Pre-Analysis Plan
The Politics of Personal Data Privacy: Experimental Evidence *

Lizhi Liu †  Stephen Weymouth‡

November 1, 2019

Work in Progress. Please do not circulate.

Abstract

Our study examines the micro-foundations of digital governance. This pre-analysis plan details informational survey experiments to identify the determinants of individuals’ attitudes about data privacy and its regulation. We estimate the elasticity of support for national privacy regulation in the United States to new information about businesses’ uses of personal data; data breaches; and business initiatives to safeguard customers’ data beyond what is required by law (“private regulation”). We further examine the extent to which an individual’s market ideology influences the estimated elasticities.

---

*We acknowledge seed funding from the Massive Data Institute at the McCourt School of Public Policy at Georgetown University. We are also grateful for a technology research grant from the McDonough School of Business at Georgetown.

†Georgetown University; lizhi.liu@georgetown.edu

‡Georgetown University; stephen.weymouth@georgetown.edu
1 Introduction

Data privacy constitutes one of the foremost policy issues of our time, especially with the rise of the digital economy and big data analytics. Recent events demonstrate that privacy breaches can have far-reaching political consequences. For example, the illicit harvesting of Facebook data by Cambridge Analytica likely influenced voting in 2016 U.S. presidential election as well as the Brexit referendum. Public concerns about personal data have lead to new regulatory restrictions on data collection such as the European Union’s General Data Protection Regulation (GDPR).

Our goal in this project is to measure individual attitudes about: 1) private firms’ data collection practices, and 2) government regulation to restrict firms’ data collection practices. The particular realm of privacy preferences we study here is sometimes called informational privacy, which is “concerned with controlling whether and how personal data can be gathered, stored, processed, and disseminated” (Kokolakis, 2017, p.2). We seek to understand the elasticity of support for information privacy with respect to new information about firms’ data collection activities.

In this pre-analysis plan, we propose survey experiments to examine the following aspects about individuals’ privacy preferences. First, we assess whether information about businesses’ usage of individual data increases individuals’ concerns about data privacy. Second, we measure how information about businesses’ data practices affects individuals’ support for privacy regulation. We focus on legal data collection practices as well as illegal data breaches. Third, we examine whether information about firms’ self-regulatory initiatives to safeguard customers’ data dampen individuals’ support for government privacy regulation. Throughout, we assess how individual characteristics, including market ideology, explain views about personal data privacy regulation in the context of new information.

Public opinion surveys suggest public concern about data privacy as the commercial uses of personal data expand, and public knowledge of data harvesting increases. Pew found
that 91% of Americans “agree” or “strongly agree” that people have lost control over the collection and use of personal information.\(^1\) Some 80% of social media users are concerned about businesses accessing their data from social media;\(^2\) just 9% believe they have a lot of control over information collected about them.\(^3\) The extent to which increased awareness about firms’ data collection contributes to these concerns, and to support for data privacy regulation, is not well understood.

Indeed, despite evidence of rising privacy concerns and their looming influence over business and public policy (Acquisti, Taylor, and Wagman, 2016), little is known about the role information may play in shifting individuals’ data privacy concerns, and individuals’ preferences for privacy regulation. Economists and business scholars have studied the economic value of data privacy: What incentives drive consumers’ willingness to share data? How much monetary value do individuals place on their private data? (See, e.g., Athey, Catalini, and Tucker (2017) and Acquisti, Brandimarte, and Loewenstein (2015).) The pioneering privacy research in political science (Newman, 2008; Farrell and Newman, 2019) provides rich detail on alternative privacy regulatory approaches, but largely ignores individual privacy attitudes. As such, the existing scholarship may be ill-suited to explain the dramatic increase in the number of countries passing privacy regulations in the recent years (Ferracane, Lee-Makiyama, and Van Der Marel, 2018).

We aim to fill a gap in the literature by studying the micro-foundations of privacy regulations: individuals’ privacy preferences. Without understanding mass attitudes toward data privacy, it is difficult to explain why some jurisdictions have adopted strict data privacy regulations. (See Figure 1 for a map of privacy laws across U.S. states.) For instance, the California state legislature passed in 2019 a stringent data privacy law, modeled after the EU’s GDPR. The California Consumer Privacy Act (CCPA) allows residents to ask retailers for any personal data collected on them. Consumers can also require businesses to delete

