The University of Chicago

Privacy in a Public Health Emergency:

An Analysis of Shifting Data Privacy Preferences during the COVID-19 Pandemic

By: Alia Shahzad

April 15, 2020

A thesis submitted for partial fulfillment

of the requirements for a Bachelor of Arts degree in

Public Policy Studies

Preceptor: Rachel Dec

Abstract

Prior pandemic-era privacy studies have asked research subject for their willingness to share (WTS) health and location data with contact-tracing applications. However, no contemporary studies have surveyed for changes in WTS across other types of data attributes from the pre- to during-COVID window. Through hypothesis testing, regressions, and qualitative coding of responses from a survey administered to a randomly selected pool of 500 respondents about their WTS data attributes before and during COVID-19, I find that WTS most data attributes has generally decreased during the pandemic, excepting willingness to share health and location information with government data-collecting bodies, which has increased. Qualitative responses suggest that this exception might be due to an increased amount of time spent online as well as a heightened sense of moral obligation to share data for the public good. Privacy preferences are also found to vary with political party affiliation, highlighting emergent research axes for privacy theory. These results inform privacy policymaking in the pandemic era. Policymakers should implement a comprehensive national privacy policy, COVID-era policy that specially protects users from private industry threats, and update protected data classes to match users' quickly changing preferences.

Acknowledgements

I am indebted to Rachel Dec, as well as Professors Jessica Vitak, Michael Zimmer, and Marshini Chetty, whose valuable comments and support made this paper possible.

This thesis is dedicated to my parents, who paid in love and labor for my freedom, dignity, and security, as well as to Amaya and Jibran, for whom I hope to do the same.

Table of Contents

Introduction

Legal scholar Alan Westin writes in *Privacy and Freedom*, a foundational text in the privacy studies field, "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists".[1] In some ways, this comment remains true today. Despite the proliferation of privacy studies in the decades following *Privacy and Freedom*'s publication, there is still no consensus in the social sciences on the subject, nor a means of arriving at one. Is privacy a fundamental civil right, equal to such beloved American ideals as liberty and equality, or is it something that we might sacrifice in pursuit of more sacrosanct goods? In a digital world that increasingly blurs private and public spaces, how do we pinpoint privacy's ever-changing definition? More practically, how can policymakers keep pace with rapidly advancing technological development and the increasing privacy incursions that accompany it?

These problems appear in the first American legal treatise of privacy, which called for the right "to be let alone" as a defense against the invention of the instantaneous photograph in 1947 — setting a precedent for the legal enshrinement of privacy rights only *after* a major technological development has infringed upon them.[2] In the 1950s, wiretapping, too, entered the public consciousness as a "national problem".[3] But come the mid-1960s, the technology became perceived as "necessary evil" in the interest of national security in the Cold War effort. The ACLU subsequently failed to block a bill permitting wiretapping by law enforcement in 1968, after successfully suing to defeat such legislation in earlier decades.[4] Congress itself also

[1] Westin, *Privacy and Freedom*.
[2] Warren and Brandeis, "The Right to Privacy."
[3] White, "A Brief History of Surveillance in America."
[4] "ACLU History."

struggled to reach an agreement about regulation. Should wiretapping be permitted for use by security agencies by their discretion, allowed under safeguards, or banned outright?[5] Here began the start of the struggle to position privacy within a hierarchy of American values — in this, case, national security — that demand privacy's sacrifice.

The national security versus privacy debate continued into the 9/11 era, when the Patriot Act permitted extensive data mining of private and public data sources to public opposition, particularly from the Islamic community and its allies.[6] Concern mounted after the revelation of the Snowden Papers in 2013, which confirmed that security agencies around the world were monitoring the most minute of their citizens' daily activities, as well as increased media coverage of private corporations' conversion of personal data into "revenue streams".[7] In a 2019 Pew survey, 81% of Americans said they have little to no control over data collected about them by companies, and 70% of adults said their personal data is less secure than it was in the past.[8] In sum, historically, political events and revelations have always played an active role in shaping the public's perception of their right to privacy.

Today, the COVID-19 pandemic presents another historical turning point for the popular conception of privacy. Citizens' personal information, and particularly their location and health data, are crucial components of curbing the disease's spread. Already, government bodies receive citizens' anonymized cell phone location data from the mobile industry.[9] In order to safely curb the spread, it is important that data privacy regulations allow for the continued

[5] Barber and Westin, *Effective Social Science : Eight Cases in Economics, Political Science, and Sociology*.
[6] Busch, "Internet and Privacy."
[7] Busch.
[8] Auxier, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information."
[9] Diaz, "Coronavirus, Location Tracking, and Civil Liberties | Brennan Center for Justice."

collection of this information; a lack of public data has already inhibited public health officials from tracking and spreading contagion.[10] On the other hand, these policies should not incur on internet users' right to privacy, nor risk setting a precedent for invasive data collection that could endure in the post-COVID era.

The existing American policy is not promising. Unlike other democracies, such as the European Union, which secured continental data privacy laws with its General Data Protection Regulation (GDPR), the US lacks a centralized data privacy legislation.[11,12] Each state regulates its own data collection and processing; only three states give residents some degree of control over their personal data, including Illinois and California.[13] Recognizing the special risk COVID-19 poses, this summer, two major privacy bills were introduced on the Senate floor — the COVID-19 Consumer Data Protection Act of 2020, by the Republican party, and the Public Health Emergency Privacy Act, by the Democratic party. Both bills died on the floor. The issue is thought to be a high priority for the Biden administration, as Vice President Kamala Harris's career history is cluttered with privacy advocacy.[14]

Effective privacy legislation in the wake of the COVID-19 pandemic must address citizens' privacy preferences particular to the new era. But as the history of the privacy field demonstrates, the theory of privacy evolves in tandem with new technologies and political currents. Understanding the depth of these preferences is no simple task. With the work and school day conducted entirely online via Zoom, the use of contact tracing and other digital health

[10] Vestal, "Lack of Public Data Hampers COVID-19 Fight."
[11] However, privacy preferences differ widely across international lines; citizens of East Asian countries are generally more willing to share data than US citizens (Zhao 2018). This suggests an ideal privacy policy should be localized to the particular country employing it.
[12] Bellman et al., "International Differences in Information Privacy Concerns."
[13] Turner, "47 States Have Weak or Nonexistent Consumer Data Privacy Laws."
[14] Bryan, "Election 2020."

monitoring applications, and the increased reliance on the internet to fulfill daily tasks from grocery shopping to banking, there are many new technologies that have eased the burden of the pandemic. But as privacy expert Angel Diaz writes for the Brennan Center, "The impulse to turn to high-tech tools in this time of crisis is understandable… At the same time, history offers ample reason to proceed with caution."[15]

In this study, I aim to understand how internet users' conceptions of online and offline privacy have evolved over the last year. I draw on existing theories, including Westin's three-pronged Privacy Identity Index and Helen Nissenbaum's contextual integrity, to analyze the results of a public opinion poll about privacy preferences during the pandemic. I hope that my work will serve as a fruitful resource for legislators and privacy experts crafting privacy policies in the post-COVID era.

[15] Diaz, "Coronavirus, Location Tracking, and Civil Liberties | Brennan Center for Justice."

Literature Review

In this literature review, I lay out the theory of contextual integrity (CI), the most widely used model of privacy in contemporary user-based studies, and analyze existing studies that use CI principles. Next, I explain the relevance of CI to designing privacy studies in the unique conditions of the COVID era. I then summarize and highlight shortcomings of privacy surveys and exploratory research published during the pandemic. I conclude by laying the foundation of — and potential challenges to — my own study.

Contextual Integrity: An Introduction

Privacy studies sits at the intersection of a rich multitude of fields: computer science, media and information studies, law, public policy, and philosophy, among others. Scholars must be able to write fluently about many of these disciplines at once, translating theory and ethics into actionable policy and user design. Helen Nissenbaum, an Information Sciences professor at Cornell University and leading expert on privacy studies, is one such multi-specialist. Nissenbaum's *Privacy in Context: Technology, Policy, and the Integrity of Social Life* draws from law, information studies, and ethics to introduce contextual integrity (CI), her groundbreaking framework for defining privacy that has influenced a generation of experimental research projects and theoretical treatises.

Prior to the publication of *Privacy in Context*, privacy theorists generally asserted that public and private spheres were strictly split and distinct, and that privacy preferences in one context were "universally" applicable to others.[16] CI rejects this binary system to propose that privacy expectations are governed by norms of appropriate information flows. These norms

[16] Vitak and Zimmer, "More Than Just Privacy."

differ from context to context, tied to the characteristics of a particular social environment the actor operates within.[17] By extension, norms also evolve within their contexts, influenced by new technological developments or lynchpin events, such as the post-9/11 surveillance of mosques by federal security agencies. Prior to 9/11, these practices would likely have been considered infringements on religious expression.

CI is the most widely applied theory in contemporary experimental and observational privacy preference studies. A simple Google Scholar search of "privacy studies" reveals that the most widely-cited publications in turn cite Nissenbaum in their bibliographies.[18, 19, 20] Here, I analyze two experimental studies with CI-informed design principles that successfully unearth user concerns.

Leon et. al's 2013 research asked participants to visit health websites with different privacy policies and levels of reputability, and then asked about their willingness to share 30 types of personal information with the platform. Researchers found that more restrictive privacy policies made users more comfortable with sharing information, while reputability of the website had no effect on willingness to share.[21] Notably, Leon's study specified a field — health care — for participants to ground their preferences in, a crucial element of CI-informed research. This also makes the study's conclusions applicable to the COVID era: to incentivize more sign ups, contact-tracing and other health data applications should employ rigorous privacy policies, rather than relying on brand name reputability.

[17] Nissenbaum, "Privacy as Contextual Integrity."
[18] Tan and Sharif, "Comparing Hypothetical and Realistic Privacy Valuations."
[19] Zimmer, "Addressing Conceptual Gaps in Big Data Research Ethics."
[20] Abaquita et al., "Privacy Norms within the Internet of Things Using Contextual Integrity."
[21] Leon et al., "What Matters to Users?"

However, the applicability of Leon et. al's study is somewhat limited. As the authors themselves note, their conclusions have "limited generizability" outside of health data-related privacy concerns.[22] Their research focused solely on a health care website and also a single data-collecting body: the advertising agency affiliated with the health care company. Broadening the experiment to include other types of actors and contexts would make the results more relevant to the COVID case, informing contact-tracing leaders what sorts of information-collecting bodies and platforms are adequate to meet the public's privacy preferences.

In another CI-oriented study, *Privacy Norms and Preferences for Photos Posted Online*, participants were shown ten images of perceived public rooms (living rooms, kitchens) and perceived private (bedrooms, bathrooms) in the household sphere. Each image showed different combinations of individuals (singles or couples), or no people present. Participants were asked for their judgement about whether each photo was shareable on various online platforms. By examining participants' privacy norms, researchers hoped to gain insight into the "broader social dimensions of privacy", examining the ways that emerging technologies and digital platform alter social behavior.[23]

Hoyle et al.'s study demonstrates that context is a restraining factor of privacy behavior, as varying factors such as perceived privacy of the room and number of people present altered participants' expressed preferences. The researchers' finding is particularly influential on this study. Likewise, I also vary the type of data shared, as well as the actors hosting the information flow, though this research uses survey-based rather than experimental design. My study also builds on Hoyle's work to examine how participants' perceptions of the privacy of different

[22] Leon et al.
[23] Hoyle et al., "Privacy Norms and Preferences for Photos Posted Online."

physical spaces varies in the COVID-19 era, when contexts that were previously construed as private, such as the bedroom, have become ostensibly public backdrops for video calls during the work and/or school day.

