Evaluating a Data Fiduciary Standard for Privacy: Developer and End-user Perspectives

Michele Tang
Pomona College
mtaa2020@mymail.pomona.edu

Liam Bayer Jr.
Pomona College
ljbq2023@mymail.pomona.edu

Leonardo Torres
Pomona College
ltta2019@mymail.pomona.edu

Eleanor Birrell
Pomona College
eleanor.birrell@pomona.edu

Abstract

As concern over data privacy and existing privacy regulations grows, legal scholars have proposed alternative models for data privacy. This work explores the impact of one such model—the *data fiduciary model*, which would stipulate that data processors must use personal information only in ways that reflect the best interest of the data subject—through a pair of user studies. We first conduct an interview study with nine mobile app developers in which we explore whether, how, and why these developers believe their current data practices are consistent with the best interest of their users. We then conduct an online study with 390 users in which we survey participants about whether they consider the same data practices to be in their own best interests. We also ask both developers and users about their attitudes towards and their predictions about the impact of a data fiduciary law, and we conclude with recommendations about such an approach to future privacy regulations.

Keywords

data fiduciary, privacy regulations, developer study, user study

1 Introduction

Increasing awareness of the amount of personal information that is collected and shared by companies—and the potential implications of how that information can be used—has led to a rise in concerns about internet privacy and proposals for comprehensive privacy regulations in the last ten years. To date, 19 U.S. states [14] and 162 countries [17] and have enacted such privacy laws. Most of these laws center *privacy self-management* [8]—the right of an individual to make decisions about how their personal information is used through consent interfaces, opt-out mechanisms, access requests, and other individual actions [48, 49]. However, decades of critiques have consistently shown that privacy self-management falls short of effecting substantive privacy guarantees. Implementations of self-management rights frequently deter people from invoking their rights by leveraging cognitive biases in so-called "dark patterns" [13, 16, 38, 60, 63]. Moreover, privacy self-management simply does not scale to the number of companies with which users regularly interact and the difficulty of identifying the many third parties with access to personal data [33, 42, 48, 49].

In response to these critiques, philosophers and legal scholars have begun to theorize alternate models of privacy. One such proposal calls for a *data fiduciary model* of privacy [6, 44], under which businesses that have access to and control over personal data would have a fiduciary responsibility to the data subjects—that is, they would be required to collect and process that information only in ways that are in the best interest of the data subjects.

In this work, we explored the impact a data fiduciary law might have if enacted in the United States. Specifically, we investigated four research questions:

- **RQ1:** How do developers interpret a best interest standard? What sorts of rationales do developers use to justify behaviors they believe satisfy a user's best interest?
- **RQ2:** Do end-users agree with developers about what data practices are in their best interest?
- **RQ3:** How and to what extent would developers change their data practices if a data fiduciary law were enacted?
- **RQ4:** Are developers and users in favor of a data fiduciary law? Why or why not?

We investigated these four research questions through a pair of user studies. We first conducted an interview study with nine mobile app developers; in this study, we leveraged the privacy label for an app each developer worked on to explore whether, how, and why these developers believe their current data practices are consistent with the best interest of their users. We also explored what changes each developer would make to current practices they deemed inconsistent with a data fiduciary standard. We then conducted an online study with 390 users in which we surveyed participants about whether they consider 26 data practices—drawn from the mobile apps discussed in the developer study—to be in their own best interest. We also asked both developers and users about whether they were in favor of a data fiduciary law and what they thought the impact of such a law would be.

We found that many of the developers we interviewed believe their current data practices are already consistent with a data fiduciary standard. However, some of the developers proposed additions to their current practices, such as increased opt-in features, increased security measures, and improved mechanisms for limiting access to data from non-intended users. Many of the developers were able to justify their current data practices, likely due to the vagueness of a "best interest" standard, suggesting that an effective data fiduciary law would require clear regulatory guidelines and

Proceedings on Privacy Enhancing Technologies 2025(3), 590–607

https://doi.org/10.56553/popets-2025-0114

robust enforcement. Overall, end users agreed with the developer's evaluation of whether a practice was in their best interest for 62% of the 26 data practices we asked about. However, we observed varying attitudes towards data collection versus data sharing: users felt that 85% of data collection practices were in their best interest, compared with only 19% of data sharing practices, and most users strongly opposed data practices that were conducted for advertising purposes.

Overall support for a law enacting a data fiduciary model of privacy was high: 8/9 developers and 89.7% of end users were in favor of such a law. In particular, many users hoped security would be improved and abusive data practices would be ended by a data fiduciary law, confirming that this alternate privacy model merits further consideration from both legal and technical sides. However, this uniformly high support may arise directly from the vagueness of this legal standard—which allows people to project their own desired outcomes onto the data fiduciary framework—suggesting that development and evaluation of concrete examples and guidelines are a critical next step towards evaluating the data fiduciary model of privacy.

2 Background: Data Fiduciaries

In general, fiduciary relationships are those between two parties—a weaker party (the *beneficiary*) and a stronger party (the *fiduciary*)—in which the behavior of the stronger party is legally and ethically constrained [4, 19]. These *fiduciary obligations* generally start with vague, general standards introduced in common law or professional guidelines which are then elaborated and refined over time by the courts through binding judicial decisions [19, 34]. A *duty of loyalty*—the duty "to act for someone else's benefit, while subordinating one's personal interests to that of the other person" [15]—is often interpreted as the core fiduciary obligation. Other fiduciary obligations can include a *duty of care*, a *duty of transparency*, and a *duty of confidentiality* [19]. Existing examples of fiduciary relationships include those between doctors and patients [6, 19, 34] and those between lawyers and their clients [6, 9].

Case Study: Doctors as Fiduciaries. The concept of doctors having a duty of loyalty dates back to ancient Greece, where physicians were members of a professional guild with shared professional principles [19, 31]. New physicians were required to swear the now-famous Hippocratic Oath, vowing to "follow that system of regimen which, according to my ability and judgment, I consider for the benefit of my patients, and abstain from whatever is deleterious and mischievous" [39]. In the United States, courts have recognized doctors as having a legally-enforceable fiduciary relationship with their patients since the 1960s [20, 30]. Exactly what behaviors are required or prohibited by this fiduciary relationship has been elaborated and defined by subsequent case law [34]. For example, in Natanson v. Kline (1960), the Kansas supreme court ruled that doctors have an obligation to "make a full and frank disclosure to the patient of all pertinent facts related to his illness" [37]. In Wickline v. State of California (1986), the Second Appellate District of the Court of Appeals of California ruled that doctors need to attempt to convince insurers to pay for care that the doctor thinks is required [66]. And in Moore v. Regents of the University of California (1990), the California supreme court ruled that physicians need to disclose any other personal interests (e.g., research or financial interests) when seeking consent for a medical procedure [35]. Doctors' fiduciary obligations have also been elaborated by professional standards; for example, the American Medical Association's ethical guidelines discuss when and how to consult with other physicians, the need to facilitate transfer of care when terminating a professional relationship, and the obligation for telehealth providers to be proficient with the relevant technologies [3].

The *data fiduciary* or *information fiduciary* model of privacy [4–6] was proposed as a way to reconcile the conflicting goals of protecting businesses' First Amendment rights and internet users' freedom and privacy. The data fiduciary model extends the general concept of fiduciary relationships to the domain of privacy: the fiduciary—companies or organizations who collect, analyze, use, sell, and distribute people's information, including internet companies, data brokers, and third-parties—would have a legal obligation to act in the interests of the beneficiaries—the end users whose data they collect [5, 6].

Subsequent work has expanded on the original concept of data fiduciaries by elaborating on the duties associated with information fiduciaries and the role of trust in a fiduciary relationship [41], by framing the data fiduciary model as a legal obligation to act in users' best interests (e.g., eliminating dark patterns) [43], by considering trustees as an analogy for data fiduciaries [21], by exploring how data fiduciary requirements should be interpreted and enforced [47], and by drafting an example regulation demonstrating what a data fiduciary law might look like [44]. Potential shortcomings—including the potential for conflicting fiduciary interests between data subjects and corporate stockholders and the potential for inherent conflicts between a data fiduciary model and current business models—have also been identified [23], although other legal scholars argue that these objections do not necessarily undermine the data fiduciary model [58].

