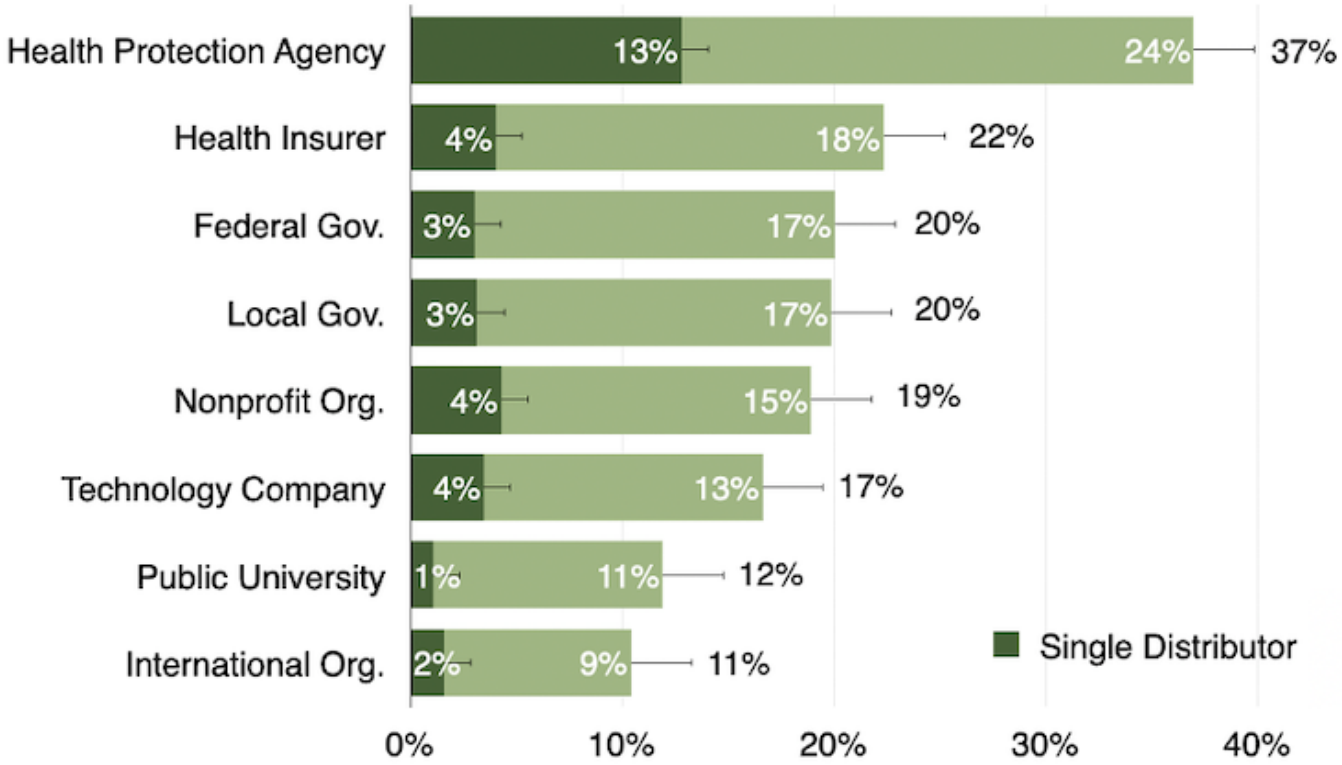

Figure 2: Percentage of sample who selected each of the distributor options. Percentages in dark green reflect responses that only listed that option; percentages in light green reflect responses that also included at least one other option.

RQ2a asked how willingness to install from one distributor related to willingness to install from another. We created a correlation matrix to identify the most and least common pairings across the eight distributor options. The strongest correlation was between HPAs and health insurance (co-occurring 14 percent of the time), pointing to the strength of health actors distributing a health-related app. The data also shows a strong correlation between those willing to use an HPA-distributed app and those willing to use those from local or federal governments (13 percent co-occurrence for each). For distributors that had a low adoption willingness, co-occurrence with other apps was consistently low. Figure 3 shows commonly occurring pairs of distributors.