Contextual Integrity for the COVID Era

In March, after the first case of COVID-19 appeared in New York City, Mayor Bill de Blasio all but identified patient zero by name on his Twitter account, providing the patient's seven-person law firm and school attended by his children to all 1.65 million of his followers. Twitter users quickly identified the patient by name, as well as the hospital supervising his treatment. The Mayor met a maelstrom of criticism for his post, which he later deleted. But De Blasio is not alone in his faux pax. The pandemic presents a whole host of new social norms regarding information flows in a variety of contexts, from online workspaces to contact-tracing applications to social media, that actors are learning to navigate on the go.

CI, which asserts that an individual's idea of privacy is set within a set of social conditions that are subject to continual change over time, is particular poignant in this climate. In an exploratory analysis, privacy experts Aaron Brough and Kelly Martin gesture towards the privacy research opportunities in the pandemic era and usefulness of CI in filling these gaps. In their paper, they note how the pandemic response has eroded privacy rights through surveillance tools to monitor COVID cases, new digital records, and government-initiated sharing of personal data.[24] Increased opportunities for breaches is likely to ensue. My research fills the gap in this

[24] Brough and Martin, "Consumer Privacy During (and After) the COVID-19 Pandemic."

exploratory paper, testing Brough and Martin's hypothesis by asking internet users' whether their concerns have in fact evolved due to the pandemic.

Other preliminary treatises on privacy during the COVID-19 pandemic also underscore the relevance of CI in approaching the era's challenges. James Andrew Lewis, Director of Strategic Technologies at the Center for International and Strategic Studies, a respected D.C.-based think tank, notes that the pandemic has amplified the different standards that public and private information-collecting bodies are held to in the legal and policy realms.[25] Policies like the Health Insurance Portability and Accountability Act (HIPAA) tightly constraint the sorts of data that the government can collect on its citizens, while private companies are given practically free reign over commodifiable personally identifiable information after users sign over their rights through obtuse privacy policies.

"The imbalance between highly regulated government use of personal data and lightly regulated commercial use dates to the 1980s and no longer makes sense," Lewis writes, pointing to the fact that privacy policies were developed well-before modern technologies have encroached on users' data.[26] But it's also likely, he notes, that there are some benefits of health surveillance during the COVID-19 pandemic that might continue to create a demand for this information in the post-COVID era. Figuring out the right balance between data surveillance necessary for the public good and protection from data-collecting bodies requires careful attention to changing user sensitivity to data collection, a primary objective of this study.

Prior work on user sensitivity has found that users generally perceive personally-identifying information as more sensitive — information such as zip code or political preference

[25] Lewis, "Big Company, Big Government, Big Brother?"
[26] Lewis.

is less sensitive than name or address.[27] However, user perception of what constitutes personally-identifying information does not always align with the reality of a rapidly technologically advancing world. [28] Willingness to share data types that were previously perceived as less personally-identifiable will likely change as users realize that, in fact, it takes very little digital information to be linkable to an offline identity. Accordingly, this study varies the types of data, also known as data attribute, tested in the survey field, ranging from name to social media network.

Two leading privacy experts in the field, Jessica Vitak (University of Maryland) and Michael Zimmer (Marquette University), use Nissennbaum's CI to evaluate long-term risks from COVID-19 surveillance in their 2020 guidelines for ensuring privacy during the pandemic, arguing that "the appropriateness of sharing data with third parties to support public health will be contextually dependent".[29] For instance, Google resisted requests from state governments who wanted to make use of application data to build a broad picture of population movements, recognizing that users would be wary of a private company collecting personally-identifiable location data. Instead, Google used Bluetooth technology, which is not personally-identifiable, to track proximity between two phones, adhering to user expectations of privacy norms.

Broadly, Vitak and Zimmer's treatise demonstrates how CI adds nuance to the rapidly changing COVID context. Even in the midst of a public health emergency, the company is loath to violate existing transmission principles to collect and analyze data that could alleviate the pandemic's effect, choosing instead to bow to user preferences. As users become increasingly aware of privacy violations and grow increasingly opposed to companies that violate privacy

[27] Malheiros, "'Fairly Truthful': The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure | SpringerLink."
[28] Schomakers et al., "Internet Users' Perceptions of Information Sensitivity – Insights from Germany."
[29] Vitak and Zimmer, "More Than Just Privacy."

norms, companies might be forced to self-regulate their privacy infringements or risk losing consumers. However, this self-regulation is limited to when infringements are in the public eye, such COVID contact tracing. Ultimately, a policy solution is necessary to track all violations, including those that are less visible.

Privacy Surveys Amidst the Pandemic

It will take decades, if not centuries, for researchers to parse through the aftermath of the COVID-19 pandemic. In recognition of this moment's significance, survey firms and research teams have seized the opportunity to record data and lay the crucial groundwork for what will surely become a sobering but informative academic concentration.

In a study of public opinion examining how organizational privacy and data protection practices have been affected by the pandemic, 933 privacy professionals were surveyed by the International Association of Privacy Professionals (IAPP) Study in May of 2020. The IAPP found that one of the "biggest challenges" brought by the pandemic were the new technologies or contracts with new vendors to enable remote work 2020.[30] They also found that employers had significantly increased the types of data on file about employees, including information about personal travel and symptoms. About a fifth of employers had shared information about which employees had tested positive for COVID-19 with local or state governments or other employees. While the study's goals differ from this one's — the average employee/internet user will have different concerns and outlooks than a privacy professional — it nonetheless reveals that serious challenges have ensued from the movement of the workplace to the online sphere.

[30] Fazlıoğlu, "Privacy in the Wake of Covid-19."

In a series of surveys conducted in April of 2020, as the pandemic was just starting to shut down parts of the US, Pew polled citizens for their views on government monitoring of cell phone data of individuals who have tested positive for COVID-19. Respondents were split down the line, with 52% agreeing this was acceptable, and 48% unacceptable. However, the poll inquired about respondents' comfort in a sole case: cell phone location data collection by the federal government. This is a significant limitation, as there are many other types of data that might be collected, as well as other privacy-collecting bodies.

Two major academic public opinion surveys centered on contact tracing and privacy during the pandemic were released in 2020. Zhang et al. asked 2000 American adults about their support for COVID-19 surveillance measures and found that most respondents supported traditional (non-digital) contact tracing methods. Contact tracing apps and monitoring of personal digital devices received less support.[31]

In a published working paper published by reputable privacy experts, Simko et. al asked for individuals' responses to a similar survey in a longitudinal study conducted weekly from April to June of 2020. Like Zhang's study, Simko focused on unearthing global public opinion on an ideal contact-tracing application's capabilities, as well as which organization should be responsible for this application's design. They found that participants strongly disagreed about the ideal application and designer, making it difficult to find a "perfect solution".[32] Overall, informed consent, that is, the ability to articulate "meaningful" consent and control over data,

[31] Zhang et al., "Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic."
[32] Simko et al., "COVID-19 Contact Tracing and Privacy."

was most likely to make people enroll in contact-tracing apps. Simko also found that these preferences were "stable over time at a population level".[33]

Notably, both of these studies focused solely on perceptions of digital and non-digital contact-tracing methods by presenting variations on a contact tracing application and testing for which option was most palatable for users. While it is important and CI-friendly to contextualize the platform and information flows in question, Zhang's lack of variance in actors (who's receiving the data) and Simko et al's lack of variance in types of information (name, zip code, email address, etc.) leaves much room for study. How has users' willingness to share *other* types of information been altered by the ongoing pandemic?

Furthermore, Simko et. al's finding that preferences were "stable over time" refers to a time period *after* the pandemic began; many European countries (which were included in their sample) were already on lockdown when researchers started collecting responses. Thus, the study fails to perform a before/during comparison of privacy preferences. This is useful, if not essential, data. An observable change in preferences from before to during the pandemic is a strong indicator (though not perfect proof) that preferences vary as a *result* of the pandemic. Of course, there's no perfect way to obtain prior-held opinions after the fact, but it is still possible to approximate these opinions by asking respondents about their past biases, as is attempted in this study.

The Research Gap

Under the CI framework, accurate privacy studies must specify data-sharing contexts rather than propose generic and ungrounded research questions (e.g., "How private of a person

[33] Simko et al.

are you?"). Most relevantly, two CI-informed pandemic-era studies have surveyed respondents for their willingness to share (WTS) health and location data with contact-tracing applications.[34, 35] I broaden the lens of these studies by surveying for privacy preferences across a range of data attributes, from name to social media accounts, as well as across the pre- and during- COVID time frames. This variation endows this study with the ability to compare trends in WTS across different types of data. Responses about more sensitive data attributes that internet users are likely less willing to share (such as address) yields a baseline against which to compare responses about less sensitive data attributes that users are likely more willing to share during the pandemic (such as health data).

Furthermore, while much CI-based privacy research has varied and carefully scrutinized different information flow norms, data-collecting bodies, and types of data, few have introduced actor demographics as a factor that could also impact data-sharing norms. By collecting demographics data and regressing it against the change in WTS, this study looks to introduce actor demographics as a potential new contextually-variant factor that affects privacy preferences in addition to information flow norms and data attributes.

Multiple limitations complicate the execution of this study. Principally, the study design prevents the quantitative analysis from coming to any causal conclusions between explanatory and outcome variables, limiting findings to correlations. Qualitative coding of survey respondents offers an opportunity to explore possible causal mechanisms.

Other limitations include sampling diversity, which is limited to domestic respondents, and a few methodological restraints I outline in the Findings section.

---

[34] Zhang et al., "Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic."
[35] Simko et al., "COVID-19 Contact Tracing and Privacy."

Data and Methods

Data Collection

The data for this study relies on de-identified survey responses collected in January of 2021 amidst the COVID-19 pandemic. The 44-question long survey (n = 500) was published on Qualtrics and distributed by Amazon Mechanical Turk, a crowdsourcing platform that links researchers to a randomized pool of respondents. Participants were paid $1 to take the approximately ten-minute survey in accordance with recommended compensation levels ($6/hour) in the industry.

The survey flow begins with demographic questions, including basic demographic categories (age, race, level of education, political affiliation, etc.), COVID-19 specific questions (such as beliefs about wearing masks), and a set of questions to identify privacy identity (per the Westin privacy index).[36] Demographics are followed by a series of questions about respondents' privacy preferences for sharing seven types of data: name, zip code, home address, smartphone location data, health information, political preferences, and social media network. Data type — also known as data attributes — are important factors to specify and vary across in CI-based privacy survey design, as some data types (e.g., name) are generally perceived to be less sensitive than others (e.g., home address). Furthermore, to avoid biasing participants to responding with more privacy-conscious answers, questions are phrased to avoid using the word "privacy", and instead asking participants about their "willingness to share".[37]

Participants are presented with a total of four variations in the WTS section:

[36] Hoyle et al., "Privacy Norms and Preferences for Photos Posted Online."
[37] Simko et al., "COVID-19 Contact Tracing and Privacy."

(1) sharing with a *government* entity *prior* to the pandemic;

(2) sharing with a *government* entity *during* the pandemic;

(3) sharing with a *private* entity *prior* to the pandemic;

(4) sharing with a *private* entity *during* the pandemic.

Varying data-collecting bodies is another important contextual factor to specify in CI-based privacy surveys, as respondents might feel differently about sharing data with public and private bodies. Longitudinal data from questions about pre- and during-COVID preferences offers insight into preference shifts over time.