In this work, we adopt Richards and Hartzog's framing of data fiduciary requirements as a duty of loyalty [43], in which data processors "would be obligated to act in the best interests of people exposing their data", meaning "they would be prohibited from designing digital tools and processing data in a way that conflicts with [beneficiaries'] best interests". We also draw on examples from their work—avoiding opportunistic behavior, reducing abusive design practices, and prohibiting certain forms of data processing and collection—to contextualize this best-interest standard.

3 Related Work

To the best of our knowledge, this is the first work to empirically evaluate the data fiduciary model of privacy. However, developer and user attitudes towards privacy laws, legal requirements, and privacy standards have been evaluated more broadly.

Developer Studies. Several papers have explored developers' attitudes towards, awareness of, and understanding of various current privacy regulations [2, 11, 12, 22, 40, 59, 62].

Alomar and Egelman [2] explored how developers of child-directed mobile apps attempt to comply with relevant regulations through surveys and interviews. 20-48% of developers said that their organization was not familiar with various relevant privacy

laws (GDPR, COPPA, and CCPA), and about 1/3 changed their perspective on whether their app was legally-compliant after being prompted with accurate information about parental consent requirements. They also found that developers often violated relevant regulations due to incomplete understandings of their apps data practices.

Waldman [62, 64] interviewed technologists and found that privacy was generally not a top priority or was considered non-essential. However, some larger companies had privacy teams that would review products before they were released.

Chalhoub et al. [12] interviewed UX designers and their colleagues from three smart home security camera companies and explored how GDPR impacted the development process.

Peixoto et al. [40] interviewed Brazilian developers to explore what factors affected perception and interpretation of privacy requirements. They found that many were not familiar with Brazil's privacy law and could not correctly interpret privacy requirements in 2019 (after the law was passed but before it went into effect).

Chalhoub and Flechais [11] interviewed smart home business leaders and UX designers. Participants shared that it was difficult for small businesses to understand legal privacy requirements and were often unsure whether various laws applied.

Keküllüoğlu and Acar [22] interviewed software developers at Turkish startups. 5/16 developers mentioned Turkey's privacy law as a consideration during development, but privacy and privacy laws were not always considered during product development.

Utz et al. [59] surveyed website developers and operators about their adoption of third-party services. They found that privacy was rarely considered, except for analytics. Only a quarter of participants reported employing privacy-protecting measures when configuring functionality, but 20/24 participants who explained their rationale for adopting privacy measures cited legal regulations.

Prior research has also explored advice or guidance available to (and used by) developers [2, 10, 27, 53–55, 64] and identified barriers to compliance from the developer's perspective [1, 2, 7, 18, 22, 28, 29, 46, 50–52, 54, 61].

User Attitudes towards Privacy Laws. As data privacy laws have been being passed within the last recent decade, such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), a few user studies about user attitudes towards privacy laws have been conducted. Most of these studies survey users to investigate concerns, opinions, and thoughts of data privacy laws.

Sheth et al. [45] surveyed users in Europe, Asia, and North America about their privacy concerns. They found that the existence of stronger data protection laws (e.g., Europe's GDPR) reduced privacy concerns and that most users believe that privacy laws will be effective.

Zhang et al. [68] investigated Canadians' awareness of and attitudes towards Canada's national data privacy law (PIPEDA). They found that most participants consider the current law to be weak and ineffective, but that many respondents were unclear about the specific privacy protections enacted by the law.

Kyi et al. [25] explored user acceptance of commonly-observed data practices. 400 users were asked a variety of questions, such as whether they would be comfortable sharing their data in specific scenarios and whether they felt a data practice was necessary for a website to function. While websites' privacy policies asserted that their purposes fell under the GDPR's "legitimate interest" standard, those surveyed embraced practices that emphasized their security and were more likely to reject others like advertising.

In follow-up work, Kyi et al. [26] conducted interviews with 23 users, relying on purposes permitted by European privacy legislation. Participants were again distrusting, especially when a data practice purpose could be construed as related to advertising.

4 Methodology

To evaluate the impact of a legal data fiduciary requirement, we conducted two complementary user studies: an interview study with developers and a census-representative online user survey.

4.1 Developer Study

To understand how developers would interpret and apply a data fiduciary standard, we conducted semi-structured interviews with nine mobile app developers. We elected to adopt an interview methodology for the developer study in order to allow an open-ended exploration of developer design decisions, thought processes, and justifications for data practices. This methodology allowed us to elicit thoughtful, expansive responses resulting in a rich qualitative dataset about how these developers would interpret and apply a data fiduciary requirement.

Study Design. At the beginning of each interview, we consented each participant and then selected one app that participant had worked on that was publicly available in the iOS or Android app store. To contextualize the conversation, we then asked general questions about the participant's development experience, their role in the development of that app, and how that company handled privacy decisions.

To gain a more in-depth understanding of the app data practices and to get participants to start thinking about privacy, we then looked at the privacy label—a standardized summary of data use practices required by the Android and iOS app stores—for the selected app, walked through each of the disclosed data practices, and asked participants to identify data practices with potential privacy implications. We also asked about whether privacy considerations affected decisions about what data to collect or share or how to use data they collected.

In order to gain an in-depth understanding of how these developers would interpret and apply a data fiduciary standard, we then proceeded to present each participant with a brief description of a hypothetical data fiduciary requirement. This language was based on elements and examples identified in the legal literature [43], although it deliberately left details open to interpretation.

> *Imagine a new privacy regulation is enacted where any party engaging in user data collection is obligated to act in the best interests of those users. Acting in the users' best interest means putting their well-being first. This could look like avoiding opportunistic behavior, reducing abusive design practices, and prohibiting certain forms of data processing and collection, among other things.*

ID	Gender	Race	Age	Years Exp.	App Cat.	Comp. Type	Downloads
P1	Male	Black or African American	25-34	5	Finance	Small tech	1M+
P2	Male	White	25-34	13	Education	Non-tech	5M+
P3	Male	Black or African American	25-34	5	Finance	Startup	10K+
P4	Male	Asian	35-44	10	Medical	Non-tech	5K+
P5	Male	Black or African American	25-34	5	Education	Non-tech	10K+
P6	Male	Black or African American	25-34	7	Shopping	Big tech	50M+
P7	Female	Asian	25-34	2	Shopping	Small tech	500M+
P8	Male	Black or African American	25-34	5	Shopping	Small tech	5M+
P9	Male	Black or African American	25-34	4	Productivity	Non-tech	5M+

Table 1: Demographic information of participants and app information. Includes participant ID, gender, race, age, years of experience (Years Exp.), app category (App Cat.), company type (Comp. Type), and number of downloads. Download counts includes only Android downloads because the iOS app store does not publish this information.

We then looked back at the privacy label for the selected app, walked through each of the disclosed data practices, and asked the participant to reflect on whether and why (or why not) each practice was in the best interest of app users. We also asked how they would change their data practices to comply with a best-interest standard.

After discussing all the individual data practices, the interview concluded with general questions about participants' opinions about such a legal requirement and what they thought the benefits or challenges would be for complying with a data fiduciary standard. Our interview script is provided in Appendix B.

Developer Recruitment. To recruit participants, we made posts on subreddits relevant to app development—`r/AppDevelopers`, `r/mAndroidDev`, and `r/iosdev`—with information about the study and a link to a screening survey. The screening survey, which is reproduced in Appendix A, contained a consent form, questions about app development experience, and demographic questions. It also asked for a link to an app on the iOS or Android app store that they had worked on. We considered people to be eligible for the study if they were at least 18 years old, resided in the United States, had experience as a software developer, and provided a link to an app that had a privacy label.