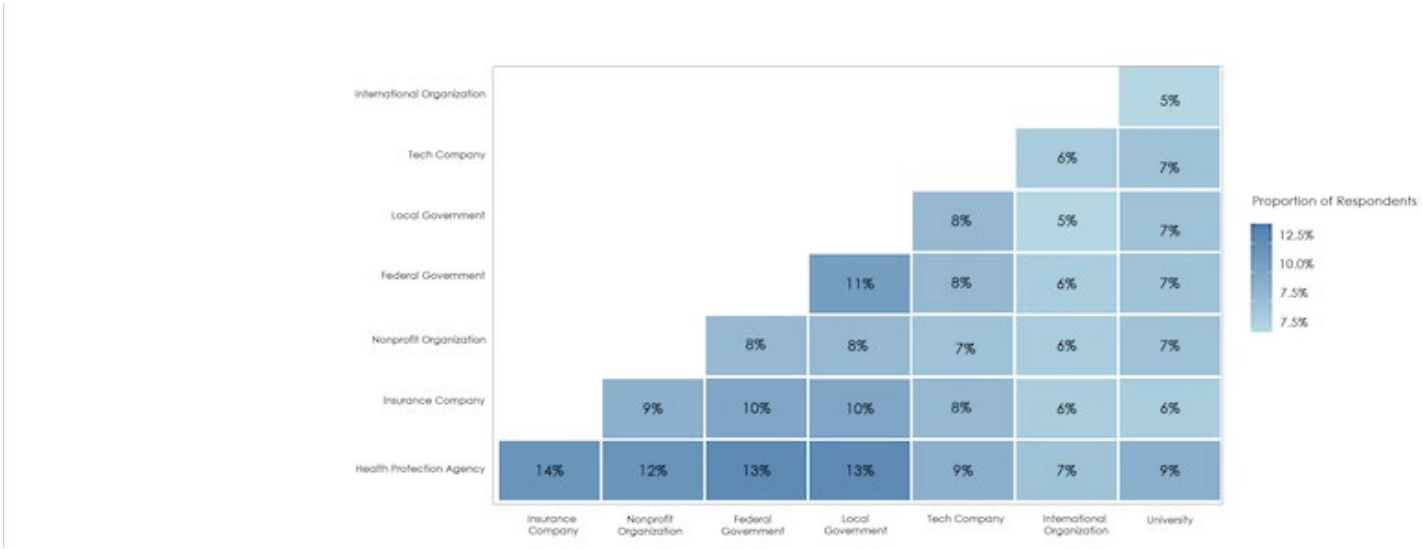

Figure 3: Percentage of two contact-tracing app distributors being selected by the same respondent.

RQ2b asked how user characteristics relate to what distributor is acceptable for installing a COVID-19 tracking app. We conducted a series of binary logistic regressions to answer this for each of the six most popular distributors: HPA, health insurance, the federal government, local government, a technology company, and a nonprofit. Looking across the models, some trends emerge. See Table 3 for details.

	Health protection agency		Federal government		State/local government		Nonprofit		Technology company		Health insurance provider	
	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval	Odds Ratio	Confidence interval
Female	1.143	[0.894, 1.462]	0.978	[0.731, 1.308]	0.981	[0.734, 1.313]	0.975	[0.726, 1.312]	0.656 ***	[0.479, 0.897]	0.961	[0.727, 1.271]
Age	0.998	[0.99, 1.007]	0.991	[0.98, 1.001]	0.991	[0.981, 1.002]	0.985 ***	[0.974, 0.995]	0.989	[0.978, 1]	1.004	[0.994, 1.014]
Urban	0.868	[0.681, 1.106]	0.846	[0.632, 1.131]	0.920	[0.689, 1.228]	0.935	[0.697, 1.253]	0.972	[0.712, 1.326]	0.864	[0.654, 1.139]
Education: some college	1.090	[0.793, 1.495]	0.958	[0.652, 1.392]	1.168	[0.804, 1.686]	1.250	[0.846, 1.834]	0.825	[0.538, 1.244]	1.235	[0.857, 1.769]
Education: college or more	1.437 *	[1.053, 1.961]	1.094	[0.755, 1.58]	1.069	[0.735, 1.553]	1.583	[1.089, 2.305]	1.010	[0.677, 1.504]	1.382	[0.968, 1.973]
Household income (logged)	1.133	[0.982, 1.31]	1.038	[0.877, 1.232]	1.060	[0.894, 1.259]	1.116	[0.937, 1.333]	1.034	[0.862, 1.245]	1.104	[0.935, 1.308]
Republican political leaning	0.847	[0.664, 1.078]	1.135	[0.838, 1.535]	1.032	[0.773, 1.374]	0.813	[0.604, 1.09]	0.780	[0.569, 1.067]	0.843	[0.639, 1.111]
High risk for Covid-19	1.573 ***	[1.218, 2.033]	1.023	[0.75, 1.391]	1.218	[0.896, 1.65]	1.504 **	[1.102, 2.05]	1.352	[0.97, 1.88]	1.298	[0.97, 1.733]
Medical staff in household	0.962	[0.661, 1.389]	1.226	[0.801, 1.843]	0.892	[0.563, 1.374]	0.762	[0.475, 1.188]	1.721 *	[1.117, 2.611]	0.934	[0.6, 1.421]
Knows someone with Covid-19	1.040	[0.755, 1.426]	1.012	[0.69, 1.461]	1.064	[0.726, 1.536]	0.993	[0.675, 1.439]	0.859	[0.558, 1.292]	0.860	[0.589, 1.237]
Internet skills	1.219 ***	[1.088, 1.368]	1.198 ***	[1.047, 1.374]	1.224 ***	[1.068, 1.406]	1.206 **	[1.048, 1.391]	1.332 ***	[1.145, 1.554]	1.132	[0.993, 1.291]
Trust in medical system	1.600 ***	[1.274, 2.021]									1.469 ***	[1.125, 1.938]
Trust in federal gov			1.544 ***	[1.251, 1.911]								
Trust in local gov					1.462 ***	[1.172, 1.833]						
Trust in business leaders									1.235	[0.984, 1.551]		
Intercept	0.019 ***	[0.004, 0.1]	0.052 ***	[0.008, 0.342]	0.037 ***	[0.005, 0.243]	0.063 ***	[0.009, 0.421]	0.067 **	[0.008, 0.505]	0.019	[0.003, 0.127]
N	1228		1229		1229		1231		1229		1228	
χ^2	72.06		36.20		28.68		38.53		51.32		34.78	
Pseudo-R^2	0.08		0.05		0.04		0.05		0.07		0.04	