Finally, respondents were also prompted to answer a qualitative question asking them to explain their evolution and/or stasis in preferences. Other questions asked about respondents' changes in work life, such as comfort with sharing physical space via video conferencing platforms and employers' use of remote work monitoring systems. These questions did not make it into this analysis due to space constraints. (See Appendix for full text of this survey).

Data Analysis

I use a combination of quantitative and qualitative analysis for this study. I begin with a basic pre- and during-correlation, examining changes in pre- and during-COVID willingness to share for each type of data (zip code, social media network, smartphone location data, political preferences, name, home address, and health location) and data-collecting body (public or private) surveyed. I examine, broadly, whether WTS increases or decreases over time for these variables.

Next, I use a Wilcoxon-signed rank test to test for the differences in before and during pandemic WTS health data responses. The Wilcoxon-signed rank test is a non-parametric alternative to the paired t-test and is commonly used for ordinal, non-normally distributed dependent variables (such as Likert data), making it the most appropriate statistical test for this dataset. Like a t-test, the Wilcoxon-signed rank test is a difference in means test, in that it also assesses whether population means differ across matched pairs. In this case, each pair consists of an individual's change in WTS health data with the government from pre- to during- COVID and the same individual's change in WTS health data with private companies.

I then look to qualitative responses to open-ended survey questions asking for explanations about respondents' change or stasis in privacy preferences during the COVID-19 pandemic. I sort these responses by respondents' change in WTS — increased, decreased, or no change — summarizing themes in responses and presenting a handful of relevant responses.

Finally, I run a series of Ordinary Least Squares (OLS) regressions to test for correlation between a selected explanatory variable (political party affiliation) and WTS.

Findings

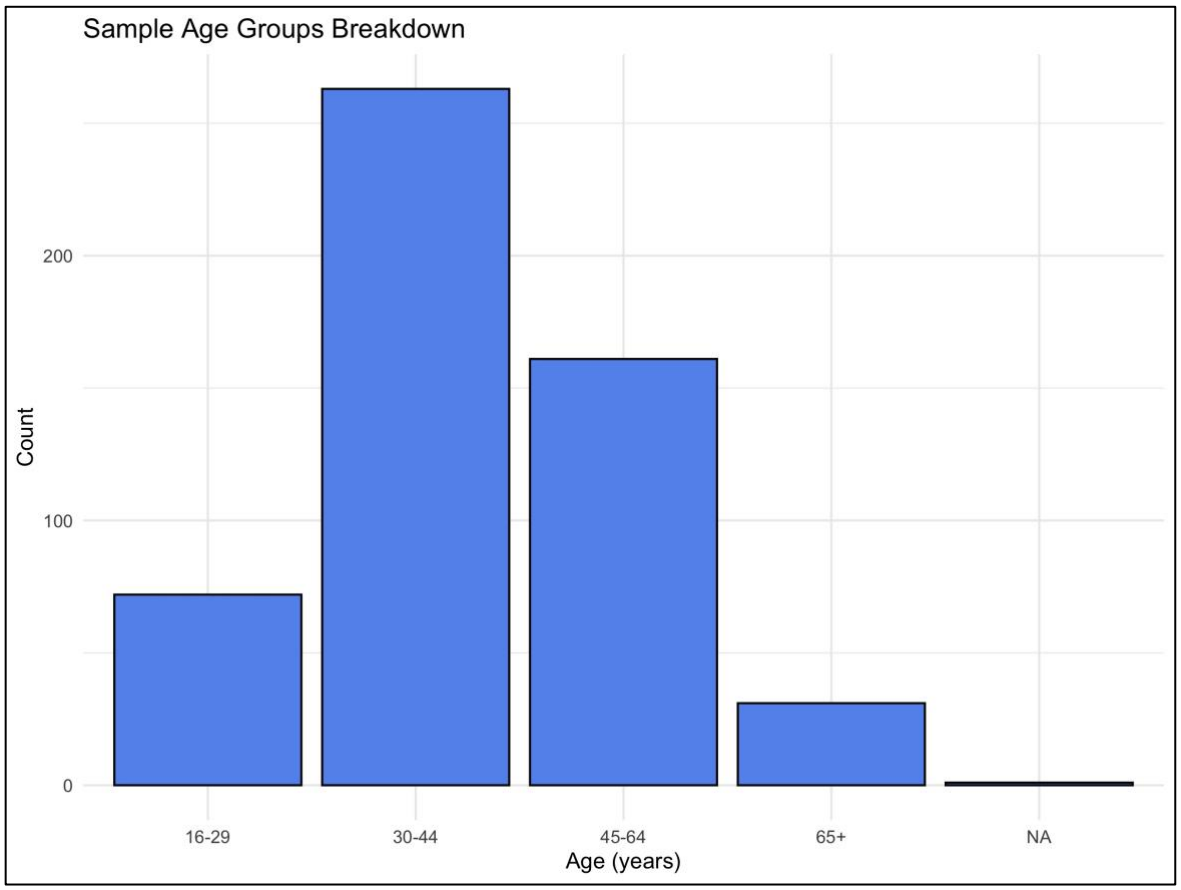
This data analysis investigates how internet users' willingness to share (WTS) different types of personal data with private and public data-collecting bodies changed during COVID-19. I examine differences in internet users' WTS data with the private and public sectors before and during the pandemic through statistical analysis. I then seek possible explanations for these trends using qualitative responses. Next, I connect respondent groups to their respective levels of WTS, revealing variations in trends at the level of political affiliation. Finally, I discuss the implications of my findings under the framework of contextual integrity and consider the limitations of my research. I start by presenting the survey respondents.

A total of n = 519 participants answered the survey. Of the respondents, 19 were excluded for completing the survey in less than 90 seconds, the cut off point for ability to comprehend and respond accurately to survey questions (average time of completion was seven minutes). This analysis focuses on the remaining 500 participants.

Respondents' age range was 18 to 98. The median age was 39 years old. (See **Fig 0.1** for age group breakdowns). A majority of respondents identified as male, though the difference between the numbers of male and female-identifying respondents is small. The majority of respondents held a 4-year bachelor's degree. (See **Fig 0.2** for education breakdowns). Most participants (250) identified as Democrats and a smaller group (131) identified as Republicans, while 109 respondents identified as Independents. The asymmetry of political identification counts is consistent with political differences between MTurk and population-based samples found in other studies. [38] This is not a cause for concern as MTurk respondents do not differ

[38] Levay, Freese, and Druckman, "The Demographic and Political Composition of Mechanical Turk Samples."

fundamentally from population-based respondents despite apparent differences.[39] The majority of respondents reported working from home, a significant group reported working in person, and a smaller group reported being laid off.



[Figure 0.1]

[39] Levay, Freese, and Druckman.

Education Frequency Table

Education	Count
Not a High School Graduate	5
High School Graduate of equivalent (e.g. GED)	94
In Process of Completing Associate's or Bachelor's Degree	13
Associate's Degree (2-year program)	75
Bachelor's Degree (4-year program)	246
Graduate Degree	78
Postgraduate Degree	16
	1

[Table 0.2]

	Privacy Identity Categories on the Westin Index			
	Unconcerned *(Extremely unconcerned)*	**Pragmatists** *(Concerned with nuance)*		**Fundamentalists** *(Extremely concerned)*
Consumers have lost all control over how personal information is collected and used by companies.	Agree	Agree	Disagree	Disagree
Most businesses handle the personal information they collect about consumers in a proper and confidential way.	Disagree	Agree	Disagree	Agree
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	Disagree	Agree	Disagree	Agree

[Figure 0.3]

On the Westin Privacy Identity Index, a widely-used scale for indexing research subjects' privacy preferences, respondents are assigned a privacy identity based off of their levels of agreement with three statements (listed in **Figure 0.3**). Privacy fundamentalists feel "very strongly about privacy matters", believing they have lost their right to privacy, and "are strongly resistant to any further erosion of it".[40] On the other end of the spectrum, privacy unconcerned have little to no anxiety about data-collecting entities infringing on their privacy rights. In between these two groups are the privacy pragmatists, who also have strong feelings about privacy and are concerned about the "abuse or misuse" of their data. However, unlike privacy fundamentalists, they permit access to their data when they understand and agree with its use.

[40] Taylor, "Most People Are 'Privacy Pragmatists' Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits."

Most respondents (81.4%) identified as privacy pragmatists, commensurate with findings in prior privacy studies.[41] (See **Table 0.4** for privacy identity category breakdowns).

Privacy Identity on Westin Index

Identity Category	Count
fundamentalist	60
pragmatist	430
unconcerned	38

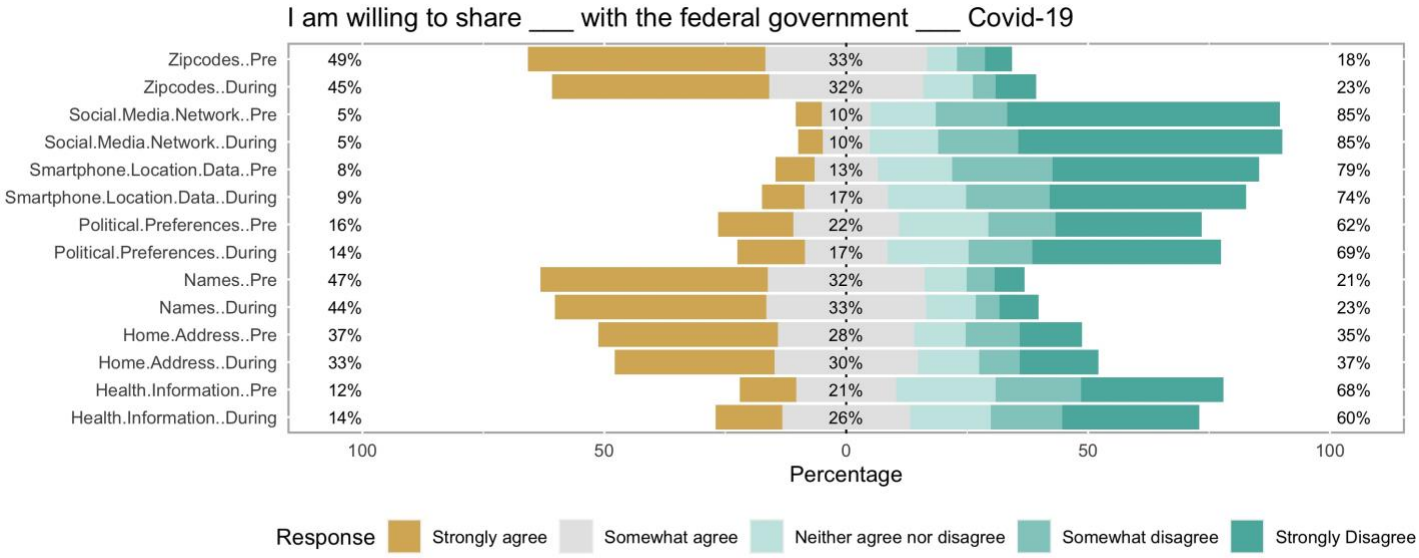
[Table 0.4]

[41] Kumaraguru and Cranor, "Privacy Indexes: A Survey of Westin's Studies."