We contacted all eligible developers who completed our screening survey, and we successfully scheduled and conducted nine developer interviews. Each interview lasted approximately 30 minutes and participants were compensated with a $30 Amazon gift card. Demographic information about our participants and the apps they worked on is provided in Table 1.

Data Analysis. After completing the interviews and cleaning the auto-transcriptions, we manually performed one round of thematic analysis on the interview transcripts using inductive qualitative coding. One author did the primary analysis, and the resulting codes were reviewed and discussed with a second author. All interview participants were included in the analysis.

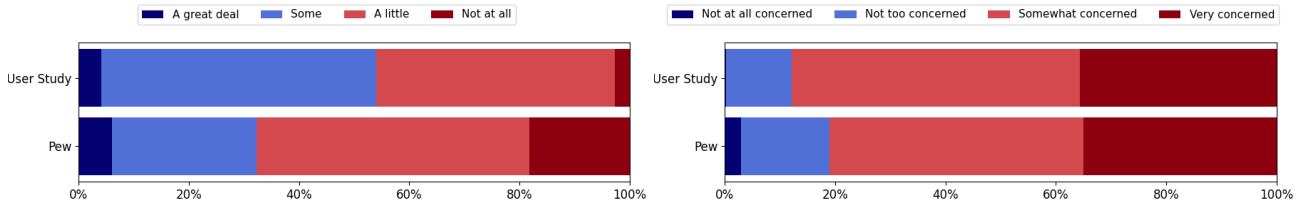
Limitations. While the interview methodology allowed us to elicit in-depth reflections and responses, the consequent small scale of our developer study inherently precludes making any generalizable claims about developer opinions or attitudes. It also precludes direct comparison between developer and user attitudes. Moreover, our results may not be representative of all developers. While the developers we interviewed represent a range of companies (both in terms of corporate size and app category), our participants skewed young (8/9 were under 35), and people of color were overrepresented (6/9 participants were Black or African American).

Moreover, the text used to prompt reflection about a hypothetical data fiduciary law was based on one particular framing—Richard and Hartzog's language framing data fiduciary responsibilities as a duty to act in the best interest of the users [43]—and is unable to capture all of the intricacies of the large body of legal scholarship pertaining to proposed data fiduciary regulations or all of the possible nuances of legal interpretation and enforcement. In addition, this work relied on data practices disclosed in app privacy labels as the ground-truth for reflecting on an app's data practices, however prior work has found that these labels are not always accurate [24, 67]. Finally, participants were reflecting on code they wrote as part of their employment; despite our confidentially guarantees, they may not have felt free to fully express negative opinions about their work.

4.2 User Study

To understand how end-users would interpret a data fiduciary standard and how user interpretations would compare to the developers' interpretations, we conducted a follow-up study with end-users. Unlike the developer study—for which we felt it was essential to elicit in-depth reflections—the core of our user study was comprised of evaluating concrete data practices. Since such responses would benefit less from in-depth justification, we felt that the benefits of scale and generalizability outweighed the drawbacks and therefore opted in favor of a large-scale online survey for our end-user study.

Study Design. Because we wanted to compare user interpretations of a data fiduciary standard directly to the app developer's interpretations, we started by identifying scenarios for users to evaluate. We identified 57 quotations from the developer study transcripts in which the developer directly addressed whether a particular data practice shown in the app privacy label was or was not in the best interest of their users. Of these, we identified 31 data practices for which the developer provided a clear rationale for why the data practice was or was not in the best interest of their users. In the interest of optimizing survey length, we eliminated five data practices that were essential to the core functionality of the app



(a) "How much do you feel you understand what companies are doing with the data they collect about you?"

(b) "How concerned are you, if at all, about how companies are using the data they collect about you?"

Figure 1: General privacy attitudes of our user study population compared to the overall United States, as determined by the Pew Research Center [32].

and seemed to be clearly consistent with a fiduciary standard—for example, a medical app that collected users' health information to share it with their doctor, leaving us with 26 data practices we asked users to evaluate.

At the start of the survey, participants were presented with the same language about a hypothetical data fiduciary regulation that was used in the developer study. We then asked participants to rank whether each of the 26 data practices were consistent with their best interest on a five-point Likert scale. In each case, we provided contextual information about the type of app, the data type, and the purpose of the data collection. All questions were designed to avoid technical terminology and language that might be not be familiar to users [36, 57]. For example, *"Imagine you use a shopping app that securely stores your email address on the company's machines in order to send you personalized offers and opportunities. Do you agree this data storage in your best interest?"* or *"Imagine you use a shopping app that securely sends your purchase history to other companies in order to prevent fraud. Do you agree this data transfer in your best interest?"*

We then asked general questions about a data fiduciary law. We asked each participant to rank their opinion of such a law on a five-point Likert scale. We then asked two free response questions: asking them to explain why they were (or were not) in favor of such a law and asking how they thought companies would change their data practices in response to a data fiduciary law.

Finally, we concluded with demographic questions and questions about general privacy attitudes.

The full user survey is provided in Appendix C.

User Study Recruitment. We recruited 400 participants through Prolific using the United States representative sample option[1]. One Prolific user declined consent and therefore did not complete the survey; nine users were omitted because the free-response answers appeared to have been auto-generated. We analyzed the remaining 390 responses. The demographics of our user study population as compared to the overall United States population, as published in the American Community Survey (ACS), are given in Table 2. Since Prolific users are generally more tech-savvy than the overall U.S. population [56], a comparison between the general privacy privacy attitudes of our user study population and the overall United States population [32] is given in Figure 1.

[1]This setting ensures that participant demographics by age, sex, and ethnicity will match the most recent United States census data.

Demographic		User Study	U.S.
Age	18-24	12.3%	12.0%
	25-34	17.7%	17.3%
	35-44	16.7%	16.9%
	45-59	32.3%	23.4%
	60-74	18.7%	21.2%
	75+	2.3%	9.2%
Race	White	59.7%	60.9%
	Black	10.5%	12.2%
	Asian	5.9%	5.9%
	Native Am.	0.3%	0.3%
	Other	23.3%	19.8%
Gender	Male	47.2%	49.1%
	Female	49.5%	50.9%
	Non-binary	2.8%	-
	Other/No answer	0.5%	-

Table 2: User study demographics compared to the demographics of the United States, as published in the American Community Survey (ACS).

Data Analysis. For the Likert-scale questions, we report descriptive statistics. For the two free-response questions, we completed two rounds of thematic analysis: an initial round of inductive coding to identify a set of labels, and a second round after clarifying the codebook and the definitions of each label. Both questions were double-coded by two authors, with Cohen's Kappa scores of .83 and .93 respectively.

Limitations. For our large-scale user study, we recruited participants through Prolific. Although we used Prolific's U.S. census-representative sample setting—and prior work has shown that Prolific responses to privacy and security surveys are generally representative of overall U.S. views [56]—Prolific users are generally younger, more highly educated, and more tech-savvy than the overall U.S. population [56]. These differences may explain the differences in general privacy attitudes between our participants and those of a recent Pew panel study (Figure 1). They also suggest that attitudes of less educated, older, and less technologically-inclined users may not be fully represented in our results.