Table 3: Binary logistic regressions predicting willingness to adopt COVID-19 tracking apps from six types of distributors.

There are no systematic differences by sociodemographic factors. While females are much less likely to want to install from a technology company, there are no gender differences for the other distributors. Age matters only in the case of nonprofits where older adults are less likely to want to install. Those at high risk of COVID-19 are more willing to install from HPAs and nonprofits. Internet skills emerged as a significant factor in all but one of the models, with those reporting greater skills being more willing to adopt an app distributed by HPAs, the federal government, state/local government, nonprofits, and a technology company.

When it comes to confidence in various institutional actors' ability to respond to the pandemic effectively, it proved to be important in all cases except for a technology company as a distributor, where confidence in business leaders was unrelated, possibly as that category is not directly about technology companies *per se*. Trust in the medical system was positively related to willingness to adopt from a health protection agency as well as a health insurance provider. Trust in the federal government was positively linked with a willingness to install from the federal government, and trust in state/local government was positively associated with local/state government as the distributor.

Discussion

With the global COVID-19 pandemic, governments, health agencies, and other groups immediately began exploring technological approaches to minimize the spread of the disease. Contact-tracing apps — which rely on Bluetooth proximity data or GPS location data from mobile devices ubiquitous in many parts of the world — quickly became one of the most discussed tools to help identify and notify those who had been exposed. We collected the data in this paper

in early April 2020, a few weeks after the United States began a lockdown, so news about COVID-19, and discussions about contact-tracing apps, were widespread at the time of data collection.

While other national polls and surveys have focused on general measures of adoption (Anderson and Auxier, 2020; *e.g.*, Timberg, *et al.*, 2020), we approached the question of contact-tracing apps by evaluating whether the *distributor* of such an app affected people's willingness to adopt it. In other words, do Americans' attitudes differ when considering a contact-tracing app distributed by a health protection agency as opposed to one distributed by a technology company, the government, a nonprofit, and international organization, or an academic institution?

This framing of the question allows us to consider the privacy implications of information flows through Nissenbaum's (2019, 2010) framework of privacy as contextual integrity (CI). As described above, preserving the contextual integrity of new information flows rests on preserving existing informational norms surrounding three key parameters that define informational norms: actors, attributes, and transmission principles. According to CI, privacy violations are likely to occur when the norms across any of these parameters become disrupted; this includes changes to the actor involved in data collection and processing, as well as changes to the transmission principles that typically guide information flows, such as the principle of confidentiality guiding health disclosures. The analysis presented above allows us to focus on the appropriateness of different actors involved in health-related disclosures and whether Americans view those actors as appropriate collectors of sensitive data.