\(^1\)https://tinyurl.com/y3ydvef4
\(^2\)Ibid.
\(^3\)https://tinyurl.com/y44cdlzd
their personal data, and to let them opt out of having their data sold. The CCPA was passed in response to a threatened ballot initiative to restrict data collection, which quickly gained political momentum after a public relations campaign designed to inform voters about businesses’ data collection practices. Our study will help explain whether new information about companies’ data harvesting shifts public opinion on data privacy regulation such as CCPA.\footnote{Other laws restrict governments’ data collection and surveillance operations. For instance, the city of San Francisco passed a comprehensive ban on city agencies’ use of facial surveillance, and set further restrictions on other personal surveillance technologies such as camera-enabled drones and license plate readers. Dozens of other US cities are considering similar laws. Our focus in this project is on data collection by private firms rather than governments.}
2 Theoretical Framework and Hypotheses

Our point of departure in the study of personal data politics is to uncover individuals’ preferences over data privacy and its regulation. In particular, we examine through surveys and experiments how information about businesses’ collection and uses of individual data influences individuals’ support for government regulation of those business activities (“data privacy regulation”). The reason for examining preferences is that policy outcomes depend in part on the policies favored by the mass public. We need to understand mass public preferences in order to explain how and why data privacy regulation may evolve.

Our study is motivated in part by a well-known “privacy paradox,” which connotes the discrepancy between individuals’ stated concerns about personal data privacy and their actual behavior (Barnes, 2006; Norberg, Horne, and Horne, 2007). Individuals tend to report concerns about the sharing and collection of their data, yet they continue to use products and applications that collect and share their personal data, especially over the internet. One possible explanation for the paradox is that people are simply unaware of the extent to which companies collect their personal data. Providing individuals with information about data collection may therefore affect individuals’ privacy attitudes; information may also affect their preferences for government regulation of data collection and usage. For this reason, we propose informational experiments.

While the politics of data privacy have received little attention in the literature, our work contributes to a central set of questions long studied in political science. These questions involve the formation of individual preferences over policy: Why do people support certain policies? What causes peoples’ preferences over policies to change? Under what conditions does new information change individuals’ preferences? (For excellent reviews of the preference formation literature, see Druckman and Lupia (2000) and Druckman and Lupia (2016).) We strive to answer these questions as they relate to the formation of preferences over privacy regulation.
2.1 The Role of Information in Preference Formation

We focus on the role of new information in shaping public preferences over data privacy regulation. Policy-specific information shapes individual attitudes (Gilens, 2001; Kendall, Nannicini, and Trebbi, 2015), and prior research demonstrates that individuals’ preferences respond to information provided by politicians (Carmines and Kuklinski, 1990) and the media (Iyengar, 1987), among other sources. Information may strongly affect preference formation when it clarifies the economic consequences of policy for individual respondents (Bearce and Tuxhorn, 2017; Rho and Tomz, 2017), or the consequences of policy on the broader population (Lü, Scheve, and Slaughter, 2012).

We expect that individual preferences for privacy regulation may vary depending on individuals’ understanding of firms’ data harvesting as well as current and proposed regulatory arrangements. A recent Pew survey indicates poor digital knowledge, including knowledge about digital privacy, among American respondents.\(^5\) Ignorance of policy-specific information may lead individuals to hold views that are different from those they hold once information is provided (Gilens, 2001). Individuals’ preferences may change when they are provided information about businesses collection and monetization of private data. Preferences may also respond to information about the data and privacy safeguards that new data regulation might provide.

In the realm of data privacy, individuals’ preferences for regulation may also depend on negative external events, such as data breaches resulting in the loss or misuse of personal data. Political and economic shocks, or abrupt changes in circumstances, have been shown to shift public preferences over policies. Prior work demonstrates that information about changing economic conditions, natural disasters, and shocks to personal security can alter policy preferences (Druckman and Lupia, 2016). Individuals exposed to new information

about data breaches may experience heightened concerns about privacy and be more likely to support stricter data privacy regulation.

2.2 Businesses’ Self-Regulation Initiatives

We recognize that businesses often act strategically to shape the information environment in their favor. In some cases, companies seek to inform the public of their efforts to address public concerns over their business activities. Sometimes businesses voluntarily restrict their activities beyond the requirements of the law, a practice known as “private regulation” (Potoski and Prakash, 2005; Vogel, 2008, 2010; Baron et al., 2014; Werner, 2012). In some cases, private regulation may assuage public concerns and thus weaken public demands for more extensive government regulation (Malhotra, Monin, and Tomz, 2019).