Additionally, the 26 scenario questions leveraged in our user study were determined by which practices developers provided

Theme	Explanation	Example Quote	Participants
Minimizing Data Collection	Limiting the amount of data collected	*"You have to actually [act in] the best interests of those users, even if it means that limiting the data that the app is collecting, just to make sure that the users are safe."*	P1, P4, P6, P7
Minimizing Access to Data	Limiting access to data from non-intended or non-necessary recipients	*"Nobody outside the teacher could see the students' progress or data."*	P1, P2
User Control	Giving users control over their data, requiring consent for data collection	*"For every action that should be taken in the app... the user should have total control of their data."*	P1, P3, P5, P6, P7, P8, P9
Transparency	Being transparent to users about data practices	*"They actually provide a detailed privacy policy that really explains how data is being collected and used."*	P9
Security	Ensuring that data is stored securely, preventing leaks	*"That data is well encrypted to make sure that it is not just easily accessible."*	P1, P2, P3, P4, P5, P6, P7, P8
Feature Support	Providing features users want	*"Linking to them to offers... that will be in the best interest."*	P2, P4, P5, P6, P7, P8, P9
App usability	Creating an easy-to-use app interface	*"You have to put yourself in the position of the user. Will it make complete sense [when it's] in their mind[?]"*	P3, P5
Prioritizing Users' Interests	Prioritizing user interests over company or profit interests	*"Putting the user in the first priority...before considering maybe the client and also maybe every other person."*	P1, P4, P8
Personalized Standards	Different users may have different ideas of what "best interest" means to them	*"The best interest is not the same for everybody."*	P7

Table 3: Developer interpretations of a "Best Interest" data fiduciary standard.

sufficient details about during the developer interview study. Consequently, the data practices discussed in our user study may not uniformly cover the full space of relevant app data practices.

4.3 Ethical Considerations

Care was taken throughout the research process to adhere to best practices and ethical standards. Prolific users were compensated $2.75 and the median completion time was 10.07 minutes, ensuring that compensation met minimum wage standards. In recognition of their expertise, developers were paid $30 for interviews that lasted no more than 30 minutes. We obtained informed consent from all participants in both studies, including explicit consent to record developer interviews, and collection of personal information was minimized. All study protocols were reviewed and approved in advance by the Pomona College IRB.

5 Results

We analyzed the data collected from our two user studies to evaluate our four research questions: (1) How do developers interpret a best interest standard? What sorts of rationales do developers use to justify behaviors they believe satisfy a user's best interest? (2) Do end-users agree with developers about what data practices are in their best interest? (3) How and to what extent would developers change their data practices if a data fiduciary law were enacted? and (4) Are developers and users in favor of a data fiduciary law? Why or why not?

5.1 Developer Interpretations of "Best Interest"

We identified eight themes in how the developers we interviewed interpreted a user's best interest and in what rationales they used to justify why particular data practices were or were not consistent with a data fiduciary standard. These themes are summarized in Table 3.

Four of these themes pertained to different privacy aspects: Minimizing Data Collection, Minimizing Access to Data, User Control, and Transparency. 8/9 developers in our study interpreted best interest as including at least one privacy aspect.

Minimizing Data Collection (P1, P4, P6, P7). 4/9 developers discussed minimizing the amount of data collected, usually interpreted as collecting only data necessary for the app to function. For example, P6 argued that their app should collect a limited amount of data for user safety: "You have to actually [act in] the best interests of those users, even if it means that limiting the data that the app is collecting, just to make sure that the users are safe." Similarly, P4 argued that only collecting enough data for the app to function was in the best interest of users, something that their app was already practicing. Specifically, their app was a health app held to HIPAA regulations, thus they did not collect more information than necessary: "Because the app is kind of focused on making sure that the patient is taken care of as best as our ability...We don't have anything in there that basically isn't necessary for tracking and monitoring [reactions]."

Minimizing Access to Data (P1, P2). 2/9 developers mentioned minimizing access to data or preventing non-intended recipients

from receiving user data. For P1's financial app, this meant that even the app owner or investors could not see user data. For P2's education app, this meant "nobody outside the teacher could see the students' progress or data."

User Control (P1, P3, P5, P6, P7, P8, P9). 7/9 developers described the user's best interest as giving users increased control over their data, whether that be through consistent requests for consent or more features for opting-into or opting-out of data collection. P6 discussed giving users more control over their data more broadly, stating: "For every action that should be taken in the app, the user has to be thought about, and the user should have total control of their data." P1 and P3 discussed consent as a way to give users more control, with P3 stating: "So it's the user who has a final say whether they want their data to be out or not. I think that means we get the consent every time from the user." P8 and P9 viewed features for opting-in to data collection as one way to give users more control over their data. P9 stated, "If I also allow users [to] opt-out of sharing their data, so these are actually acting in the user's best interest." And P8 mentioned making collection of photos and videos optional, "If our user is interested to share it, then it will act to their best interest... Some users feel like they want to share, others feel like they don't want to share, so [it's] just up to them." P5 and P6 identified supporting a right to delete as being in the best interest of their users.

Transparency (P9). P9 mentioned being transparent to users about data practices, specifically in the privacy policy. This was something they believed their app already did a good job with: "It means being transparent about the data collected [and] being used...[for example,] actually provide a detailed privacy policy that really explains how data is being collected and used."

We also identified three themes that did not directly relate to privacy: Data Security, Feature Support, and App Usability. All 9 developers in our study interpreted best interest to include a non-privacy aspect.

Security (P1, P2, P3, P4, P5, P6, P7, P8). 8/9 developers discussed promoting security measures, such as using encryption or preventing data breaches, as being in the best interest their users. For example, P1 discussed encrypting data as one way to secure data, "Maybe that data is well-encrypted to make sure that it is not just easily accessible," and six developers noted that encrypting data in transit—a practice that is disclosed in Android data safety labels—was in the best interest of their users. P2, who worked on an education app, discussed secure authentication as being in their users best interest, "I would expect passwords and stuff to be stored [securely] I would even expect there would be some [two factor authentication] on the teacher side, which we didn't have at the time when I was working on that app." P1 and P3 both discussed fraud prevention as being in their users best interest; however, while P1 only used this rationale to collect Device ID ("it's important that we have the Device ID just to protect [our users]"), P3 used this justification for collecting user ID, address, phone number, and sexual orientation.

Feature Support (P2, P4, P5, P6, P7, P8, P9). 7/9 identified supporting particular features as being in the best interest of their users. For example, both P6 and P8 stated that it was in the best interest of their users to collect email addresses so they could "link one with opportunities to offers" (P6). P7 and P8 mentioned features that support convenience, such as saving personal information, "Once we have that data... next time they don't have to put in that data... It's saving them time and also making their work easier" (P8). P2, P4, P5, and P9 justified collecting particular data because it was needed to support features in their app. For example, P4 stated that collecting data about messages is in the best interest of their users because "this is basically the default communication method that most people have access to, so I'm not sure that there's really another option for a reliable way to send people messages". P5 justified collecting precise location as, "Yeah, it's in the user's best interest because, you know, the location is important, especially precise location, to ease their movements in and out."

App Usability (P3, P5). 2/9 developers discussed having a user-friendly interface as being part of their users' best interest. P3's response started with a broad discussion of developers' responsibility to understand their users and develop an app that makes sense to them, "You as a developer can map out and assume anyone can use this application in this manner in which it's making complete sense in your mind, but now you have to put yourself in the position of the user. Will it make complete sense [when it's] in their mind?" For P5, user-friendliness was connected to developing privacy related features. They stated that acting in the best interest for their app would be, "having an app which is actually user friendly and ... [the user] can choose maybe to be more incognito."

In addition to these outcome-based themes, some developers also interpreted a best-interest standard as requiring a particular process, such as prioritizing the user over other stakeholders or applying personalized standards. 4/9 developers discussed process-based themes.

Prioritizing Users' Interests (P1, P4, P8). 3/9 developers discussed prioritizing users' interests over those of other stakeholders such as shareholders or business clients. For example, P8 described acting in the best interest of the user as "putting the user in the first priority... before considering maybe the client and also maybe every other person." P4 described social media apps that "see [their] users as a harvest-able kind of thing" as an example of companies failing to act in the best interest of users by not prioritizing their interests.

Personalized Standards (P7). P7 mentioned that "best interest" may look different depending on the user, "I guess it's hard to say because— I don't really know. Maybe the best interest is not the same for everybody." This raised the prospect that a data fiduciary law might require companies to discover and comply with a diverse set of individual interpretations of what constitutes their best interest.

5.2 User Alignment with Developer Evaluation

In general, users frequently agreed with the app developer about whether it was in the their best interest for various apps to collect various types of data for various different purposes (Figure 2). However, we found a lot of discrepancies about sharing data with third parties (Figure 3).