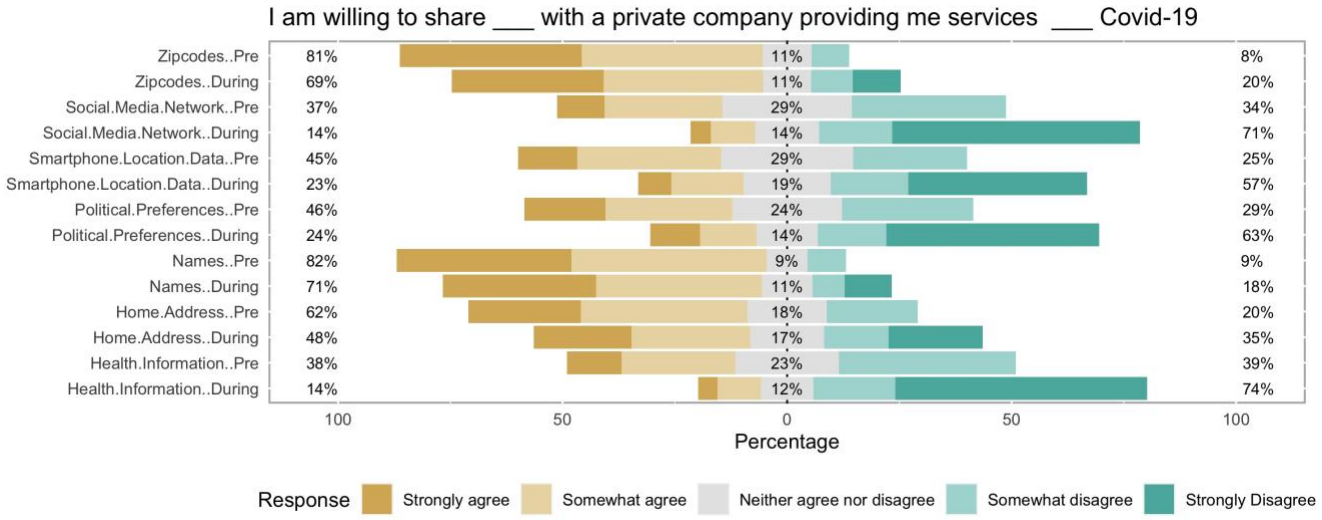
Willingness to Share: Quantitative Analysis

In this section, I focus on the difference between WTS health and smartphone location data to the public and the private sectors prior to COVID-19. Health and location data are selected for two reasons. Firstly, the sharing of this data is the most relevant to the conditions of the pandemic. Secondly, health and smartphone location data are the only types of data sampled for which respondents reported a significant *increase* in WTS during the pandemic. **Figures 1.1** and **1.2** shows changes in WTS over all data types sampled, with the federal government and private sector respectively, on Likert scale plots.

Notably, WTS all data types with private companies decreased during the pandemic, and WTS all data types besides health and smartphone location data with the government also decreased during the pandemic. From-top level observation of the figures below, the decrease in WTS with private companies appears to be larger than the decrease in WTS data with public data collecting bodies, indicating that respondents are generally more concerned about privacy infringement by private companies than government incursions.



[Figure 1.1]



[Figure 1.2]

Respondents' increase in concern correlated with an increased amount of time spent online. The mean number of hours spent online over the sampled period increased from 7.05 hours to 8.35 hours. Respondents also reported that tasks that were performed offline pre-pandemic, such as work or their children's' school days, were moved online. Of the participants working from home, 34% reported working more hours during COVID-19 than they did previously, and 17% reported that their employer implemented digital monitoring tools to supervise their remote work. I further discuss the potential link between the increased amount of time spent online and the observed decrease in WTS in the next section using qualitative data.

The results of the Wilcoxon-signed rank test confirms that the decrease in WTS with private companies is larger than the decrease in WTS data with the government. The null hypothesis (H_0) for the test is as follows:

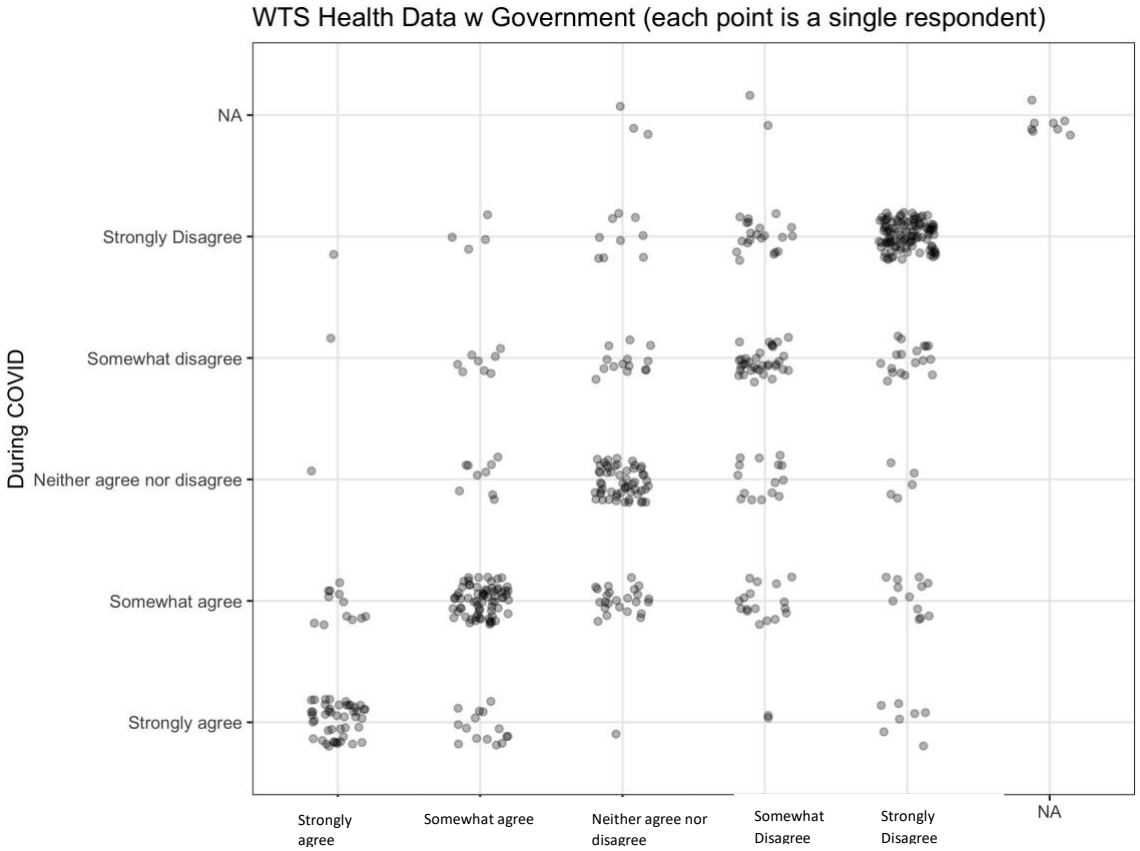
> H_0: The average difference in pre- and during WTS health data with the government is *identical* to the average difference in pre- and during- WTS health data with the private industry.

The alternative hypothesis (H_1) for the test is as follows:

> H_1: The average difference in pre- and during WTS health data with the government is *non-identical* to the average difference in pre- and during- WTS health data with the private industry.

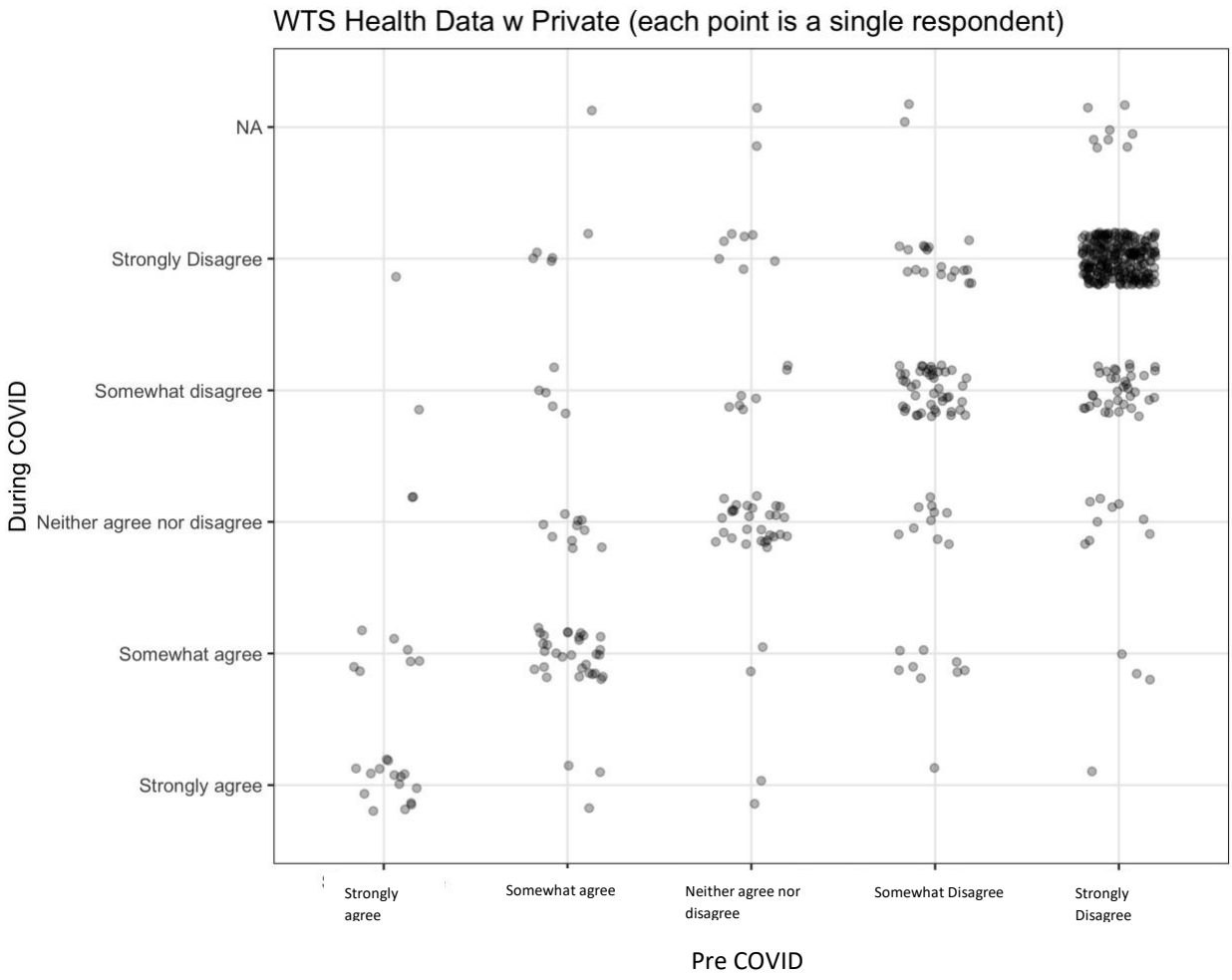
The significance threshold used for the test was p = .05, the standard accepted significance threshold for social science research. The calculated p-value (0.0014) for the test was less than the significance threshold, rejecting the null hypothesis (H_0) and supporting the alternative hypothesis (H_1) that the average difference in pre- and during-COVID-19 WTS health data with the government is non-identical to the average difference in pre- and during-COVID-19 WTS health data with the private industry.

In sum, the results of the Wilcoxon-signed rank test indicate that respondents' change in privacy preference varied significantly between sharing with the public and private sectors. Generally, respondents are more comfortable sharing data with the government. This trend is also observable from the two paired correlation plots below. The first plot compares the mean WTS with government pre- and post-pandemic **(Fig 1.3).**



[Figure 1.3]

The second plot compares the mean WTS health data with private companies pre-pandemic and during the pandemic **(Fig 1.4).**



[Figure 1.4]

Comparing the strongly disagree pre COVID, strongly agree during COVID region of both figures, significantly more respondents became more WTS with the government than with private companies.