In response to public concerns over data privacy, some businesses have announced private regulatory practices to protect individual customer data – practices that extend beyond what is required by law. For instance, Apple has embedded a commitment to privacy into their marketing initiatives, stating on their website “we believe privacy is a fundamental human right,” while also promising that “Apple doesn’t gather your personal information to sell to advertisers or other organizations.”6 No existing U.S. statutes require Apple to make such a commitment. Apple’s approach may reflect idiosyncratic values; it may also be designed to assuage public concerns over data privacy.

The effect of these private regulatory efforts on individuals’ views of government privacy regulation, however, is unclear. As the SugarCRM CEO Larry Augustin claimed, “When you have the CEO of Facebook testifying on these issues in Congress, which makes all of the television and news, I’m not sure that self-regulation is going to be something that Congress will accept...Companies will certainly go down the self-regulation path, but I don’t think there’s a lot of trust for that right now.”7 Thus, an important empirical question

---

6https://www.apple.com/privacy/
is whether private regulation dampens public demand for stricter government data privacy regulation.

\section*{2.3 Hypotheses}

To assess how information affects individual data privacy preferences, we will conduct survey experiments on a nationally representative sample in the US. Our survey experiments seek to test three sets of hypotheses.

First, we assess whether information about businesses’ usage of individual data increases individuals’ concerns about data privacy and support for national privacy regulation.

\textbf{Hypothesis 1A} Information about firms’ harvesting (i.e., collection, storage, and sale) of private data will increase concerns about individual data privacy.

\textbf{Hypothesis 1B} Information about firms’ harvesting (i.e., collection, storage, and sale) of private data will increase support for privacy regulation.

\textbf{Hypothesis 1C} Information about firms’ harvesting (i.e., collection, storage, and sale) of private data will increase the likelihood that an individual engages in political action in support of privacy regulation.

Second, we measure how information about illegal data breaches affect individuals’ concerns about data privacy and support for national privacy regulation.

\textbf{Hypothesis 2A} Information about data breaches will increase concerns about data privacy.

\textbf{Hypothesis 2B} Information about data breaches will increase support for data privacy regulation.

\textbf{Hypothesis 2C} Information about data breaches will increase the likelihood that an individual engages in political action in support of privacy regulation.
Third, we examine whether information about firms’ self-regulatory initiatives to safeguard customers’ data dampen individuals’ concerns about data privacy and support for national privacy regulation.

**Hypothesis 3A** Information about business private regulation of customer data will reduce concerns about data privacy.

**Hypothesis 3B** Information about business private regulation of customer data will reduce support for data privacy regulation.

**Hypothesis 3C** Information about business private regulation of customer data will lower the likelihood that an individual engages in political action in support of privacy regulation.

### 2.4 Heterogeneous Treatment Effects

We will examine whether the treatment effects vary by political ideology. Prior experimental and survey research finds that economic ideology helps explain individual preferences over economic and regulatory policies (Malhotra and Margalit, 2010; Margalit, 2013; Alesina, Stantcheva, and Teso, 2018; Ahlquist, Clayton, and Levi, 2014; Bechtel, Hainmueller, and Margalit, 2014). Individual ideology – a constellation of values and beliefs that organize and inform individual positions on a variety of issues – may explain variation in regulatory and other policy preferences.

For our purposes, a relevant ideological dimension concerns individuals’ views of the role of the state in the economy, which we refer to here as “market ideology.” Individuals on the right of the market ideology spectrum tend to believe that market competition can discipline business in ways that benefits consumers. Those on the left contend that government regulatory intervention is required to protect consumers.

We will examine whether the treatment effects vary along this spectrum of market ideology. Individuals with different market ideologies might respond differently to the treatment conditions. Individuals that favor more government involvement may be more inclined
to favor stricter privacy laws after receiving new information about data harvesting and data breaches. In contrast, new information about firms' private regulation efforts may weaken support for stricter privacy laws among individuals with right-leaning market ideology.

Ideology relates closely to individuals’ partisan orientation – their support for specific political parties. Partisanship is a central divide in American politics, and on economic and regulatory issues Republicans tend to favor a more limited role of government (Goren, 2005). Partisanship can explain individuals’ policy preferences, particularly after partisan leaders of different parties take definitive and differing stances on particular policy issues (Zaller et al., 1992; Berinsky, 2009; Guisinger and Saunders, 2017; Nelson and Steinberg, 2018).