(a) Developer says is in users' best interest, Users agree is in their best interest.

(b) Developer says is in users' best interest, User opinions are mixed.

(c) Developer says is in users' best interest, Users say is *not* in their best interest.

(d) Developer says is *not* in users' best interest, Users say is in their best interest.

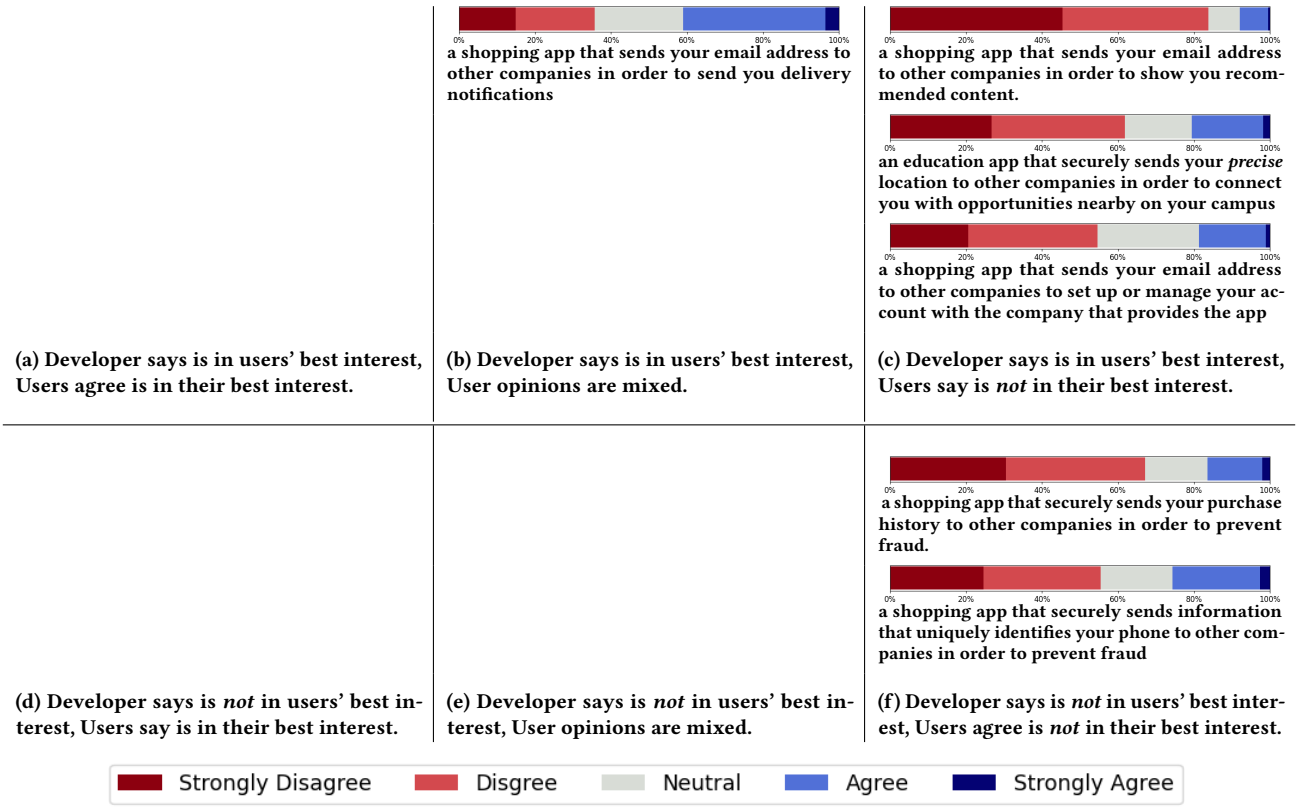
(e) Developer says is *not* in users' best interest, User opinions are mixed.

(f) Developer says is *not* in users' best interest, Users agree is *not* in their best interest.

Figure 2: User alignment with developer opinions about which data *collection* practices are in their users' best interest.

Data Collection Practices. Overall, we found that users generally agreed with the developer's evaluation of whether collecting particular data for a particular purpose was appropriate for their app.

Of the 15 data collection practices that the developer deemed to be in the best interest of their users, a majority of users agreed that 7/15 were in their best interest and there was no consensus for another 7/15. The strongest agreement was about a shopping app that stores users' email addresses in order to contact the user if an issue arises (both the developer and 70.3% of users considered this data collection to be in users' best interest) and about a medical app that stores emails sent to them so that doctors can communicate with patients (both the developer and 62.6% of users considered this data collection to be in users' best interest). Example data collection practices for which there was no consensus among users—that is, the median score was to neither agree nor disagree—include a shopping app storing device identifiers in order to authenticate the user (45.4% of users thought it was in their best interest, 26.2% thought it was not) and a shopping app storing email addresses in order to send personalized offers and opportunities (31.0% of users thought it was in their best interest, 44.1% thought it was not).



(a) Developer says is in users' best interest, Users agree is in their best interest.

(b) Developer says is in users' best interest, User opinions are mixed.

(c) Developer says is in users' best interest, Users say is *not* in their best interest.

(d) Developer says is *not* in users' best interest, Users say is in their best interest.

(e) Developer says is *not* in users' best interest, User opinions are mixed.

(f) Developer says is *not* in users' best interest, Users agree is *not* in their best interest.

Figure 3: User alignment with developer opinions about which data *sharing* practices are in their users' best interest.

There was only one data collection practice that the developer thought was in the best interest of their users while a majority of users disagreed. 67.2% of users disagreed with developer P7's assertion that it was in their best interest for a shopping app to store precise location in order to set up or manage their users' accounts. This is consistent with prior work that has found that users consider precise location to be particularly sensitive information.

Similarly, our user survey included five data collection practices that the developer identified as violating a best-interest standard. Of these five data practices, a majority of users agreed that 2/5 practices were not in their best interest (e.g., 72.1% of users agreed with developer P7 that a shopping app that collects device identifiers in order to send ads or marketing communications would not be acting in their best interest). For another 2/5 such data collection practices, user opinions were mixed.

There was only one data collection practice that the developer flagged as not in their users' best interest but that a majority of users considered compatible with this standard: 59.7% of users thought it would be in their best interest for a medical app to store their name in order to include it in medical documents. In that case, developer P4 thought that data collection could be minimized by using a pseudonymous identifier rather than name in order to be more compatible with a data fiduciary standard, a view that may reflect HIPAA's emphasis on simple de-identification techniques such as removing names as a mechanism to reflect privacy. However, users felt that including their name in medical documents was appropriate in this context.

Data Sharing Practices. We surveyed users about six data sharing practices: four practices that the developer considered to be in the best interest of their users and two practices that the developer deemed to violate this standard. However, we found that users were highly skeptical that any data sharing was in their best interest. There was one data practice (a shopping app that sends your email address to other companies in order to send you delivery notifications) for which there was no consensus among end-users about whether or not this was in their best interest. For the other five data sharing practices, a majority of users thought that data sharing in that context was not in their best interest. This meant that the only two data sharing practices for which users were in alignment with the app developer were the two such practices that the developer identified as not being in their users' best interest.

Some of the misalignments we observed may result from user misunderstandings about how third-party services and libraries are used in the modern app development ecosystem. For example, users may not recognize how commonly features like delivery notifications and account management are implemented using third-party libraries or services. However, the strongest points of misalignment appear to signify significant disagreements between the developer and the end users about how to interpret a best-interest standard. For example, developer P6 thought it was in their users' best interest

to send their email address to third-parties in order to show the user recommended content on their shopping app, but 83.8% of users thought it was not in their best interest. And developer P5 thought it was in their users' best interest to send precise location data to third-parties in order to connect users with opportunities near their campus, but 61.8% of users thought it was not. Both of these example practices were evaluated by developers who thought that feature support such as linking users with offers was in their users' best interest, as discussed in Section 5.1. However, as discussed in Section 5.3.2, many users thought that a data fiduciary law would prohibit or restrict current data sharing practices, suggesting a high level of skepticism that data sharing is in their best interest.