In sum, quantitative analysis supports Nissenbaum's contextual integrity theory for privacy research. Varying across data attributes, data-collecting bodies, and temporal context

revealed subtle changes in respondents' WTS that would have gone undsicovered with more generic, decontextualized privacy questions. This conclusion also has important implications for legislators writing privacy policies, as well as future instances of government contracting with private industry to produce contact-tracing or health data applications. I examine these implications in the Policy Recommendations section.

Willingness to Share: Qualitative Responses

Qualitative responses provide an explanation for the finding that, generally, respondents are less WTS all data types other than health and location data, and even then, only with the government.

When respondents who demonstrated less WTS during the pandemic were prompted to explain what changed their "privacy preferences and/or privacy behavior during the COVID-19 pandemic" at the survey's conclusion, most replied with an answer relating an increased amount of time spent online with increased vulnerability to security breaches. (See Appendix II: Selected Qualitative Responses for a table listing all the quotes cited in this section). One respondent said, "Spending more time online will give people more of a chance to get my information so I am very concerned about giving too much away." Another respondent focused on the impact of time spent on video communications platforms on the boundaries of physical privacy: "My privacy behavior changed during the COVID-19 pandemic because I spend more time working from home and more time video chatting at home. This makes me more self-conscious of sharing my surroundings to others."

A smaller group of respondents who demonstrated less WTS during the pandemic did not connect their change in preference to increased internet usage, but instead to an unrelated increased cognizance of potential threats. For instance, one respondent said their privacy preferences grew stronger after learning about "the constant data breaches, attacks, and weaknesses in IT infrastructure." This rationale is ostensibly independent of the conditions of the pandemic, as the change in perception of privacy risks is contingent on knowledge they could have acquired even if the pandemic had not occurred, unlike the respondents who explicitly pointed to increased time spent online due to the pandemic as the source of their preference shift.

Respondents who reported an increase in WTS (again, principally in health and location data) usually cited moral or ethical reasoning as the primary cause of their preference shift. One respondent said, "I'm trying to aid agencies gathering more data to the best of my ability in order to aid COVID-19 cases." This response could explain why there appears to be a difference in WTS with the government and private industries — namely, respondents distinguish government monitoring to be in the express purpose of public health, while private companies do not fall within this moral scope. It might also explain why respondents were more WTS smartphone and location data, which could be perceived as most relevant to contact-tracing applications. As another respondent said, their preferences changed, "To help the government learn more about my health status."

Some respondents explicitly weighed ethical concerns against privacy rights or acknowledged that they had to make some sort of sacrifice to meet the information-sharing needs of the health emergency. One respondent put this sentiment bluntly: "People's health and wellbeing is more important than privacy." Similarly, another respondent said, "Times are different, and I need to adjust to what's needed today."

Notably, a number of respondents also reported that their preferences remained unchanged during the pandemic. Of the respondents with static preferences, few proffered explanations beyond "My preferences did not change". The selected few who did expressed a different understanding of the relationship (or lack thereof) between catastrophic events and security. One respondent, "My preferences have not changed. Security risks are not dependent upon world events, rather, they are dependent upon the method or vehicle in which information is shard and how vulnerable it is." In other words, the health emergency on its own is not necessarily consequential enough as to affect WTS. Other respondents attributed their lack of concern to their status as average citizens. One respondent said, "I'm just a regular dude. No one cares what I'm doing. My privacy isn't a concern."

A smaller proportion of static respondents expressed a resignation to the inevitability of privacy infringement regardless of their preferences — a group Nissenbaum would call privacy cynics.[42] One respondent said, "I don't think my privacy preferences and/or privacy behavior has changed all that much. I figure if someone wants my information bad enough, they'll find a way to steal it." Others expressed an even deeper resignation that the status quo cannot be altered. Another respondent stated, "Any policy put in place to protect my privacy can be ignored by those in power."

In sum, while qualitative responses indicate that the pandemic affected respondents' preferences differentially, a few explanations for the quantitative trends emerge. Generally, respondents who are less WTS cite concerns about increases in privacy vulnerability as they spend more time online during the pandemic. Those who report that they are more WTS largely

[42] Nissenbaum, "Privacy as Contextual Integrity."

attribute this change to a moral obligation to share data with the government during a public health emergency, possibly explaining why WTS health and location data with public bodies defied the general downwards trend in WTS for all other categories.

These findings have strong implications for privacy policy. If respondents report being willing to sacrifice their right to privacy for the sake of a public health emergency, then policy makers should consider the creation of exceptional privacy laws that make these data attributes easier to share during emergency situations. Furthermore, the finding that respondents vary in their WTS indicates that creating choice frameworks that allow users to opt-in or opt-out of contact-tracing policies is ideal for the many users who do not want to share any data.

Political Affiliation and Privacy Preferences

Seeking to explain outcomes in WTS with political affiliation revealed subtle and unexpected differences between groups' preferences, namely that Republicans are more likely to disagree that they are willing to share cell phone location with the government than Democrats. The tables below present the summary statistics of an OLS regression with political party as the explanatory variable and WTS smartphone location (**Figure 3.1**) and health (**Figure 3.2**) data with the government. WTS is scaled from 1 (respondent strongly disagree they are WTS) to 5 (respondent strongly agrees they are WTS).

Linear Regression Sum Statistics

Variable	Coefficient	SE	T-Statistic	P Value
(Intercept)	3.38	0.088	38.49	0.000
PolPartyIndependent	0.62	0.159	3.92	0.000
PolPartyNonaffiliated	0.48	0.267	1.78	0.075
PolPartyOther (specify below)	1.45	0.562	2.58	0.010
PolPartyRepublican	0.31	0.150	2.07	0.039

[Figure 3.1: Linear Regression Sum Statistics for WTS *Location* Data with Government During COVID-19]

Linear Regression Sum Statistics

Variable	Coefficient	SE	T-Statistic	P Value
(Intercept)	2.85	0.091	31.35	0.000
PolPartyIndependent	0.64	0.164	3.87	0.000
PolPartyNonaffiliated	0.32	0.276	1.17	0.243
PolPartyOther (specify below)	1.32	0.581	2.27	0.024
PolPartyRepublican	0.66	0.155	4.27	0.000

[Figure 3.2: Linear Regression Sum Statistics for WTS *Health* Data with Government During COVID-19]

Using the linear regression formula,

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3$$

Republicans are more likely to disagree they are WTS location data ($y \mid x_1 = 1$) than Democrats (average WTS represented by $\beta_0 = 3.38$) by 0.31 points on the Likert scale. This is approximately one-third of the distance between any two points on the Likert scale, e.g., between "strongly disagree" and "somewhat disagree". Republicans are more likely to disagree they are WTS health data ($y \mid x_1 = 1$) than Democrats (average WTS represented by $\beta_0 = 2.85$) by 0.66 points on the Likert scale.

Similar trends appear for Republican WTS name, zip code, and home address with the government, though no correlation was found between political affiliation and WTS political preferences or social media network. Regressions run with pre-COVID WTS as the outcome variable yielded significantly lower values of β_1 but approximately the same β_0 for name, zip code, home address, and health data as the during-COVID regressions, indicating that the partisan gap in WTS increased during the pandemic. Interestingly, no significant correlation was found for pre-COVID WTS cell phone location data with the government, indicating that the sharing of this data attribute has become politicized over the last year. Furthermore, no statistically significant relationship between political affiliation and WTS health and location data with *private* industries after the pandemic was found.

These finding demonstrates that the calculus used to make privacy preferences varies with political groups *only* when the data-sharing body in question is the government. Timeline also clearly makes a difference in the equation. Within the span of a year, Republicans and Independents demonstrated larger changes in preference than their Democratic counterparts.

How might these correlations be explained? One feasible possibility is that the transfer of

the office of the presidency to the Democratic party and the loss of the Republican majority in the Senate decreased Republicans' trust in the government to secure private information. However, it is ultimately outside of the scope of this study to look for a causal mechanism behind this trend.

Discussion

In one possible read of COVID's impact on data privacy preferences, users become *more* comfortable sharing private information. As internet users are forced to move day-to-day activities from in-person to online, they become more accustomed to sharing information they might not have been comfortable sharing online pre-pandemic. For instance, increased usage of online banking requires sharing more financial data with banking websites as opposed to with a teller. Increased usage of food delivery applications such as GrubHub requires sharing personal addresses with third-party apps instead of local restaurant owners.

The results of this study defy this expectation. Individuals have generally become less willing to share information, *except* for health and smartphone location data, and even then, specifically exclusively with public data-collecting bodies. One reason for this, as qualitative data indicates, is that many users became more aware of threats to their data privacy as data that might not have previously been digitized (e.g., meetings, classes, family reunions) all went digital during the pandemic, increasing the amount of data shared by users.

Furthermore, making sweeping generalization about trends in users' WTS is ultimately a fruitless task. Claims about WTS are contingent on political affiliation, context (pre-/during-COVID), data type, and data-collecting body. When respondents who demonstrated change in WTS asked to provide their rationale, they took a step beyond asking themselves: *is this data*

private or public? Instead, they largely focused their explanations on the ways that COVID has impacted their data-sharing context — such as spending more time online, or the moral implications of choosing to share or not share. In other words, to make their decisions, respondents were asking themselves a more specific question: *What new factors have the pandemic introduced to the data-sharing context, and against this changing context, what type of information is it necessary that I share?*

This finding is in strong alignment with CI theory. To reiterate, CI rejects a binary system of private versus public data to propose, instead, that privacy expectations are governed by data attributes, actors, and norms of appropriate information flows. Importantly, norms "differ from context to context, tied to the characteristics of a particular social environment the actor operates within".[43] By extension, then, these norms also evolve *with* their associated context's evolution, as the results of this study demonstrate. While respondents were largely less WTS most data attributes with any data-collecting actors during COVID than pre COVID, in alignment with trends unearthed in prior studies about trends in WTS during the pandemic, [44] the increase in WTS health and location data with the public bodies point to a new transmission principle tied to the context of COVID. Internet users are, to some extent, willing to compromise their personal privacy preferences for the sake of a public interest they perceive to be greater than their own — but they only trust the government, and not private companies, with their data.

This finding has important implications for policymakers. As Zimmer and Vitak note in their paper, "Thinking about privacy through the lens of CI forces us to reject simplistic arguments like 'since you're sharing health information with some, you're okay with sharing it

[43] Nissenbaum.
[44] Auxier, "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information."

with anyone.'"[45] Policymakers must be careful to specify the particular conditions — when, with who, and what types of data — sharing can occur in the instance of future public heath epidemics that require large-scale contact tracing and public health monitoring. If consumers do not trust private companies with their health and smart phone location data, then private companies should not be allocated the role of collecting and analyzing such data.

The finding that respondents who reported a change in privacy preferences attributed this change to factors like more time spent online and a sense of moral obligation due to the pandemic also has an important implication for privacy policy. If these factors are capable of causing respondents' preferences to evolve rapidly over short periods time during crisis, we might ask, what happens when the lockdown ends and risk of contagion decreases, people presumably revert to spending less time online, and there is no moral obligation to share location and health data? In short, we cannot conclude that the finding reached by quantitative analysis — that people are more willing to share health and location data, and less willing to share other types of data — constitutes a status quo that will endure beyond the conditions of the pandemic. This underscores the danger of function creep, the gradual widening use of information for something other than its original purpose.[46] Currently, users might accept the widening collection and analysis of certain types of personal data, but policymakers must recognize that the norm that they build policy around today might change by the time a given bill lands on the floor. Future post-pandemic research is necessary to updating understanding of users' preferences.