While left-right market ideology may help explain preferences over privacy regulation, we believe it is unlikely that partisanship separately divides the mass public with respect to data privacy regulation. One reason is that partisan elites such as the president and other party leaders have yet to take sustained, public positions on privacy regulation. This lack of position-taking is relevant. Individuals’ use information from party leaders, sometimes called cues, as information shortcuts. Public statements about privacy regulation by party leaders may serve as cues that facilitate individuals’ own preference formation. To the extent that privacy has entered public debate of political elites, members of both parties appear amenable to some form of national privacy legislation, though little legislative progress has been made, and few debates have publicly been aired. Thus, at this point, we believe an individual’s political party affiliation is unlikely to explain her concerns about data privacy or support for privacy regulation.

Another large body of research finds that the personal economic impact of a particular policy explains individuals’ preferences over that policy. We think that individual economic interests are unlikely to explain preferences over data privacy regulation. Importantly, the economic implications of data privacy regulation are not well understood by either
economists or the mass public. Unlike taxes or trade policy where the winners and losers are more clearly delineated and policy preferences sometimes reflect those divisions (Mayda and Rodrik, 2005; Bartels, 2005), the distributional effects of enhanced consumer privacy protections are not clear.

3 Survey and Experimental Design

In this section, we specify how we construct and randomize the treatments, how we operationalize the outcome and control variables, and how we plan to implement the survey experiments.

3.1 Survey Data Collection

We plan to collect three waves of survey data. The first wave is a small pilot survey on approximately 500 respondents on Amazon’s Mechanical Turk (mTurk). The main purpose of the pilot survey is to test whether the questions are realistic and appropriate. As a low-cost method to recruit respondents, mTurk has a few limitations. First, it leads to a non-probability sample. To better interpret the results, we will compare the demographic characteristics of our sample with those of reliable nationally representative samples of US adults, especially those that are conducted around the time of our survey. We will also use a generic survey title to recruit respondents. This prevents our sample from biasing towards those who are particularly interested and knowledgeable about privacy issues. Second, a large number of mTurk participants are

---

8It is possible that a permissive regulatory environment enables firms to offer cheaper products and services in exchange for private data. Data privacy regulation could increase costs to firms and reduce the incentives to offer free services. In this way, consumers may benefit from less data regulation. Further, individuals employed by businesses whose bottom lines are negatively impacted by privacy regulations may be harmed by new regulations. While suggestive of possible economic distributional motivations for privacy preferences, these mechanisms remain highly speculative.
non-US residents. To ensure that we only sample US adults, we follow Kuziemko et al. (2015) by restricting survey invitations to those who have US addresses, and by fielding the survey during daytime hours in the US. Further, we ask the respondents to confirm their US residency in the consent form. These measures help reduce the likelihood of non-US residents from faking into the respondent group.

After the pilot survey, we will administer the main survey on a nationally representative sample of approximately 2,000 US adults on YouGov.² YouGov is a premier online panel commonly used in public polling and political science research. One advantage of YouGov is that the survey data will be statistically weighted not only by the respondents’ demographic characteristics (e.g., age, gender, education, region, social class), but also by their level of political interest and voting records at the previous election. Since our study focuses on individuals’ policy preferences, ensuring sample representativeness in baseline political ideology will increase the external validity of the findings.

We will also field a short follow-up survey one month after the main survey to test whether the treatment effects persist.

The subsequent sections only describe the survey design of the main survey.

### 3.2 Treatment Construction and Randomization Protocol

To test our hypotheses, we construct three treatments: “personal data”, “breach”, and “self-regulation”. The first treatment (“personal data”) primes the respondents with a brief article about how companies collect, use and sell a variety of personal data, often without the consumers’ knowledge. The second treatment (“breach”) presents the information about the frequency of data breaches, and the fact that even the most prominent firms are very opaque about how they handle data breaches. It is important to distinguish these two treatments. While some individuals care about companies’ collection of personal data, others may not be

²As we have six different treatment groups, we need a relatively large sample size to ensure statistical power.
concerned absent infringements to the security of personal data. The third treatment ("self-regulation") provides information about voluntary self-regulation efforts by companies. This treatment allows us to examine whether private regulations preempt public regulations by popular support for a national-level privacy law. The three treatments are described in detail below.

We randomly assign respondents into one of seven groups:

- The Control Group (CG) will not receive any treatment.
- Three Treatment Groups (TG) receive one of the three treatments (TG1: personal data; TG2: breach; TG3: self-regulation).
- Three TGs receive two of the three treatments (TG4: personal data + breach; TG5: personal data + self-regulation; TG6: breach + self-regulation).

Notes: “Data” means that the treatment group has received the personal data treatment; “Bre” indicates the breach treatment received; “Reg” is short for the self-regulation treatment.
For a visual representation of the randomization protocol, see Figure 2.