5.3 Anticipated Effects of a Data Fiduciary Law

We asked participants in both studies about what effects they would anticipate if a data fiduciary law were enacted. For the developers, we asked what changes they would make every time they identified a data practice as not in the best interest of their users; we also asked them to reflect at the end about the extent to which they would change their data practices if such a regulation were enacted. For users, we asked one free-response question about how they thought companies' data practices would change to comply with a hypothetical data fiduciary law.

5.3.1 Developer Anticipated Effects. How much impact the developers we interviewed thought a data fiduciary law would have depended both on their interpretation of the best interest standard and on their app's current data practices.

3/9 developers in our developer study (P3, P4, and P8) said that they would not make any changes to their app if a data fiduciary law were enacted because they believe that their app is already compliant with a best interest standard. For example, P8 said their projects always prioritize the user's best interests, "I prioritize the users... I had the user at the best interest, that's why I made options, and I really make sure that the data is encrypted." P4, who worked on a health-app and had ensured that the app was HIPAA-compliant, thought that a data fiduciary regulation would be less strict than HIPAA, "I imagine that whatever regulations that we're held under are probably a little bit more strict than what would be the legislation that theoretically you're proposing."

5/9 developers (P1, P2, P5, P6, and P9) anticipated that they would make minor changes to their app if a data fiduciary regulation were enacted. P1 mentioned getting ongoing affirmative consent from users rather than implicit or one-time consent, "[Right now] it's just in our terms and conditions, but it's not really that serious... I think maybe that could be a little bit adjusted because sometimes a user may consent today and a user may change their mind tomorrow. So I think it's just important every time [to] just get consent rather than having one-time consent." P2 would ensure that data was properly encrypted so outsiders could not access user data and would also minimize internal access to data, noting that "I could look up any teacher's ID and see their usage as a developer. I guess I could see how well classes [are] performing and that's probably not good... If the production environment somehow had another layer that I could just see what they were doing... where I don't need to know the teacher's name... I think that would be an improvement." P5 would add more options for users to choose the data they wanted to expose and would create a private mode. P6 would would improve encryption, reduce data collection, add a feature in the app interface to support data deletion, and would add customer service support for discussing privacy concerns; P6 also said that they would connect users to more sales and promotions. P9 would revise their privacy policy to improve transparency and would add a feature allowing users to use the app anonymously.

Developer P7 anticipated that substantial changes would be required to make their shopping app compliant with a data fiduciary regulation. In general, they interpreted a core element of a user's best interest to be more conservative about minimizing data collection and sharing and therefore thought that "a lot of changes would have to be made." For example, they noted that their app currently shares device or other IDs with other companies, but said "I don't really know how that information is helpful... so I don't really see why that would be necessary." They also thought that their app currently included predatory features, such as location-based shopping suggestions, "[we] also show you suggestions of what to buy based on your location, based on what other people [at] your location have looked at... Best interest I would probably say is not even store approximate location because showing people things that they didn't ask for which might interest them feels a little bit predatory." They also suggested that apps should make it optional to save or store personal information.

5.3.2 User Anticipated Effects. Many users anticipated that such a law would have a positive impact on privacy. Most anticipated changes aligned with interpretations of the best-interest standard that we had previously observed in our developer study. 16.9% of users anticipated that this law would minimize data collection, 13.1% anticipated it would result in increased user control of data collection or use, and 20.8% said it would enhance transparency about corporate data practices. However, the most commonly mentioned anticipated effect was that a data fiduciary standard would stop the practice of transferring data or sharing data with third parties (22.6%) and that it would prohibit sale of personal information to third parties (15.4%); this was not an effect anticipated by participants in our developer study, and the resulting discrepancy explains many of the misalignments between the developer and user interpretations of best interest. Moreover, 13.6% of users mentioned that a data fiduciary law would require companies to eliminate deceptive or abusive practices that were inconsistent with privacy, with many particularly stating that it would preclude using personal information for targeted advertising. This theme did not emerge in our developer interviews; only P7 mentioned eliminating predatory features, and none of the developers interviewed considered targeted advertising to be incompatible with a data fiduciary law.

Like the developers, some users also anticipated that a data fiduciary law would have impacts that are not directly tied to privacy. 13.8% users anticipated that a data fiduciary law would require companies to improve their system security, a theme that is consistent with the results of our developer study. However, none of our users mentioned improvements to usability or the introduction of new features as potential impacts of a best-interest standard, despite these themes emerging repeatedly in our developer interviews.

Some users were skeptical that a data fiduciary law would have any positive impact. 4.9% thought loopholes would render such a law ineffective, and 4.6% thought a "best interest" standard was too vague to be effective. Six users thought that a data fiduciary law would result in no changes, and two mentioned potential unintended consequences such as forcing companies to charge for their products or putting companies out of business.

5.4 Attitudes towards a Data Fiduciary Law

Overall attitudes towards a data fiduciary law were strongly positive, with 8/9 developers and 89.7% of users in favor of enacting such a law.

5.4.1 Developer Attitudes. 8/9 developers were in favor of enacting a data fiduciary law requiring companies to process personal information only in ways consistent with the best interest of the data subjects.

Six developers explicitly identified aspects of their interpretation of "best interest" as positive impacts that a data fiduciary law would have, thereby justifying the adoption of such a regulation. Three developers (P1, P2, and P3) thought that a data fiduciary law would be a good idea because it would increase user control over their data. For example, P1 said, "I think that's the direction that developers need because it has to be users' best interest in everything that we do...to really make sure that the user is really in control." P2 reflected that this would give people ownership of their data, "data should be your own, no matter what application you're using." Two developers (P6 and P9) referred to anticipated improvements in the user-friendliness of apps as a reason such a law would be a good idea. For example, P6 said, "at the end of the day we want to have more users using our app and if we have services that prioritizes users and they have their data well [protected], everything [is] working fine, the interface is easy to use—if a person is using [the app] for the first time, they don't have a hard time operating, then that's in the user's best interest." P5 discussed anticipated improvements in security, stating that adversaries are "getting smarter every day" and thus that "it's important to get a step ahead in protecting data."

Other reasons cited for why a data fiduciary law would be a good idea included increased trust in an app (P8: "If the users feel confident using the app, then that's an advantage even to the client who owns the project") and a general sense that there was a need for stronger privacy regulation in the United States (P4: "I definitely think that there's probably an overstepping of privacy violations. A lot of these services kind of use people as a revenue source... It's like the saying that if the product is free, then you're the product... I think that a lot stronger privacy regulations [are needed]. I'm kind of a fan of GDPR. Our app is also used in Europe and the version of the app that we use in Europe is a lot more...the patient's rights are more so than the American version"). P2 emphasized that such a law would codify what they already view as a developer's responsibility to develop software that prioritizes their users' best interest, "I think as developers, we have a responsibility to push for this, even if business decisions aren't thinking of this. I think upper management doesn't think of this. Yeah I think it's a great idea."

Only one developer interviewed (P7) expressed opposition to a data fiduciary law. Their primary concerns were that such a law might prohibit existing features that users might like, such as targeted advertising ("Maybe someone might want to see other items that they didn't think of to search, but they might still want to buy") and the ability to save personal information for future use ("A lot of it also is convenience because not being able to save addresses or your location—I feel like it's also saved for convenience, not just targeted ads"). They also discussed challenges for developers in complying with a hypothetical data fiduciary standard, including the cost of developing and maintaining the more complicated control flow necessitated by additional opt-in interfaces ("There probably would need to be a lot more opt-in save this data. Because I feel like [some users] still want the convenience, maybe there's these users who would want their data to be stored, so I feel like a lot more things have to be opt-in and then there would have to be different flows based on that") and the challenges of balancing functionality and privacy ("[The app I worked on] has many features such as location sharing, calendar syncing, that requires user data... So it can be difficult to create an app that provides useful features and also protects the user's privacy").