First, when thinking about entities involved in developing and deploying contact-tracing apps, three groups have received the most attention: health agencies, governments (federal and local), and technology companies, as seen most notably in Apple and Google's exposure notification system. Looking across the eight distributors included in the survey, HPAs and insurance providers were viewed as the most appropriate distributors of a COVID-19 tracking app by our respondents, with HPAs being the lone acceptable distributor for some, or typically paired with other distributors. This may seem unsurprising on its surface, but it highlights how much actors and transmission principles play a role in determining the appropriateness of information flows, even in the face of a global pandemic. While some might argue that people should be willing to take any and all steps to fight against a global pandemic, our results show that the distributor plays an important role in one's willingness to adopt a contact-tracing app, and that data flows viewed as most appropriate (in this case, individual health data flowing to health-based actors) is seen as the most appealing. The larger the number of users who adopt a contact-tracing app, the more effective it is (Kreps, *et al.*, 2020). Thus, ensuring that the data collected by the app are normatively aligned with the distributor is vital as users are more comfortable adopting an app if the distributor is an actor who is trusted to maintain appropriate transmission principles when it comes to personal health data. These findings offer policy implications for which distributors should be issuing contact-tracing apps and suggest that an inter-operable ecosystem of partnered apps may help maximize adoption.

In addition to viewing an actor's collection of certain types of data, trust plays an important role in assessing whether CI has been violated, as violations of the contextual integrity of information flow have been shown to impact trust in institutions negatively (Martin, 2018). For example, individuals' trust that transmission principles will be preserved informs what they consider appropriate data flows; if a data breach, for example, reveals to consumers that their data were not properly secured, their trust in that actor will be negatively impacted. In the survey, we measured respondents' trust in actors by asking whether they had a great deal, some, or hardly any confidence in four institutions' ability to respond to the pandemic: medical system, local government, federal government, and business leaders. Confidence in the medical system was positively correlated with willingness to adopt an app, and to adopt apps from the two healthcare distributors (HPAs and health insurers). Likewise, we found that confidence in the federal government and state government was associated with one's willingness to adopt apps from those distributors, which highlights trust's role in accepting an information flow, even when the actor and context are not directly aligned. The role that this (mis)alignment plays in evaluations of a contact-tracing app is especially apparent when looking at people's willingness to adopt any of the proposed apps. When controlling for other factors, only trust in the medical system predicted one's willingness to download a COVID-19 tracking app.

CI offers a unique view into why certain distributors of health tracking apps are trusted over others. Recognizing the importance of transmission principles, Nissenbaum (2010) notes how technological solutions often violate the principle of confidentiality that has historically been at the core of medical practice "in the name of improved healthcare delivery and medical outcomes" [6]. CI reminds us that the transmission principles governing norms of information flow matter, and that not just any distributor supporting public health will be deemed acceptable. As individuals remain skeptical of the ability of government and industry to manage their health data safely, our findings confirm that those who have a historical and ethical commitment to maintaining the contextual integrity of existing transmission principles will be most trusted, even when faced with a global pandemic.

CI also asks for a wider examination of the moral and political implications of new information flows to make a more complete assessment as to whether technology should be allowed or resisted. Nissenbaum (2010) urges consideration of more than just adherence to transmission principles, but also that we consider how new practices and information flows might pose threats to autonomy and freedom, asking: "What might be the effects on power structures, implications for justice, fairness, equality, social hierarchy, democracy, and so on?" [7]. When considered in this vein, even if competing contact-tracing apps collect and process the same information in the same ways, the broader commitment of HPAs to support public health poses less of a moral or political risk to Americans than those of government or industry, with the latter considered more likely to engage in practices that might unfairly impact individuals (Auxier, *et al.*, 2019).

Examining our findings more broadly sheds light on some individual differences worth further discussion. The role of respondent age across our models is notable since younger respondents were less willing to adopt any contact-tracing app although this does not hold once we control for institutional trust. This age finding appears counterintuitive given the general embrace of technology and apps by the younger populace, but there are several possible explanations. This could be due to the early belief that younger people were less susceptible to COVID-19 and thus had no need to even consider a tracking app, or perhaps a general distrust among younger Americans in key institutions; data from the Pew Research Center highlights that young adults have the lowest trust in elected officials, law enforcement, and business leaders than any other age group (Gramlich, 2019). Indeed, the fact that age is no longer significant once we control for institutional trust suggests this may well be the case.

The other standout finding was that respondents with higher Internet skills were more willing to adopt an app from all distributors except health insurance providers. This suggests that for these participants, their comfort and perceived savviness with Internet technologies might give them the confidence to address any possible privacy concerns related to contact-tracing apps, even when distributed by actors lacking a longstanding commitment to maintaining transmission principles within the healthcare context.

Limitations and future work

While getting an early account of individuals' trust in institutions and willingness to download a COVID-19 tracking app is important, one limitation of this study is that the American public's understanding of COVID-19 and how best to respond to the growing pandemic was still evolving in April 2020. For example, we suggest that young people may have expressed less willingness to use a contact-tracing app because young people were initially seen as being at low risk; since that time, this belief has been disproven (Rabin, 2020) and may have changed younger adults' attitudes toward apps. Future work could compare later opinions with these early results to determine any changes in the public's trust and willingness to embrace contact tracking.