3.2.1 Personal Data Treatment

The following paragraphs are adapted from articles appearing in a prominent newspaper. Please read them carefully.

Are you ready? Here is all the data digital companies may have on you

The harvesting of our personal details goes far beyond what many of us could imagine. Want to freak yourself out? I’m going to show just how much of your information businesses may store about you without you even realising it.

The data that companies collect on you includes:

• tracking where you are, which events you attended, and when
• the photos you’ve taken on your phone
• every email you’ve sent
• the businesses you’ve bought from and the products you’ve bought
• what applications you have installed, when you use them, what you use them for
• your contacts, your emails, your calendar, your call history, the messages you send and receive, the files you download, the games you play, your music, your search history, your browsing history...

The data are used by companies to create an advertisement profile of you. The data are often sold to other companies so that they can offer products targeted to you.

Companies can access also access your webcam and microphone. When a user grants an app access to their camera and microphone, the app could do the following:

• Take pictures and videos without telling you
• Upload the pictures and videos without telling you
• Run real-time face recognition to detect facial features or expressions.
• Livestream the camera on to the internet

This is one of the craziest things about the modern age. We would never let the government or a corporation put cameras/microphones in our homes or location trackers on us. But we just went ahead and did it ourselves because – to hell with it! – I want to watch cute dog videos.

3.2.2 Breach Treatment

A data breach is when personal data records collected by companies are lost or stolen. As indicated in the figure, data breaches are very common.

10The sources are https://tinyurl.com/y6cq82y2 and https://tinyurl.com/y2abg3rg
Now please view the table displaying companies’ commitments to disclosure in the event of a data breach resulting in the loss of private data that the company collects. “No Commitment” means that the company has no formal policy to notify consumers who might be affected by a data breach. “Partial” means there is a policy, but the commitment to notifying consumers is vague.11

<table>
<thead>
<tr>
<th>Company</th>
<th>Disclosure Commitment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>Partial</td>
</tr>
<tr>
<td>Facebook</td>
<td>No Commitment</td>
</tr>
<tr>
<td>Google</td>
<td>No Commitment</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Partial</td>
</tr>
<tr>
<td>Twitter</td>
<td>No Commitment</td>
</tr>
</tbody>
</table>

3.2.3 Self-Regulation Treatment

Some people think the U.S. government should pass a comprehensive federal privacy protection law to regulate companies’ collection, use and dissemination of consumers’ personal data.

11For detailed descriptions of the index, please go to this link rankingdigitalrights.org/index2019/indicators/p15/
Other people think that such a law will be overly prescriptive and burdensome, restricting companies’ capacity to meet consumer needs.

Companies sometimes take voluntary steps to protect the privacy of personal data – they do more than what the U.S. government legally requires. Many companies allow users to view and delete the data collected on them, and to opt out of having their data collected in the future. For example, Google recently launched an option called “My Activity” that allows you to see all of the information Google has collected and stored about you, at any given point in time. You can delete these data and turn off specific tracking so that some specific data will not be collected in the future. You can delete your user history and pause tracking in Google searches, Google Maps, Youtube, and various other apps and services provided by Google. As another example, Apple’s privacy commitment is included in the figure.

3.3 Outcome Variables

We study four set of outcome variables: privacy concerns, privacy settings, privacy policy preferences, and political actions. Each set of questions is detailed below. Since the order
in which answer options are presented has been shown to affect survey response, we will randomize response items when appropriate.\(^{12}\)

**Privacy Concerns.** These questions ask to what extent respondents regard privacy as a serious issue, and whether they are concerned about companies’ collection and usage of their personal data, or about data breaches.

- Do you think personal data privacy is a serious problem in America? [Not a problem at all; A small problem; A problem; A serious problem; A very serious problem]
- How concerned are you about the collection and sale of your personal data by companies? Where would you rate yourself on a scale of 1 to 5, where 1 means not concerned at all, and 5 means that you are very concerned? [1; 2; 3; 4; 5]
- How concerned are you about the breach of your personal data? Where would you rate yourself on a scale of 1 to 5, where 1 means not concerned at all, and 5 means that you are very concerned? [1; 2; 3; 4; 5]
- In general, thinking about the companies and organizations that you interact with, how confident are you that they will keep your personal records safe from hackers or unauthorized users? [Very confident; Somewhat confident; Not too confident; Not at all]

**Privacy Settings.** As suggested by the literature on “privacy paradox” (Barnes, 2006; Norberg, Horne, and Horne, 2007), it is entirely possible that concerns do not translate into actions of privacy protection. We therefore ask whether the respondents will take actions to adjust their privacy settings in the next month. In the follow-up survey conducted one month after the main survey, we will survey the same respondent and ask if she has indeed adjusted the privacy settings. In this way, we can test for the persistence of treatment effects.