5.4.2 User Attitudes. 89.7% of users said that they "strongly agree" or "agree" that enacting a data fiduciary law would be a good idea. 6.7% of users were neutral and 3.6% disagreed or strongly disagreed. We also qualitatively analyzed free-response answers explaining why each person was or was not in favor of a data fiduciary law.

The most common explanation for why users were in favor of a data fiduciary law was a general sense that such a law would result in increased protections for user data. 35.9% users mentioned such themes. For example, "Because it would be looking out for the privacy of my data and security," "Companies should have an obligation to protect your data," and "[it] could eliminate so-called 'accidental' breaches because having data exposed to data hacking attempts would not be in the user's best interest." While many of these explanations were vague, they reflected a optimistic attitude toward the potential impact of a data fiduciary regulation.

Many users were in favor of a data fiduciary law because they anticipated that it would have a specific positive impact on various aspects of privacy, as discussed in Section 5.3.2. 21.3% critiqued current data practices they identified as abusive and believed would be prohibited by such a regulation. For example, one participant simply stated that "too much user data is [currently] being used for nefarious reasons" and another predicted "It would prevent companies from misusing the information they are collecting." Several participants mentioned reducing data use for advertising purposes and interrupting the current data economy as a reason to support a data fiduciary law. For example, one said, "Our well-being should be first and foremost, NOT giving out our private data willy-nilly in order to bombard us with advertisements and risk sharing our data with untoward companies. The companies and apps making money should not trump our privacy." Another participant reflected, "This privacy law, if it functions as intended, could protects users from their data being stored or passed around in ways they are uncomfortable with. It might reduce instances of companies taking advantage of users through advertising, deception, and capitalizing on a large amount of a user's data."

Other anticipated privacy benefits that were mentioned in support of a data law included limiting data sharing (mentioned by

15.9% of our users, for example one participant simply said they were in favor because a data fiduciary law would "prevent unnecessary sharing of personal information"), eliminating data sale (mentioned by 10.0% of our users, for example "A lot of companies nowadays get by off selling your information to third parties, so having your best interests at mind would help to protect you"), and limiting data collection (mentioned by 8.2% users, for example "I am tired of companies collecting information about me in order to make money"). 10.5% of participants cited anticipated improvements in user control over personal information as a reason why they support a data fiduciary law, for example, "Because it should always be the user's choice where their data is stored or sent." And 7.9% mentioned anticipated improvements in transparency about data practices as reasons why they are in favor of such a law, for example, "Because we as users have no idea how our personal information is being shared. If that information is provided, it is buried so deep in the privacy agreement that Sherlock Holmes couldn't find it. And if found, the wording is such that we users cannot understand what we are reading. This is wrong!"

Finally, many users indicated support for a data fiduciary law because such a regulation would be compatible with their philosophical ideas of how companies should handle user data. 25.6% explicitly reflected support for requiring companies to prioritize user interests over profits. For example, users said, "I think anything that puts the consumer first over profit is a good idea" and "I am a user. This law works towards the best interests of users. It follows that the law works in my best interest. Therefore, its in my best interest to support this law." Additionally, 9.7% of users mentioned that they were in favor of expanded regulatory oversight, which such a law would provide, for example, "corporations cannot be trusted to act in my best interest without legal ramifications" and "Privacy regulation is becoming more important in the digital age and needs legislation to enforce restrictions." 9.7% of users mentioned that they would trust companies more if such a regulation were in effect.

However, a small minority of users did not support enacting a data fiduciary regulation. Among these, the most common critique (5.9% of users) was that a best interest standard would be too vague to be effective. For example, one user said, "It is too subjective. What the company believes is in the best interest may be different from what I believe is in my best interest." 2.8% of users, including 6/7 users who strongly disagreed with enacting a data fiduciary law, said that such a law would not go far enough, for example, "I am strongly against data collection and this would still allow data collection. Data should be private, regardless of some law." 2.1% of users predicted that loopholes or non-compliance would render such a law ineffective. For example, "My concern is that it would be defined in a way that leaves loopholes you could drive a truck through" and "they can just lie about what they're doing so it makes no difference. They will just find ways around the laws." Additional critiques that were mentioned by fewer that 5/390 participants included that there was already too much regulation or that such a law might have unintended consequences.

6 Discussion

Our results lead to two important and related insights. The first is variety. Different stakeholders interpret data fiduciary requirements differently. They anticipate that a fiduciary law would have different effects. Their attitudes towards such a requirement varies. The second points to a key shortcoming of this legal proposal: its vagueness.

Participants in our user studies interpreted the described data fiduciary law—and its "best interest" standard—in myriad ways. While many of the interpretations focused on various aspects of data privacy, some of these interpretations reflected data practices already mandated by current privacy regulations (e.g., data minimization, user control and consent, and transparency), albeit perhaps in a stronger form, while other interpretations would prohibit data practices that are common under current privacy regulations (e.g., eliminating transferring data or sharing data with third parties, prohibiting the sale of personal information, and banning use of personal information for targeted advertising). Other interpretations (e.g., improving system security, supporting personalization and other features, and improving interface usability) had no direct privacy implications. Notably, 8/9 developers we interviewed interpreted the best-interest standard as being generally consistent with current practices, whereas 42.6% of the end-users we surveyed interpreted it as prohibiting data practices in ways that would disrupt current practices around data sharing and targeted advertising.

We hypothesize that the extremely high level of support we observed for a data fiduciary law arises directly from the vagueness of the best-interest standard. Because of its vagueness, people project their own desired outcomes onto the standard; they are then naturally in favor of enacting a regulation that requires their desired outcomes. We saw evidence for this theory in both of our user studies. The eight developers who were in favor of a data fiduciary regulation were the same eight developers who anticipated making few or not changes if such a law were enacted, presumably because they interpreted this legal standard to require data practices similar or identical to those they had already voluntarily adopted. And six of these developers explicitly identified aspects of their interpretation of "best interest" as positive impacts that a data fiduciary law would have, thereby justifying the adoption of such a regulation. In our user study, many of the same themes emerged for anticipated effects of a data fiduciary law (Section 5.3.2) and for why people supported a data fiduciary law (Section 5.4.2) because many users cited their interpretation of the law in both places. For example, one user who thought that a data fiduciary law would require companies "to stop selling personal data to third parties such as advertisers" then said that they were in favor of a data fiduciary law because, "Companies should have an obligation to protect your data, not sell it." Conversely, another user who interpreted this standard as requiring consent for data collection ("that company's websites would have consent statements on them to, obtain permission to store and save users data") then said that they were in favor of such a law because "user information would be safe guard[ed] from be used by companies without our consent."

Further research will be required to validate this hypothesis. Future research should also explore the extent to which this hypothesis extends to current regulatory requirements such as data minimization and privacy by design.

The disparate and inconsistent interpretations that arise from this vagueness also pose a challenge to implementation of a data fiduciary law. Passage of a vague standard might suffer from regulatory capture. It takes time for legal challenges to make their way through the court system to create binding case law, and FTC rulemaking likewise takes time. In the interim, the gap between the vague language on the books and the reality on the ground would create an opportunity for companies—particularly big tech-industry actors—to define and interpret rules according to their own best-interest, behavior that had been observed in prior work [64, 65]. This effect could potentially minimize the impact of a data fiduciary standard in favor of a narrower interpretation, e.g., focused on user control, transparency, security, and personalized features. That sort of narrow interpretation would fall short of user expectations and force minimal changes in industry data practices, as predicted by most of the developers we interviewed. In order to be effective, a data fiduciary law would therefore need to provide concrete guidance about how it should be interpreted and applied.

Future interdisciplinary research should develop proposed regulatory language—including examples and guidelines—and then empirically evaluate the draft statute to identify whether and how a more precise legal standard that could generate shared understanding. This would empower a data fiduciary model with consistent interpretations and would bring corporate data practices into alignment with social norms.