An additional limitation relates to the broad wording of the primary question posed to respondents about their willingness to install a tracking app. Again, as data collection occurred prior to general public awareness of approaches offered by Apple/Google and related providers, the question was silent as to the specificity of locational data that would be collected (GPS location, Bluetooth proximity to other users, etc), how long data would be retained, who might have access, and so on (Redmiles, 2020). Leveraging the various parameters that contribute to preserving contextual integrity, future work could include measures across various possible data attributes.

There are also potential limitations concerning the relationship of participants to COVID-19. There was nothing in the survey invitation to suggest that it was a study about the pandemic and thus related interest or lack thereof should not have driven participation. While we asked a question about following coronavirus-related news, we do not have assessments of people's concern about catching the virus or its repercussions for their personal lives nor whether they even believe COVID-19 to be a real threat to anyone. In the future, such questions about pandemics should be included.

Conclusion

When making decisions about technological interventions to resolve a crisis like COVID-19, there are a number of important questions that should be addressed during the design process. Contextual integrity provides a useful framework through which to identify and address the appropriateness of data flows between the users (in this case, the

American public) and the provider of that technology.

In this paper, we found that while two-thirds of our respondents indicated a willingness to download a COVID-19 tracking app to stop the spread of the virus, the institution distributing the app affected said willingness. Distributors already operating in health contexts were most frequently selected, and trust in the medical system's ability to respond to the pandemic was positively associated with willingness to adopt. Viewed through the lens of contextual integrity, the appropriateness of how a contact-tracing app might disrupt personal information flows was tied to a distributor's ability to respect and preserve existing transmission principles: a health protection agency was preferred over other government or industry bodies presumably because such an agency is already entrusted with ensuring patient confidentiality.

Our findings suggest that policy-makers and technology developers alike need to recognize that merely promising to protect individual privacy is not sufficient to ensure that the contextual integrity of our health information is preserved. Instead, developers and regulators must consider several factors related to who is collecting the data, whether data transmission between the sender and recipient is perceived as appropriate, and what underlying principles guide these disclosures. Individuals expect the preservation of longstanding transmission principles within the health context, and providers entering from outside that context, even during a global pandemic and with the best of intentions, may not be trusted (Nissenbaum, 2010). Furthermore, solutions proposed by these institutions may be met with skepticism when there have been prior breaches of contextual integrity; in the U.S., the public has consistently reported low trust in government and industry following Edward Snowden's revelations about government spying (Lupton and Michael, 2017), as well as data breaches like Facebook's Cambridge Analytica scandal (Kahn and Ingram, 2018).

In the case of COVID-19, we recommend that tools that collect sensitive personal information — including location data like GPS or Bluetooth proximity information, as well as health and contact data — provide clear guidance on not just what data are being collected, but also what actors will access that data, how long that data will be kept, and what limitations will be placed on uses of the data. Ensuring the actors involved in data collection have clear connections to the health context is one way to increase trust in the tool, as is engaging in data minimization practices to ensure that contact-tracing apps do not become a part of the larger "function creep" happening with mobile data. To establish trust, these data should only be used for the narrow purpose of minimizing the spread of COVID-19 and deployed by distributors with a longstanding commitment to preserving the confidentiality of health data without extending to other forms of surveillance and monitoring of individuals. In combination, these design guidelines can help encourage the adoption of COVID-19 apps from trustworthy distributors that can limit the spread of the virus and protect the public, both in terms of their health as well as their privacy.

About the authors

Eszter Hargittai is professor and holds the Chair of Internet Use & Society in the Department of Communication and Media Research, University of Zurich. Her research looks at inequalities in Internet use with a special focus on differences in people's Web-use skills. She is editor of *Research exposed: How empirical social science gets done in the digital age* (New York: Columbia University Press, 2020).
E-mail: pubs [at] webuse [dot] org

Elissa M. Redmiles is Faculty Member & Research Group Leader at the Max Planck Institute for Software Systems. She leads the Safety & Society research group, which focuses on understanding and mitigating inequities that arise in users' digital safety-related decision-making processes and experiences. She is also the Founder & Principal of Human Computing Associates, a research consulting firm.
E-mail: eredmiles [at] gmail [dot] com

Jessica Vitak an associate professor in the College of Information Studies at the University of Maryland, College Park. Her research evaluates the privacy and ethical implications of big data and develops tools to help people make more informed decisions when using new technologies and sharing sensitive data.
E-mail: jvitak [at] umd [dot] edu

Michael Zimmer is an associate professor in the Department of Computer Science at Marquette University. His work focuses on digital privacy, Internet research ethics, data ethics, and the broader social & ethical dimensions of emerging technologies.
E-mail: michael [dot] zimmer [at] marquette [dot] edu

Acknowledgements

The authors would like to thank Marina Micheli for her helpful input.