- Over the next month, will you create an account with an online service when you feel worried about how your personal information would be handled? [Yes; No]
- Over the next month, if an app on your smartphone or tablet seeks your permission to use your location, how often will you allow it to use your location? [Frequently; Sometimes; Hardly; Never; I don’t have a smartphone].
- Over the next month, will you conduct the following activities? Choose all that apply. [Use a search engine that doesn’t keep track of your search history; Adopt email encryption, such as PGP; Adopt mobile encryption for calls or text messages; Use more complex passwords; Proxy servers; Add a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger; Change your privacy settings on social media such as Facebook or Twitter; Use locally-networked communications such as FireChat; Use anonymity software such as Tor; Use another software or network tool to make your activities more private; Other, please specify; Will not do any of the above]

**Privacy Policy Preferences.** This group of questions concern whether the respondents support legislative efforts to establish a comprehensive federal privacy law.

\(^{12}\)Order bias has two major forms: primacy bias (the tendency to pick the first option) and recency bias (the tendency to pick the last option in a list).
• Overall, do you approve or disapprove of companies’ collection of personal data to improve their services? [Approval; Disapprove]
• Do you support government restrictions on personal data collection by companies? [Yes; No]
• One U.S. state has implemented a consumer data protection law. The new law provides the residents “an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a ‘readily usable format’ that enables its transfer to third parties without hindrance.” (source: HBR article) Do you support such a law being passed nationally? [Yes; No]

Political Actions. Respondents may go one step further and petition for privacy protection through contacting their senator(s). Following Kuziemko et al. (2015), we provide the respondents with the contact list of Senators and a sample letter (see appendix). We ask whether they will contact their senators, and if so, whether they will petition for increasing or decreasing privacy protection. In the follow-up survey conducted one month after the main survey, we survey the same respondent if she has indeed contacted her senator(s).

• We would like to know whether you will take one of the following actions: [I sent or will send an email to my Senator asking for increased data privacy regulation; I sent or will send an email to my Senator asking to not increase data privacy regulation; I do not want to email my Senator]

3.4 Other Variables

To control for potential confounders that affect both treatment and outcome variables, and to explore heterogeneous treatment effects, we construct additional variables, described here. As before, we randomize response items when appropriate to minimize order bias.

Privacy Baseline. Prior knowledge and perceptions about privacy issues, as well as exposure to data breaches, may also determine outcome variables.

• Have you ever chosen to NOT use or NOT create an account with an online service because you were worried about how your personal information would be handled? [Yes, have done this/No, have not done this]
• When an app on your smartphone or tablet seeks your permission to use your location, how often you allow it to use your location? [Frequently; Sometimes; Hardly ever; Never; I don’t have a smartphone].
• Have you ever conducted the following activities? Choose all that apply. [Used a search engine that doesn’t keep track of your search history; Adopted email encryption, such as
PGP; Adopted mobile encryption for calls or text messages; Used more complex passwords; Proxy servers; Added a privacy-enhancing browser plugin like DoNotTrackMe or Privacy Badger; Changed your privacy settings on social media such as Facebook or Twitter; Used locally-networked communications such as FireChat; Used anonymity software such as Tor; Used another software or network tool to make your activities more private; Other, please specify; Haven’t done any of above

- How much, if anything, have you heard about companies collecting information through the services that they provide to customers? Have you heard... [A lot; A little; Nothing at all]
- Have you ever experienced a personal data breach? [Yes; No]

**Political Ideology.** Market ideology may affect people’s perceptions about privacy and whether the privacy issue should be left to the government or to the business to address.