Finally, if WTS increasingly differs with political affiliation, coming to a data privacy policy that satisfies all users becomes complicated. Should policy makers cater to the group who

[45] Vitak and Zimmer, "More Than Just Privacy."
[46] Vitak and Zimmer.

is most anxious about sharing location and health data, despite the ongoing public emergency's demand for this information? Or should they respect the wishes of the majority of users who are willing to compromise on their personal privacy for the sake of the public good?

To answer this question, I propose a new dimension of CI called *privacy preference groups.* A privacy preference group is made up of individuals who generally share the same privacy preferences when faced by a given context. Multiple privacy preference groups would respond to the same privacy context with different levels of WTS, such as Republicans being less WTS location and health data with the government than Democrats during COVID. This distinction adds to the existing CI theory by incorporating into its vocabulary recent findings that group psychology hugely impacts privacy preferences.[47] Beyond this study, privacy preference groups might be useful in investigating other demographic groups' change in privacy preferences following significant events, such as Muslims' WTS after the Bush Era "Muslim Registry", which Trump proposed renewing in 2016.[48]

Counterclaims & Limitations

The most reasonable counterclaim to this study is methodological: generally, survey respondents report preferences that are different from the preferences they act on in the real-life context. Proponents of this theory, known as the privacy paradox, might argue that the results of this study lack external validity, and the conclusions of this thesis do not apply outside of the observational study environment. A privacy paradox supporter would argue that the only way to conclude that privacy preferences have changed due to COVID is via a randomized control trial. A control group living in a counterfactual world that did not experience the COVID-19 pandemic

[47] Stuart, Bandara, and Levine, "The Psychology of Privacy in the Digital Age."
[48] Lind, "Donald Trump's Proposed 'Muslim Registry,' Explained."

would take the survey, and their results would be compared to the preferences of a treatment group living in this world to conclude a casual influence (or lack thereof) of the pandemic on WTS.

However, conducting an RCT is impossible in the constraints of the pandemic — no one has been untouched by the disease's grasp. It is true that sans an RCT, this study can only conclude correlation — the observed differences in WTS from pre COVID-19 to during COVID-19 time periods might have occurred *regardless* of the pandemic's occurrence, due to some other confounding factor that was not recorded or analyzed in this study. Given the natural limits of the experimental environment, observational data offers the best (and only) alternative to an RCT to answer the proposed research question. Qualitative response data offers another means of pointing to potential casual links between the pandemic and WTS for future studies, though they cannot independently establish causality. Furthermore, the specific concerns of the privacy paradox have recently been debunked, indicating that differences between reported and actual privacy preferences are not as significant as previous studies have suggested.[49]

The sampling method also potentially undermined the accuracy of this study. Prior studies have found issues with using Amazon MTurk as a sampling method, primarily due to concerns about MTurk workers being significantly younger, better educated, and more liberal than the rest of the US population.[50] However, the sample surveyed was fairly large (n = 500), and demographic analysis indicated it to be largely representative of the US population of internet users. Furthermore, perfectly random sampling is difficult, if not impossible, in real world scenarios, especially when the survey method uses online distribution. Even if MTurk is

[49] Tkacik, "Overcoming the Privacy Paradox."
[50] Chandler et al., "Online Panels in Social Science Research."

not the perfect solution, it is the most effective. Importantly, this critique underscores the limitation that respondents are from the US, and likely mostly maintain American conceptions of privacy. On average, American privacy preferences varies significantly from other nations.[51] This study's findings are thus not applicable to other countries.

Finally, asking participants to accurately reveal today the preferences that they held a few months ago is less ideal than asking participants for preferences a few months ago when they actually held them. The incongruence between reported and factual priors could be a type of response bias. Future iterations of studies with similar research questions might consider re-using surveys from the pre-pandemic time period to conduct the same survey during the pandemic, and matching respondents across these time periods to statistically test for changes in preference.

[51] Schomakers et al., "Internet Users' Perceptions of Information Sensitivity – Insights from Germany."

Policy Recommendations

Based on the results of this study, I suggest the implementation of comprehensive privacy legislation, with special rules amidst the pandemic regulating private industry data collection, by the federal government in the long run-term state governments in the short-term. I also recommend the consistent, contextual integrity-conscious updating of legislation to match evolving user preferences and point to shortcomings in the bills proposed during the pandemic. I then call for more research into addressing the differential privacy needs of privacy preference groups, as well as reassurance from policymakers to their constituents that their data will not be used for non-public health related purposes. Finally, I outline the roadblocks to designing and implementing comprehensive privacy legislation.

The majority of survey respondents identify as privacy pragmatists on the Westin privacy index, indicating most internet users have strong feelings about their privacy and are concerned about protecting their data from misuse. They are also willing to allow data-collecting bodies access to their data *only* when they understand and agree with the purpose of its collection. Further quantitative analysis shows that users are less willing to share nearly every type of data with both private industry and the government during the pandemic than they were before the pandemic. In sum, users agree want more control over how their personal information is collected and used by public and private industries, as well as the ability to specify what type of data is being shared and who it is being shared with. Comprehensive data privacy legislation is the only way to satisfy this need.

There is no consensus in the field on the contents of comprehensive data privacy legislation, but most privacy advocates generally agree it must entail a list of 15 rights and

regulations.[52] From the results of this study, I underscore the need for two related regulations: the restriction of processing bodies, and the limitation of purpose & processing. Users are currently more WTS health and location information than they were prior to the pandemic — but only if the government is the entity collecting the data. Legislation must reflect this preference; consumers should be able to opt out from private industry data collection and processing of health and location data, even if it is collected for public health purposes.

Furthermore, policymakers should limit the scope of information processing to ensure that data collected for the sake of public health is not misused for any purposes unrelated to public health. Both of the two pandemic-era data protection bills proposed in 2020 made this specification, though neither bill passed.[53] The need to fill this gap in privacy protections, in light of the findings of this study, is particularly urgent.

At the very least, in recognition of the fact that users' WTS health and location data is directly tied to conditions of the pandemic, policymakers should mandate deletion of this information after the public health emergency concludes. While this study did not make any definite conclusions about users' future WTS, extrapolating from the reasons that respondents cited for their change in preferences, such as moral obligation and more time spent online, WTS will likely decrease after the emergency concludes and the moral obligation to share vanishes.

Who should be responsible for writing and implementing this policy? Ideally, in the long run, the federal government will fill this role. Currently, outside of industry-focused federal laws regulating the health, financial, and selected public sectors, as well as data belonging to children, most of the internet remains unregulated by the federal government, much like "the wild, wild

[52] Turner, "47 States Have Weak or Nonexistent Consumer Data Privacy Laws."
[53] Kerry, "Game On."

west," as one Congressional staffer told a privacy advocacy group. [54] Privacy is instead regulated by state legislatures, creating a landscape that varies wildly from state-to-state. The majority of states have very weak digital privacy laws, very much out of line with the users' increasing reluctance to share data found in this study. [55] Ultimately, the internet is not siloed on a state-by-state basis. To adequately satisfy user preferences, comprehensive privacy legislation must operate on the national landscape.

However, in the short-run, states are better suited for undertaking comprehensive privacy legislation reform. As Washington state Sen. Reuven Carlyle told GovTech, it could take years for a gridlocked Senate to pass comprehensive privacy legislation.[56] States, on the other hand, have more rapid policy pipelines, as well as the flexibility to experiment with new policies. Already, states are on the vanguard of the privacy legislation: take the California Consumer Privacy Act, which meets half of the 15 recommended privacy rights and regulations generally agreed on by privacy advocates, a significant increase to the measly two met by existing national laws.[57] Other states like Illinois and New York have taken similar steps to shore up protections.[58]

Any new privacy legislation must also factor in this study's finding that users' preferences changed during the pandemic. Most users are currently willing to compromise on their privacy preferences for the sake of the public good, but what about after the pandemic? Protected classes of data in privacy bills must be updated in accordance with changing information flow norms and contexts.

---

[54] Turner, "47 States Have Weak or Nonexistent Consumer Data Privacy Laws."
[55] Andy Green Updated: 4/2/2021, "Complete Guide to Privacy Laws in the US | Varonis."
[56] "As Privacy Concerns Grow, States Create Bold Policies."
[57] Turner, "47 States Have Weak or Nonexistent Consumer Data Privacy Laws."
[58] Turner.

Both of the proposed COVID-era data protection bills introduced in 2020 "require express consent for processing of personal data defined as 'sensitive' by private companies," though they differ in defining sensitive data.[59] The Democratic-backed proposal, the Public Health Privacy Emergency Act introduced by Senator Mark R. Warner (D-VA), protects email address, telephone numbers and "metadata".[60] But there are other types of data that users are concerned about sharing, such as social media networks and zip codes. Furthermore, users are generally less WTS data with both private *and* public bodies — and there is no mention, interestingly, of regulating public bodies in the Republican-backed proposal, the COVID-19 Consumer Data Protection Act of 2020, introduced by Senator Roger Wicker (R-MS), despite the preferences of their Republican followers found in this study. Legislators must think carefully and *contextually* about data types, data-sharing body, and changing informational norms when defining the scope of "sensitive" data.

Furthermore, policymakers should consider how to address differences between privacy preference groups — specifically, differences between Democrats and Republicans. Should policymakers legislate privacy as defined by the interests of the majority who are WTS for the sake of the pandemic, or by the minority that is more reluctant to share personal information? Ultimately, in line with CI, which "demands 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", this is a moral rather than research-based policy question. More research on ethical implications by philosophers and legal scholars is necessary to come to a working definition of privacy in the post-COVID era.

[59] Kerry, "Game On."
[60] Kerry.

In the meanwhile, policymakers who are interested in encouraging their constituents to share health and location data for contact-tracing purposes would be well-served with more information on non-sharers' rationale behind their aversity. Republicans less trustworthy of Democratic-controlled leadership's ability to protect their privacy rights could be easily reassured by a commitment to preventing "the potential misuse of health data by government agencies with no role in public health", as proposed by the Health Emergency Privacy Act.

A few procedural issues potentially stand in the way of these proposals. Firstly, it is possible that preferences update faster than legislation that accommodates these changes can be passed. While this study did not specify the time frame over which preferences were surveyed, the time period is approximated to be about a year, assuming pre-COVID preferences were held prior to March. The writing and passage of federal legislation can easily take longer than this, meaning that by the time a bill comes to fruition, preferences might have shifted, rendering the legislation ineffectual. States might be better positioned to design and pass legislation that is responsive to users' immediate needs.

The proposed policy might also face a hefty implementation challenge. In both of the bills proposed during the pandemic, the FTC is named as the responsible party for monitoring privacy breeches by private corporations.[61] But the FTC might not have the infrastructure to police tech giants such as Facebook, which collects 500 terabytes of data daily.[62] Increased funding and support for the FTC's technological capabilities is necessary to making a comprehensive privacy bill enforceable.

[61] Kerry.
[62] Constine, "How Big Is Facebook's Data?"

Conclusion

In the aftermath of the COVID-19 pandemic, American society faces a pivotal privacy crossroads. Individuals must decide whether they are willing to sacrifice personal privacy for the sake of public good — in other words, what constitutes their "desirable balance of values".[63] This study finds that, at least currently, Americans are willing to share certain data types when doing so is in the express interest of the public good. To ensure this willingness to share is not taken advantage of by private industry, comprehensive privacy legislation must be designed and implemented immediately.