Notes

1. Cook and Schilke, 2010, p. 104.

2. Westin, 1967, p. 7.

3. Marwick and boyd, 2014, p. 1,063.

4. Nissenbaum, 2019, p. 227.

5. Nissenbaum, 2019, p. 231.

6. Nissenbaum, 2010, p. 175.

7. Nissenbaum, 2010, p. 182.

References

American National Election Studies, 2020. "The ANES guide to public opinion and electoral behavior," https://electionstudies.org/resources/anes-guide/, accessed 6 October 2020.

M. Anderson and B. Auxier, 2020. "Most Americans don't think cellphone tracking will help limit COVID-19, are divided on whether it's acceptable," *Pew Research Center* (18 April), ar https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/, accessed 6 October 2020.

B. Auxier, L. Raine, M. Anderson, A. Perrin, M. Kumar, and E. Turner, 2019. "Americans and privacy: Concerned, confused and feeling lack of control over their personal information," *Pew Research Center* (15 November), at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, accessed 6 October 2020.

J.B. Barney and M.H. Hansen, 1994. "Trustworthiness as a source of competitive advantage," *Strategic Management Journal*, volume 15, number S1, pp. 175–190.
doi: https://doi.org/10.1002/smj.4250150912, accessed 6 October 2020.

A.J. Berinsky, M.F. Margolis, and M.W. Sances, 2014. "Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys," *American Journal of Political Science*, volume 58, number 3, pp. 739–753.
doi: https://doi.org/10.1111/ajps.12081, accessed 6 October 2020.

Centers for Disease Control and Prevention, 2020. "CDC's response to support state, tribal, local, and territorial health departments" (15 May), at https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/response-corps.html, accessed 6 October 2020.

K.S. Cook and O. Schilke, 2010. "The role of public, relational and organizational trust in economic affairs," *Corporate Reputation Review*, volume 13, number 2, pp. 98–109.
doi: https://doi.org/10.1057/crr.2010.14, accessed 6 October 2020.

M.J. Culnan, 1993. "'How did they get my name?' An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, volume 17, number 3, pp. 341–363.
doi: https://doi.org/10.2307/249775, accessed 6 October 2020.

M.J. Culnan and R.J. Bies, 2003. “Consumer privacy: Balancing economic and justice considerations,” *Journal of Social Issues*, volume 59, number 2, pp. 323–342.
doi: https://doi.org/10.1111/1540-4560.00067, accessed 6 October 2020.

Á. Díaz, 2020. “Coronavirus, location tracking, and civil liberties,” *Brennan Center for Justice* (7 April), at https://www.brennancenter.org/our-work/analysis-opinion/coronavirus-location-tracking-and-civil-liberties, accessed 6 October 2020.

T. Dinev and P. Hart, 2006. “An extended privacy calculus model for e-commerce transactions,” *Information Systems Research*, volume 17, number 1, pp. 61–80.
doi: https://doi.org/10.1287/isre.1060.0080, accessed 6 October 2020.

eHealth Network, 2020. “Mobile applications to support contact tracing in the EU’s fight against COVID-19: Common EU toolbox for member states” (15 April), at https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf, accessed 6 October 2020.

J. Ermisch, D. Gambetta, H. Laurie, T. Siedler, and S.C. Noah Uhrig, 2009. “Measuring people’s trust,” *Journal of the Royal Statistical Society: Statistics in Society. Series A*, volume 172, number 4, pp. 749–769.
doi: https://doi.org/10.1111/j.1467-985X.2009.00591.x, accessed 6 October 2020.

P. Finkelman, 2003. “Limiting rights in times of crisis: Our Civil War experience — A history lesson for a post-9–11 America,” *Cardozo Public Law, Policy & Ethics Journal*, volume 2, number 25, pp. 25–48.

F. Fukuyama, 1995. *Trust: The social virtues and the creation of prosperity*. New York: Free Press.

Google/Apple, 2020. “Privacy-preserving contact tracing,” at https://www.apple.com/covid19/contacttracing, accessed 6 October 2020.

J. Gramlich, 2019. Young Americans are less trusting of other people — and key institutions — than their elders, *Pew Research Center* (6 August), at https://www.pewresearch.org/fact-tank/2019/08/06/young-americans-are-less-trusting-of-other-people-and-key-institutions-than-their-elders/, accessed 6 October 2020.