- Think more broadly about the purpose of government. Where would you rate yourself on a scale of 1 to 5, where 1 means you think the government should do only those things necessary to provide the most basic government functions, and 5 means you think the government should take active steps in every area it can to try and improve the lives of its citizens? [1; 2; 3; 4; 5]
- Do you agree with the following statement? Government regulation of business usually does more harm than good. [Strongly agree; Agree; Neither agree nor disagree; Disagree; Strongly disagree]
- Do you agree with the following statement? Business corporations make too much profit. [Strongly agree; Agree; Neither agree nor disagree; Disagree; Strongly disagree]
- If you had to choose, would you rather have a smaller government providing fewer services, or a bigger government providing more services? [Smaller government, fewer services; Bigger government, more services; Depends; Don’t know]
- On economic policy matters, where do you see yourself on the liberal/conservative spectrum? [Very liberal; Liberal; Moderate; Conservative; Very conservative]
- In politics today, do you consider yourself a ...? [Republican; Democrat; Other]
  - (IF DEM) Do you consider yourself a strong or moderate Democrat? [Strong Democrat; Moderate Democrat]
  - (IF REP) Do you consider yourself a strong or moderate Republican? [Strong Republican; Moderate Republican]
  - (IF NEITHER REP NOR DEM) As of today, do you lean more to [The Republican Party; The Democratic Party]
- Who did you support in the presidential election in 2016? If you were not able to vote, just choose the person you wanted to win the election at that time. [Hillary Clinton; Donald Trump; Other]
- Which candidate do you plan to vote for in the 2020 presidential election? [Republican; Democrat; Other; Will not vote]

**Trust in Government/Business.** For respondents who have low trust in government, even if they have substantial concerns over privacy, they may not believe the government
can regulate data security. In contrast, low trust with business may lead to more support for government regulations on privacy issues.

- How much of the time do you think you can trust government in Washington to do what is right? [Just about always; Most of the time; Only some of the time; Never]
- How much of the time do you think you can trust companies/businesses to do what is right? [Just about always; Most of the time; Only some of the time; Never]
- In general, do you place more trust in markets or in governments to deliver economic prosperity? [Markets; Governments]

**Political Interest.** Level of political interest may influence whether the respondents will take political actions to push for privacy protection regulation (e.g., emailing the Senator).

- How interested are you in politics? Where would you rate yourself on a scale of 1 to 5, where 1 means not interested at all, and 5 means that you are very interested? [1; 2; 3; 4; 5]

**Demographic Variables.** The age, income, education, internet usage, and employment status of the response may influence outcome variables.

- See Appendix.

### 3.5 Addressing Methodological Issues

The goal of the experimental analysis is to measure the causal effects of our treatments on individuals’ data privacy attitudes and their preferences for data privacy regulation. In this section, we discuss our plans to address threats to internal validity and other methodological concerns.

We recognize that sample representativeness should not be taken for granted. We will assess the representativeness of our sample by comparing the demographics statistics of our sample with those of established nationally representative polling outfits. If we use mTurk, we will limit the possible participants to US respondents.

We will address common concerns relating to incomplete surveys (“attrition”). One concern is differential attrition between the treatment and the control groups. Differential attribution can be problematic to the extent that attrition relates to the treatment itself. As an example, it would be a problem for our randomization protocol if information about data
privacy led respondents most concerned about data privacy to exit the survey. They might be concerned about the personal nature of the data collected by our survey, or perhaps the information we provide leads some respondents in the treatment group to leave the survey to immediately change their data privacy settings. To test for differential attrition, we will check the randomness of the treatment assignment by assessing whether the treatment induces certain groups to quit the survey with higher frequency than other groups. That is, we will used regressions to ensure that attrition is not correlated with specific respondent characteristics.

One critique of survey experiments is that the treatment effects identified within the survey do not necessarily coincide with changes in actual behavior. In other words, surveys measure stated preferences, which are not the same revealed preferences, and so it’s not obvious that the effects measured in survey experiments actually “matter” politically.\textsuperscript{13} Scholars have begun to address this critique by embedding questions about actual behavior in their surveys.

We will follow this approach by including a behavioral question in our survey and by conducting a follow-up survey one month after the completion of our primary survey. In terms of behavior, we will ask respondents to send an email to their senators stating their support for a national privacy bill. Moreover, we will test the persistence of any of estimated effects. Our follow-up survey will measure our outcomes to see if any of our potential initial effects hold up. We will also test for differential selection in the follow-up sample.

We will also attempt to improve data quality in several ways. Following Alesina, Stantcheva, and Teso (2018), the consent page will emphasize the importance of thoughtful responses using statements such as “responding without adequate effort may result in responses being flagged for low quality.” Moreover, we will appeal to respondents’ sense

\textsuperscript{13}While stated preferences may be different (or, in some cases, inflated), this should not affect the relative differences between treated conditions. See Malhotra, Monin, and Tomz (2019), footnote 9.
of social responsibility by including on the consent page “we are nonpartisan researchers who seek to improve knowledge on social and political issues. It is very important for our research that you answer questions honestly and read each question carefully before answering.” Moreover, we will track response times and drop respondents who spend less than a specific minimum number of minutes, to be determined. Before the experimental portion of the survey, we will implement an “attention check” question (Meade and Craig 2012, Alesina et al) such as “have you devoted your full attention so far and do you believe we should use your responses for the study?” We will also conduct an instructional manipulation check and screen out inattentive subjects at the beginning of the survey (Oppenheimer, Meyvis, and Davidenko 2009, Huang 2015).