Designing legislation that adequately satisfies the diverse American populace will not be an easy task. Willingness to share varies significantly across political party identification. The naivete of early internet users has been traded, for many, with an unshakeable distrust. CI-informed policy offers one way of addressing users' evolving concerns and avoiding the "wholesale violation of privacy and government lawlessness" that as has occurred in prior public emergencies.

At stake here is the status of privacy as a potentially unalienable right — a right that "imposes obligations and restrictions" on corporations and the government in the interest of the right so be left alone and un-surveilled. In a rapidly changing digital and national context, is vital that this right be "circumscribed in a non-arbitrary manner." [64]

[63] Barber and Westin, *Effective Social Science : Eight Cases in Economics, Political Science, and Sociology*.
[64] Nissenbaum, "Privacy as Contextual Integrity."

Citations

Abaquita, Denielle, Paritosh Bahirat, Karla A. Badillo-Urquiola, and Pamela Wisniewski. "Privacy Norms within the Internet of Things Using Contextual Integrity." In *Companion of the 2020 ACM International Conference on Supporting Group Work*, 131–34. GROUP '20. New York, NY, USA: Association for Computing Machinery, 2020. https://doi.org/10.1145/3323994.3369891.

American Civil Liberties Union. "ACLU History: Wiretapping: A New Kind of 'Search and Seizure.'" Accessed January 16, 2021. https://www.aclu.org/other/aclu-history-wiretapping-new-kind-search-and-seizure.

Andy Green Updated: 4/2/2021. "Complete Guide to Privacy Laws in the US | Varonis." Inside Out Security, December 16, 2019. https://www.varonis.com/blog/us-privacy-laws/.

"As Privacy Concerns Grow, States Create Bold Policies." Accessed April 12, 2021. https://www.govtech.com/policy/As-Privacy-Concerns-Grow-States-Create-Bold-Policies.html.

Auxier, Brooke. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." *Pew Research Center*, November 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Barber, Bernard, and Alan F. Westin. *Effective Social Science : Eight Cases in Economics, Political Science, and Sociology*. Russell Sage Foundation, 1988.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20, no. 5 (November 2004): 313–24. https://doi.org/10.1080/01972240490507956.

Brough, Aaron R., and Kelly D. Martin. "Consumer Privacy During (and After) the COVID-19 Pandemic." *Journal of Public Policy & Marketing* 40, no. 1 (January 1, 2021): 108–10. https://doi.org/10.1177/0743915620929999.

Bryan, Kristin. "Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation." Consumer Privacy World, November 12, 2020. https://www.consumerprivacyworld.com/2020/11/election-2020-looking-forward-to-what-a-biden-presidency-may-mean-for-data-privacy-and-data-privacy-litigation/.

Busch, Andreas. "Internet and Privacy." In *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, edited by James D. Wright, 593–99. Oxford: Elsevier, 2015. https://doi.org/10.1016/B978-0-08-097086-8.75024-0.

Chandler, Jesse, Cheskie Rosenzweig, Aaron J. Moss, Jonathan Robinson, and Leib Litman. "Online Panels in Social Science Research: Expanding Sampling Methods beyond Mechanical Turk." *Behavior Research Methods* 51, no. 5 (October 1, 2019): 2022–38. https://doi.org/10.3758/s13428-019-01273-7.

Constine, Josh. "How Big Is Facebook's Data? 2.5 Billion Pieces Of Content And 500+ Terabytes Ingested Every Day." *TechCrunch* (blog), August 22, 2012. https://social.techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day/.

Diaz, Angel. "Coronavirus, Location Tracking, and Civil Liberties | Brennan Center for Justice," April 7, 2020. https://www.brennancenter.org/our-work/analysis-opinion/coronavirus-location-tracking-and-civil-liberties.

Fazlıoğlu, Müge. “Privacy in the Wake of Covid-19.” International Assosciation of Privacy Professionals, May 2020.

Hoyle, Roberto, Luke Stark, Qatrunnada Ismail, David Crandall, Apu Kapadia, and Denise Anthony. “Privacy Norms and Preferences for Photos Posted Online.” *ACM Transactions on Computer-Human Interaction* 27, no. 4 (August 3, 2020): 30:1-30:27. https://doi.org/10.1145/3380960.

Kerry, Cameron F. “Game on: What to Make of Senate Privacy Bills and Hearing.” *Brookings* (blog), December 3, 2019. https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

Kumaraguru, Ponnurangam, and Lorrie Faith Cranor. “Privacy Indexes: A Survey of Westin’s Studies,” n.d., 22.

Leon, Pedro Giovanni, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, and Lorrie Faith Cranor. “What Matters to Users?: Factors That Affect Users’ Willingness to Share Information with Online Advertisers.” In *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS ’13*, 1. Newcastle, United Kingdom: ACM Press, 2013. https://doi.org/10.1145/2501604.2501611.

Levay, Kevin E., Jeremy Freese, and James N. Druckman. “The Demographic and Political Composition of Mechanical Turk Samples.” *SAGE Open* 6, no. 1 (January 1, 2016): 2158244016636433. https://doi.org/10.1177/2158244016636433.

Lewis, James. “Big Company, Big Government, Big Brother? Privacy after Covid-19,” April 7, 2020. https://www.csis.org/analysis/big-company-big-government-big-brother-privacy-after-covid-19.

Lind, Dara. “Donald Trump’s Proposed ‘Muslim Registry,’ Explained.” Vox, November 16, 2016. https://www.vox.com/policy-and-politics/2016/11/16/13649764/trump-muslim-register-database.

Malheiros, Miguel. “‘Fairly Truthful’: The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure | SpringerLink.” *Trust and Trustworthy Computing*, 2013, 250–66.

Nissenbaum, Helen. “Privacy as Contextual Integrity.” *Washington Law Review* 79, no. 1 (February 2004): 119–57.

Schomakers, Eva-Maria, Chantal Lidynia, Dirk Müllmann, and Martina Ziefle. “Internet Users’ Perceptions of Information Sensitivity – Insights from Germany.” *International Journal of Information Management* 46 (June 1, 2019): 142–50. https://doi.org/10.1016/j.ijinfomgt.2018.11.018.

Simko, Lucy, Jack Lucas Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. “COVID-19 Contact Tracing and Privacy: A Longitudinal Study of Public Opinion.” *ArXiv:2012.01553 [Cs]*, December 4, 2020. http://arxiv.org/abs/2012.01553.

Stuart, Avelie, Arosha K. Bandara, and Mark Levine. “The Psychology of Privacy in the Digital Age.” *Social and Personality Psychology Compass* 13, no. 11 (2019): e12507. https://doi.org/10.1111/spc3.12507.

Tan, Joshua, and Mahmood Sharif. “Comparing Hypothetical and Realistic Privacy Valuations.” *WPES’18: Proceedings of the 2018 Workshop on Privacy in the Electronic Society*, January 2018, 168–82.

Taylor, Humphrey. “Most People Are ‘Privacy Pragmatists’ Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits,” January 1, 2003.

Tkacik, Daniel. “Overcoming the Privacy Paradox.” *CyLab: Carnegie Melon University Security Privacy Instiute*, June 28, 2019. https://www.cylab.cmu.edu/news/2019/06/28-privacy-con.html.

Turner, Gabe. “47 States Have Weak or Nonexistent Consumer Data Privacy Laws.” *Security.Org* (blog), April 14, 2020. https://www.security.org/resources/digital-privacy-legislation-by-state/.

Vestal, Christine. “Lack of Public Data Hampers COVID-19 Fight.” Pew Stateline, August 3, 2020. https://pew.org/3jYE8mV.

Vitak, Jessica, and Michael Zimmer. “More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies.” *Social Media + Society* 6, no. 3 (July 30, 2020). https://doi.org/10.1177/2056305120948250.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4, no. 5 (1890): 193–220. https://doi.org/10.2307/1321160.

Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.

White, April. “A Brief History of Surveillance in America.” Smithsonian Magazine, April 2018. https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/.

Zhang, Baobao, Sarah Kreps, Nina McMurry, and R. Miles McCain. “Americans’ Perceptions of Privacy and Surveillance in the COVID-19 Pandemic.” *PLOS ONE* 15, no. 12 (December 23, 2020): e0242652. https://doi.org/10.1371/journal.pone.0242652.

Zimmer, Michael. “Addressing Conceptual Gaps in Big Data Research Ethics: An Application of Contextual Integrity.” *Social Media + Society* 4, no. 2 (April 1, 2018): 2056305118768300. https://doi.org/10.1177/2056305118768300.

Appendix

I: Survey Form

COVID 19 and Privacy

Participation Consent Form

Description: We are researchers at the University of Chicago conducting a research study about data privacy in the COVID-19 era. The interview consists of multiple choice and short answer questions related to your data privacy practices prior to and during the COVID-19 pandemic. Researchers will analyze this data to answer research questions about data privacy and COVID-19. Participation should take about 8-10 minutes. Your participation is voluntary.

Incentives: You will be paid $1.00 for participating in this survey.

Risks and Benefits: Your participation in this study does not involve any risk to you beyond that of everyday life. Taking part in this research study may not benefit you personally.

Confidentiality: Data is recorded by Qualtrics and de-identified. It will be stored and secured on the University of Chicago's cloud service. The data will be retained after the conclusion of the research on the researchers' electronic devices for replication purposes.
• If you decide to withdraw from this study, any data already collected will be destroyed.
• No identifiable data will be collected. Identifiable data will never be shared outside the research team.
• The information collected as part of this research might be used or shared for future research studies, without further informed consent.
• M-Turk worker IDs will only be collected for the purposes of distributing compensation and will not be associated with survey responses or linked to the data set.

Disclaimer: Any work performed on M-Turk can be linked to the user's public profile page. Thus, workers may wish to restrict what information they choose to share in their public profile. Participants might wish to consult Amazon's warning to M-Turk workers here.

Contacts & Questions: If you have questions or concerns about the study, you can contact Alia Shahzad at ashahzad@uchicago.edu

If you have any questions about your rights as a participant in this research, feel you have been harmed, or wish to discuss other study-related concerns with someone who is not part of the research team, you can contact the University of Chicago Social & Behavioral Sciences

Institutional Review Board (IRB) Office by phone at (773) 702-2915, or by email at sbs-irb@uchicago.edu.

Consent: Participation is voluntary. Refusal to participate or withdrawing from the research will involve no penalty or loss of benefits to which you might otherwise be entitled. Consent is indicated by digitally clicking the "Agree" box below. By clicking "Agree" below, you confirm that you have read the above consent form, are at least 18 years old, and agree to participate in the research. Please print or save a copy of this page for your records.

○ I agree to participate in the research. (1)

○ I do NOT agree to participate in the research. If you do not consent, you will exit from the survey page. (2)

Skip To: End of Block If Consent: Participation is voluntary. Refusal to participate or withdrawing from the research will... = I do NOT agree to participate in the research. If you do not consent, you will exit from the survey page.

End of Block: Consent Form

Start of Block: Informational + Demographics

This survey aims to understand your conceptions of data privacy before and after COVID-19. Please consider the following questions carefully and answer precisely.

Do you describe yourself as a man, a woman, or in some other way?

- ○ Man (1)
- ○ Woman (2)
- ○ Nonbinary (3)
- ○ Prefer not to respond (4)

What's your age in years?

_____

Are you of Hispanic, Latino, or Spanish origin?

- ○ Yes (1)
- ○ No (2)

How do you like to describe yourself? (You may select multiple boxes).

- ☐ American Indian or Alaska Native (1)
- ☐ Asian (2)
- ☐ Black or African American (3)
- ☐ Native Hawaiian or Other Pacific Islander (4)
- ☐ White (5)
- ☐ Some other race (specify below) (6)

_____

What's your highest completed level of education?