E. Hargittai and A. Marwick, 2016. “‘What can I really do?’ Explaining the privacy paradox with online apathy,” *International Journal of Communication*, volume 10, at https://ijoc.org/index.php/ijoc/article/view/4655, accessed 6 October 2020.

E. Hargittai and Y.P. Hsieh, 2012. “Succinct survey measures of Web-use skills,” *Social Science Computer Review*, volume 30, number 1, pp. 95–107.
doi: https://doi.org/10.1177/0894439310397146, accessed 6 October 2020.

C.P. Hoffmann, C. Lutz, and G. Ranzini, 2016. “Privacy cynicism: A new approach to the privacy paradox,” *Cyberpsychology*, volume 10, number 4, article 7.
doi: https://doi.org/10.5817/CP2016-4-7, accessed 6 October 2020.

J.B. Imber, 2008. *Trusting doctors: The decline of moral authority in American medicine*. Princeton, N.J.: Princeton University Press.

C. Kahn and D. Ingram, 2018. “Americans less likely to trust Facebook than rivals on personal data: Reuters/Ipsos poll,” *Reuters* (25 March), at https://www.reuters.com/article/us-usa-facebook-poll/americans-less-likely-to-trust-facebook-than-rivals-on-personal-data-reuters-ipsos-poll-idUSKBN1H10K3, accessed 6 October 2020.

L. Kelion, 2020. “Coronavirus: UK contact-tracing app is ready for Isle of Wight downloads,” *BBC News* (4 May), at https://www.bbc.com/news/technology-52532435, accessed 6 October 2020.

G. King and L. Zeng, 2001. “Logistic regression in rare events data,” *Political Analysis*, volume 9, number 2, pp. 137–163.
doi: https://doi.org/10.1093/oxfordjournals.pan.a004868, accessed 6 October 2020.

S. Kreps, B. Zhang, and N. McMurry, 2020. “Contact-tracing apps face serious adoption obstacles,” *Brookings Institution* (20 May), at https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles/,

accessed 6 October 2020.

R.S. Laufer and M. Wolfe, 1977. “Privacy as a concept and a social issue: A multidimensional developmental theory,” *Journal of Social Issues*, volume 33, number 3, pp. 22–42.
doi: https://doi.org/10.1111/j.1540-4560.1977.tb01880.x, accessed 6 October 2020.

D. Lupton and M. Michael, 2017. “‘Depends on who’s got the data’: Public understandings of personal digital dataveillance,” *Surveillance & Society*, volume 15, number 2, pp. 254–268.
doi: https://doi.org/10.24908/ss.v15i2.6332, accessed 6 October 2020.

K. Martin, 2018. “The penalty for privacy violations: How privacy violations impact trust online,” *Journal of Business Research*, volume 82, pp. 103–116.
doi: https://doi.org/10.1016/j.jbusres.2017.08.034, accessed 6 October 2020.

A.E. Marwick and d. boyd, 2014. “Networked privacy: How teenagers negotiate context in social media,” *New Media & Society*, volume 16, number 7, pp. 1,051–1,067.
doi: https://doi.org/10.1177/1461444814543995, accessed 6 October 2020.

M. Murray, 2019. “Poll: Americans give social media a clear thumbs-down,” *NBC News* (5 April), at https://www.nbcnews.com/politics/meet-the-press/poll-americans-give-social-media-clear-thumbs-down-n991086, accessed 6 October 2020.

S. Nellis and P. Dave, 2020. “Apple, Google ban use of location tracking in contact tracing apps,” *Reuters* (4 May), at https://www.reuters.com/article/health-coronavirus-usa-apps-idUSL1N2CM1AA, accessed 6 October 2020.

C. Newton, 2020. “Tech companies could face more pressure to share location data with governments to fight coronavirus,” *The Verge* (20 March), at https://www.theverge.com/interface/2020/3/20/21186772/coronavirus-location-sharing-government-israel-england-facebook-google-o2, accessed 6 October 2020.

H. Nissenbaum, 2019. “Contextual integrity up and down the data food chain,” *Theoretical Inquiries in Law*, volume 20, number 1, pp. 221–256, and at http://www7.tau.ac.il/ojs/index.php/til/article/view/1614, accessed 6 October 2020.

H. Nissenbaum, 2010. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford Law Books.

M. Pirson, K. Martin, and B. Parmar, 2019. “Public trust in business and its determinants,” *Business & Society*, volume 58, number 1, pp. 132–166.
doi: https://doi.org/10.1177/0007650316647950, accessed 6 October 2020.