4 Conclusion

Our study tackles one of the most salient regulatory issue in the digital economy – individual data privacy – by providing the first comprehensive and rigorous study of the microfoundations of the data privacy debate. We seek to explain individuals’ privacy stances – how and where they vary, and the reasons why. Privacy attitudes will be central to the evolution of digital governance. It is vital that we understand mass public attitudes toward data privacy and what shapes them.

We propose survey experiments in the United States to measure the effect of new information on individuals’ privacy preferences. We seek to explain how information about private sector data harvesting, data breaches, and private regulatory initiatives influence individual support for national privacy regulation. Along with the main treatment effects, we examine whether market ideology explains variation in public support for national privacy regulation.

This project has broader implications for understanding the economic and regulatory policies in the digital economy. One of the foremost policy challenges in the coming decade
involves balancing the economic risks associated with restricting data exchange against citizens’ legitimate privacy concerns. Today, much of the digital economy involves the exchange of personal data for services. At the same time, firms and governments are developing new surveillance tools to track individuals, usually under the guise of crime prevention and security. Advances in artificial intelligence (AI) enable the recognition of personal images and information to understand and predict unlawful behavior. The exchange of personal data occurs all the time, but individual consumers – the data subjects – generally cannot enter the market, and they generally cannot earn profits on the sale of their personal data, leading to increasing public frustration over data policies, or the lack thereof. The contentious politics of data privacy are only just beginning, and our research will contribute microfoundations to the coming debates.
References


Appendix

Survey questions on basic demographic and economic characteristics of the respondents:

- What is your gender? [Male; Female]
- What is your age?
- What was your TOTAL household income, before taxes, last year (2019)? [$0 - $9,999; $10,000 - $14,999; $15,000 - $19,999; $20,000 - $29,999; $30,000 - $39,999; $40,000 - $49,999; $50,000 - $69,999; $70,000 - $89,999; $90,000 - $109,999; $110,000 - $149,999; $150,000 - $199,999; $200,000+]
- Please indicate your marital status [Single; Married; Other]
- In which state do you live
- How would you describe your ethnicity/race? [European American/White; African American/Black; Hispanic/Latino; Asian/Asian American; Other]
- Which category best describes your highest level of education? [Eighth Grade or less; Some High School; High School degree/GED; Some College, no degree; 2-year College Degree; 4-year College Degree; Master’s Degree; Doctoral Degree; Professional Degree (JD, MD, MBA)]
- What is your current employment status? [Full-time employee; Part-time employee; Self-employed or small business owner; Unemployed and looking for work; Student; Not in labor force (for example: retired, or full-time parent)]
- Do you use the internet or email, at least occasionally? [Yes; No]
  - (IF YES) About how often do you use the internet? [Almost constantly; Several times a day; About once a day; Several times a week, OR Less often]
- How often do you use your cell phone? [Almost constantly; Several times a day; About once a day; Several times a week, OR Less often]
  - (IF YES) Do you have a smartphone [Yes; No; I don’t know what a smartphone is]

Letter to senator. The following details our outcome question regarding political behavior (i.e., respondent willingness to contact her senator).

“Writing to the Senators of your state gives you an opportunity to influence privacy regulation. Few citizens email their elected officials, therefore Senators and their staff tend to take such emails from their constituents very seriously. If you would like to write to your Senator, go to the official US Senate list and click on your Senator’s contact webpage. Two sample letters are provided below, one asking for increased data privacy regulation, one asking not to increase data privacy regulation. Feel free to cut-and-paste and edit the text.
before sending it to your Senator. Most Senators’ websites ask for your name and address to avoid spam. We are not able to record what you write on the external (Senator’s) website, so your letter and private information are kept fully confidential.”

Sample letter for increasing data privacy regulation: Dear Senator, In the coming months as you debate data privacy regulation, one of the priorities for Congress should be increasing privacy standards and protecting individual data.

Sample letter for not increasing data regulations: Dear Senator, In the coming months as you debate data privacy regulation, one of the priorities for Congress should be maintaining the open flow of data so that companies can use it to provide high quality services to consumers.

[Email the Senator to increase data privacy regulation; Email the Senator to decrease data privacy regulation; Do not want to email my Senator]