- ○ Not a High School Graduate (1)
- ○ High School Graduate of equivalent (e.g. GED) (2)
- ○ In Process of Completing Associate's or Bachelor's Degree (3)
- ○ Associate's Degree (2-year program) (4)
- ○ Bachelor's Degree (4-year program) (5)
- ○ Graduate Degree (6)
- ○ Postgraduate Degree (7)

In which state do you currently reside?

▼ Alabama (1) ... I do not reside in the United States (53)

Are you currently working remotely?

- Yes (1)
- No (2)
- Unemployed (5)

Are you a student?

- Yes (1)
- No (3)

Display This Question:

If Are you a student? = Yes

Are you currently attending school remotely?

- Yes (1)
- No (2)

Are you a parent of an elementary, middle or high school-aged child (5 to 18 years) who is attending school remotely?

- ○ Yes (1)
- ○ No (2)

What political party do you affiliate with the most?

- ○ Democrat (1)
- ○ Republican (2)
- ○ Independent (3)
- ○ Nonaffiliated (4)
- ○ Other (specify below) (5) _____

End of Block: Informational + Demographics

Start of Block: COVID Response

Respond with your level of agreement to the following statements.

	Strongly disagree (6)	Somewhat agree (7)	Neither agree nor disagree (8)	Somewhat agree (9)	Strongly agree (10)
Social distancing is important to slowing the spread of the COVID-19 pandemic. (1)	○	○	○	○	○
Wearing masks is important to slowing the spread of the COVID-19 pandemic. (2)	○	○	○	○	○
The federal government has done an adequate job of responding to the COVID-19 pandemic. (3)	○	○	○	○	○
My home state government has done an adequate job of responding to the COVID-19 pandemic. (4)	○	○	○	○	○

End of Block: COVID Response

Start of Block: Privacy Identity

Have you used any contact-tracing applications on your laptop or smartphone?

- ○ Yes (1)
- ○ No (2)

Do you plan on downloading any contact-tracing applications on your laptop or smartphone?

- ○ Yes (1)
- ○ No (2)
- ○ I'm not sure (3)

Are you worried about data breaches or cyberattacks compromising your personal data on the internet?

- ○ Yes (1)
- ○ No (2)

Should vulnerable groups such as undocumented immigrants receive special or additional data privacy protection from employers?

- ○ Yes (1)
- ○ No (4)

Respond with your level of agreement to the following statements.

	Strongly Disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
Consumers have lost all control over how personal information is collected and used by companies. (1)	○	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way. (2)	○	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today. (3)	○	○	○	○	○

During a global pandemic, public health concerns should take precedence over individuals' privacy preferences. (4)	○	○	○	○	○

End of Block: Privacy Identity

Start of Block: Pre COVID

Read and respond to the following questions about your online behavior BEFORE the COVID-19 pandemic.

*

Before the COVID-19 pandemic, about how many hours per day did you spend on digital devices with internet connectivity (e.g. computer, phone, tablet)? Include both leisure and work activities.

_____

Before the COVID-19 pandemic, did you ever stop using any web platforms or service (e.g., internet browsers, Instagram, smartphone applications) due to privacy concerns?

- ○ Yes (1)
- ○ No (2)

Display This Question:

If Before the COVID-19 pandemic, did you ever stop using any web platforms or service (e.g., interne... = Yes

What web platform(s) and/or service(s) (e.g., internet browsers, Instagram, smartphone applications) did you stop using due to privacy concerns, and why did you choose to stop using these services?

_____

_____

_____

_____

_____

Display This Question:

If Are you a parent of an elementary, middle or high school-aged child (5 to 18 years) who is attend... = Yes

Before the COVID-19 pandemic, were you ever concerned about your child/children's online privacy?

- ○ Yes (1)
- ○ No (4)
- ○ I'm not sure (5)

Read the following statements and respond with your level of comfort BEFORE the COVID-19 pandemic.

1) Before COVID-19, I would be willing to share ____ with a government entity (e.g. Department of Health and Human Services).

	Strongly Disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
My name (1)	○	○	○	○	○
My zipcode (4)	○	○	○	○	○
My home address (5)	○	○	○	○	○
My smartphone location data (6)	○	○	○	○	○
My health information (7)	○	○	○	○	○
My political preferences (8)	○	○	○	○	○
My social media network (e.g. list of Facebook friends or Instagram followers) (9)	○	○	○	○	○

Before COVID-19, I would be willing to share ____ with a private company providing me with services (e.g. Uber, Google, smartphone applications).

	Strongly disagree (5)	Somewhat disagree (6)	Neither agree nor disagree (7)	Somewhat agree (8)	Strongly agree (9)
My name (x1)	○	○	○	○	○
My zipcode (x4)	○	○	○	○	○
My home address (x5)	○	○	○	○	○
My smartphone location data (x6)	○	○	○	○	○
My health information (x7)	○	○	○	○	○
My political preferences (x8)	○	○	○	○	○
My social media network (e.g. list of Facebook friends or Instagram followers) (x9)	○	○	○	○	○

Before COVID-19, I would be comfortable taking work, school, or organizational video conferencing calls (e.g. Zoom, Skype) using _____ as a visible backdrop during my call.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Somewhat agree (5)
My bedroom (1)	○	○	○	○	○
My living room (2)	○	○	○	○	○
My bathroom (3)	○	○	○	○	○
My backyard (4)	○	○	○	○	○

End of Block: Pre COVID

Start of Block: During COVID

Read and respond to the following questions about your online behavior DURING the COVID-19 pandemic.

*

During the COVID-19 pandemic, how many hours a day do you spend on digital devices with internet connectivity (e.g. computer, phone, tablet)? Include both leisure and work activities.

_____

During the COVID-19 pandemic, have you started any new activities online, such as attending remote concerts, playing games, family video calls, etc.?

- Yes (1)
- No (2)

Display This Question:

If Are you currently working remotely? = Yes

During the COVID-19 pandemic, do you work more hours per day than before the pandemic?

- Yes (1)
- No (2)
- I don't know (3)

Display This Question:

If Are you a parent of an elementary, middle or high school-aged child (5 to 18 years) who is attend... = Yes

During the COVID-19 pandemic, have you become more concerned about your child/children's online privacy than prior to the pandemic?

- Yes (1)
- No (2)
- I'm not sure (4)

Display This Question:

If Are you currently working remotely? = Yes

During the COVID-19 pandemic, has your employer used any digital monitoring tools to supervise your remote work day?

- ○ Yes (1)
- ○ No (2)
- ○ I don't know (3)

During the COVID-19 pandemic, have you stopped using any web platforms or service (e.g., internet browsers, Instagram, smartphone app) due to privacy concerns?

- ○ Yes (1)
- ○ No (2)

During the COVID-19 pandemic, have you become more comfortable taking video calls in "private spaces" (e.g. bedrooms)?

- ○ Yes (1)
- ○ No (2)

Display This Question:

If During the COVID-19 pandemic, have you stopped using any web platforms or service (e.g., internet... = Yes

Or During the COVID-19 pandemic, have you become more comfortable taking video calls in "private spa... = Yes

What has prompted you to change your privacy preferences and/or privacy behavior during the COVID-19 pandemic?

_____

_____

_____

_____

_____

Read the following statements and respond with your level of comfort DURING the COVID-19 pandemic.

Carry Forward All Choices - Displayed & Hidden from "1) Before COVID-19, I would be willing to share ____ with a government entity (e.g. Department of Health and Human Services)."

During the COVID-19 pandemic, I am willing to share ____ with a government entity (e.g. Department of Health and Human Services).

	Strongly Disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
My name (x1)	○	○	○	○	○
My zipcode (x4)	○	○	○	○	○
My home address (x5)	○	○	○	○	○
My smartphone location data (x6)	○	○	○	○	○
My health information (x7)	○	○	○	○	○
My political preferences (x8)	○	○	○	○	○
My social media network (e.g. list of Facebook friends or Instagram followers) (x9)	○	○	○	○	○

Carry Forward Selected Choices from "During the COVID-19 pandemic, I am willing to share ____ with a government entity (e.g. Department of Health and Human Services)."

During the COVID-19 pandemic, I am willing to share ____ with a private company providing me with services (e.g. Uber, Google, smartphone applications).

	Strongly Disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
My name (xx1)	○	○	○	○	○
My zipcode (xx4)	○	○	○	○	○
My home address (xx5)	○	○	○	○	○
My smartphone location data (xx6)	○	○	○	○	○
My health information (xx7)	○	○	○	○	○
My political preferences (xx8)	○	○	○	○	○
My social media network (e.g. list of Facebook friends or Instagram followers) (xx9)	○	○	○	○	○

Carry Forward All Choices - Displayed & Hidden from "Before COVID-19, I would be comfortable taking work, school, or organizational video conferencing calls (e.g. Zoom, Skype) using _____ as a visible backdrop during my call."

During COVID-19, I am comfortable taking work, school, or organizational video conferencing calls (e.g. Zoom, Skype) using _____ as a visible backdrop during my call.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly Agree (5)
My bedroom (x1)	○	○	○	○	○
My living room (x2)	○	○	○	○	○
My bathroom (x3)	○	○	○	○	○
My backyard (x4)	○	○	○	○	○

During the COVID-19 pandemic, I am comfortable with ____ being made publicly available (e.g., on my home county's online COVID dashboard) if I test positive for COVID-19.

	Strongly disagree (1)	Somewhat disagree (2)	Neither agree nor disagree (3)	Somewhat agree (4)	Strongly agree (5)
My name (1)	○	○	○	○	○
My zipcode (4)	○	○	○	○	○
My home address (5)	○	○	○	○	○
My employer (6)	○	○	○	○	○
My location since probable infection (e.g. grocery store, gym) (7)	○	○	○	○	○

Any final comments on your willingness to share personal data during the COVID-19 pandemic?

_____

_____

_____

_____

_____

End of Block: During COVID

Start of Block: Survey Code

Here is your survey code: ${e://Field/Random%20ID}

Copy this value to paste into MTurk.

When you have copied this ID, please click the next button to submit your survey.

End of Block: Survey Code

II: Selected Qualitative Responses

What has prompted you to change your privacy preferences and/or privacy behavior?

WTS Category	**Respondent's Privacy Identity**	**Quote**
Less WTS	Fundamentalist	Spending more time online will give people more of a chance to get my information so I am very concerned about giving too much away
Less WTS	Pragmatist	My privacy behavior changed during the COVID-19 pandemic because I spend more time working from home and more time video chatting at home. This makes me more self-conscious of sharing my surroundings to others
Less WTS	Pragmatist	the constant data breaches, attacks, and weaknesses in IT infrastructure. Any policy put in place to protect my privacy can be ignored at will by those in power
More WTS	Fundamentalist	I'm trying to aid agencies gathering more data to the best of my ability in order to aid COVID-19 cases."
More WTS	Pragmatist	To help the government learn more about my health status.
More WTS	Unconcerned	People's health and wellbeing is of higher importance than privacy.
More WTS	Pragmatist	Times are different, and I need to adjust to what's needed today."
Unchanged WTS	Unconcerned	My preferences have not changed. Security risks are not dependent upon world events, rather, they are dependent upon the method or vehicle in which information is shard and how vulnerable it is
Unchanged WTS	Pragmatist	I'm just a regular dude. No one cares what I'm doing. My privacy isn't a concern."
Unchanged WTS	Fundamentalist	I don't think my privacy preferences and/or privacy behavior has changed all that much. I figure if someone wants my information bad enough, they'll find a way to steal it.