R.D. Putnam, 2000. *Bowling alone: The collapse and revival of American community*. New York: Simon & Schuster.

R.C. Rabin, 2020. “Coronavirus may pose a new risk to younger patients: Strokes,” *New York Times* (14 May), at https://www.nytimes.com/2020/05/14/health/coronavirus-strokes.html, accessed 6 October 2020.

L. Rainie and M. Duggan, 2016. “Privacy and information sharing,” *Pew Research Center* (14 January), at https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/, accessed 6 October 2020.

L. Rainie, S. Keeter, and A. Perrin, 2019. “Trust and distrust in America,” *Pew Research Center* (22 July), at https://www.pewresearch.org/politics/2019/07/22/trust-and-distrust-in-america/, accessed 6 October 2020.

E.M. Redmiles, 2020. “User concerns & tradeoffs in technology-facilitated contact tracing,” *ACM Digital Government: Research and Practice*, volume 1, number 4 (October); see also *arXiv*:2004.13219v3 (12 May), at https://arxiv.org/abs/2004.13219v3, accessed 6 October 2020.

L. Robinson, S.R. Cotten, H. Ono, A. Quan-Haase, G. Mesch, W. Chen, J. Schulz, T.M. Hale, and M.J. Stern, 2015. “Digital inequalities and why they matter,” *Information, Communication & Society*, volume 18, number 5, pp. 569–582.
doi: https://doi.org/10.1080/1369118X.2015.1012532, accessed 6 October 2020.

J.B. Rotter, J.E. Chance, and E.J. Phares, 1972. *Applications of a social learning theory of personality*. New York:

Holt, Rinehart and Winston.

E. Selinger and W. Hartzog, 2016. “Facebook’s emotional contagion study and the ethical problem of co-opted identity in mediated environments where users lack control,” *Research Ethics*, volume 12, number 1, pp. 35–43. doi: https://doi.org/10.1177/1747016115579531, accessed 6 October 2020.

K. Servick, 2020. “Cellphone tracking could help stem the spread of coronavirus. Is privacy the price?” *Science* (22 March), at https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price, accessed 6 October 2020.

I. Sherr, 2020. Apple, “Google give a look at coronavirus tracking tech, promise more privacy protections,” *CNET* (5 May), at https://www.cnet.com/news/apple-google-give-a-look-at-coronavirus-tracking-tech-promise-more-privacy-protections/, accessed 6 October 2020.

H.J. Smith, T. Dinev, and H. Xu, 2011. “Information privacy research: An interdisciplinary review,” *MIS Quarterly*, volume 35, number 4, pp. 989–1,016.

B. Tau, 2020. “Government tracking how people move around in coronavirus pandemic,” *Wall Street Journal* (28 March), at https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202, accessed 6 October 2020.

C. Timberg, D. Harwell, and A. Safarpour, 2020. “Most Americans are not willing or able to use an app tracking coronavirus infections. That’s a problem for Big Tech’s plan to slow the pandemic,” *Washington Post* (29 April), at https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic/, accessed 6 October 2020.

J. Turow, M. Hennessy, and N. Draper, 2015. “The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation,” *Annenberg School for Communication, University of Pennsylvania*, at https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and, accessed 6 October 2020.

T. Van Green and A. Tyson, 2020. “5 facts about partisan reactions to COVID-19 in the U.S.,” *Pew Research Center* (2 April), at https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and, accessed 6 October 2020.

S.D. Warren and L.D. Brandeis, 1890. “The right to privacy,” *Harvard Law Review*, volume 4, number 5, pp. 193–200.
doi: https://doi.org/10.2307/1321160, accessed 6 October 2020.

A.F. Westin, 1967. *Privacy and freedom*. New York: Atheneum.

Wikipedia, 2020. “Template: COVID-19 pandemic data/United States medical cases,” at https://en.wikipedia.org/w/index.php?title=Template:COVID-19_pandemic_data/United_States_medical_cases&oldid=958144654, accessed 6 October 2020.

World Health Organization, 2020. “WHO Director-General’s opening remarks at the media briefing on COVID-19 — 11 March 2020,” at https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020, accessed 6 October 2020.

World Health Organization, 2017. “Contact tracing” (9 May), at https://www.who.int/news-room/q-a-detail/contact-tracing, accessed 6 October 2020.

Editorial history

Received 9 September 2020; revised 11 September 2020; revised 14 September 2020; accepted 20 September 2020.

Americans' willingness to adopt a COVID-19 tracking app: The role of app distributor
by Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer.
First Monday, volume 25, number 11 (November 2020).
doi: https://dx.doi.org/10.5210/fm.v25i11.11095