Regardless of whether a data fiduciary law is adopted in the United States, our results provide further evidence that there is widespread dissatisfaction with common data practices such as sharing data with third parties, selling personal data, and using personal information for targeted advertising. A data fiduciary regulation with appropriate language and guidelines is one possible approach to banning such practices and bringing corporate data practices into alignment with social norms. However, these data practices are a core component of the current data economy. A law that prohibits such practices could potentially cause significant economic disruption, motivate adoption of new monetization models (e.g., subscription services), trigger as-yet unpredicted changes to the dynamics of the tech industry, or introduce new regulatory obligations.

In order to support the adoption of effective privacy regulations, future work should continue to explore the potential impact of prospective regulations rather than focusing exclusively on enacted laws. Interdisciplinary work should also explore how such possible future laws would impact all stakeholders, including developers, corporations, end-users, and regulators.

7 Conclusion

In this work, we conducted the first empirical evaluation of the impact a data fiduciary law might have if enacted in the United States. We identified a broad range of different ways different developers and end-users would interpret and apply such a legal standard. We also found that users generally agreed with the developers we interviewed about which first-party uses were consistent with a best-interest standard. However, users considered most data sharing to not be in their best interest, and many users specifically identified data sharing, sale of data to third parties, and targeted advertising as not being in their best interest. While we found that most users—and most of the developers we interviewed—were in favor of a data fiduciary law, we argue that the vagueness of the proposed legal standard is likely to undermine its effect and that additional research and evaluation is needed before such an approach should be pursued.

Acknowledgments

Many thanks to Ari Waldman for sharing his legal expertise and for discussions about the discussion. This work was supported in part by NSF grant 2317115 and by internal funds from Pomona College.

References

[1] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. 2020. Why are Developers Struggling to Put GDPR into Practice when Developing Privacy-Preserving Software Systems? *arXiv preprint arXiv:2008.02987* (2020).
[2] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 4 (2022), 250–273.
[3] The American Medical Association. 2024. Code of Ethics Conduct, Ethics Opinions. https://code-medical-ethics.ama-assn.org/opinions. Accessed December 20, 2024.
[4] Jack Balkin. 2014. Information Fiduciaries in the Digital Age. *Balkinization Blog* (2014).
[5] Jack M. Balkin. 2015. Information Fiduciaries and the First Amendment. *UC Davis Law Review* 49 (2015), 1183–1234.
[6] Jack M Balkin. 2020. The fiduciary model of privacy. *Harvard Law Review Forum* 134 (2020), 11–33.
[7] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. 2019. Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society* 35, 3 (2019), 122–142.
[8] Eleanor Birrell, Jay Rodolitz, Angel Ding, Jenna Lee, Emily McReynolds, Jevan Hutson, and Ada Lerner. 2024. SoK: Technical Implementation and Human Impact of Internet Privacy Regulations. In *2024 IEEE Symposium on Security and Privacy (SP)*. 235–235.
[9] Sande Buhai. 2008. Lawyers as Fiduciaries. *Saint Louis University Law Journal* 53 (2008), 553–592.
[10] C. Castelluccia, S. Guerses, M. Hansen, J.H. Hoepman, J. van Hoboken, and B. Vieira. 2017. Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR. ENISA, the European Union Agency for Network and Information Security.
[11] George Chalhoub and Ivan Flechais. 2022. Data Protection at a Discount: Investigating the UX of Data Protection from User, Designer, and Business Leader Perspectives. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–36.
[12] George Chalhoub, Ivan Flechais, Norbert Nthala, and Ruba Abu-Salma. 2020. Innovation inaction or in action? The role of user experience in the security and privacy design of smart home cameras. In *16th Symposium on Usable Privacy and Security*. 185–204.
[13] Nora A Draper and Joseph Turow. 2019. The Corporate Cultivation of Digital Resignation. *New media & society* 21, 8 (2019), 1824–1839.
[14] Andrew Folks. 2024. US State Privacy Legislation Tracker. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. Accessed August 9, 2024.
[15] Bryan A. Garner. 2019. *Black's Law Dictionary, 11th Edition.* Thomson Reuters.
[16] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.
[17] Graham Greenleaf. 2023. Global data privacy laws 2023: 162 national laws and 20 Bills. *181 Privacy Laws and Business International Report 1, 2-4* (February 2023).
[18] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (2018), 259–289.
[19] Sam F. Halabi. 2020. Against Fiduciary Utopianism: The Regulation of Physician Conflicts of Interest and Standards of Care. *UC Irvine Law Review* 11 (2020), 433–488.
[20] Hammonds v. Aetna Casualty & Sur. Co. 1965. 237 F. Supp 96, 102 (N.D. Ohio).

[21] Claudia E. Haupt. 2020. Platforms as trustees: Information fiduciaries and the value of analogy. *Harvard Law Review Forum* 134 (2020), 34–41.

[22] Dilara Keküllüoğlu and Yasemin Acar. 2023. "We are a startup to the core": A qualitative interview study on the security and privacy development practices in Turkish software startups. In *IEEE Symposium on Security and Privacy*. 2015–2031.

[23] Lina M. Khan and David E. Pozen. 2019. A skeptical view of information fiduciaries. *Harvard Law Review* 133, 2 (2019), 497–541.

[24] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. 2022. Keeping privacy labels honest. *Proceedings on Privacy Enhancing Technologies* 4 (2022), 486–506.

[25] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J Biega. 2023. Investigating deceptive design in GDPR's legitimate interest. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–16.

[26] Lin Kyi, Abraham Mhaidli, Cristiana Teixeira Santos, Franziska Roesner, and Asia J. Biega. 2024. "It doesn't tell me anything about how my data is used": User Perceptions of Data Collection Purposes. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–12.

[27] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How developers talk about personal data and what it means for user privacy: A case study of a developer forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–28.

[28] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–24.

[29] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. 2024. Data Safety vs. App Privacy: Comparing the Usability of Android and iOS Privacy Labels. *Proceedings on Privacy Enhancing Technologies* (2024).

[30] Lockett v. Goodill 1967. 71 Wash. 2d 654, 656, 430 P.2d 589, 591.

[31] Dayna Bowen Matthew. 2011. Implementing American health care reform: The fiduciary imperative. *Buffalo Law Review* 59 (2011), 715–808.

[32] Colleen McClain, Michelle Faverio, Monica Anderson, and Eugenie Park. 2023. *How Americans View Data Privacy: The role of technology companies, AI and regulation – plus personal experiences with data breaches, passwords, cybersecurity and privacy policies.* Technical Report. Pew Research Center. http://www.jstor.org/stable/resrep57319

[33] Aleecia M. McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543–568.

[34] Maxwell J. Mehlman. 2015. Why physicians are fiduciaries for their patients. *Indiana Health Law Review* 12 (2015), 1–64.

[35] Moore v. Regents of the Univ. of Cal. 1990. 793 P.2d 479 (Cal. 1990) (en banc).

[36] Charlotte Moremen, Jordan Hoogsteden, and Eleanor Birrell. 2024. Generational Differences in Understandings of Privacy Terminology. *Proceedings on Privacy Enhancing Technologies* 3 (2024), 580–605.

[37] Natanson v. Kline 1960. 350 P.2d 1093, 1101–02 (Kan. 1960).

[38] Sean O'Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. (Un)clear and (In)conspicuous: The Right to Opt-Out of Sale Under CCPA. In *Workshop on Privacy in the Electronic Society*. 59–72.

[39] Ambroise Paré, William Harvey, Edward Jenner, Oliver Wendell Holmes, Joseph Baron Lister, Louis Pasteur, Charles Lyell, et al. 1910. *Scientific Papers: Physiology, Medicine, Surgery, Geology*. Vol. 38. PF Collier.

[40] Mariana Peixoto, Dayse Ferreira, Mateus Cavalcanti, Carla Silva, Jéssyka Vilela, João Araújo, and Tony Gorschek. 2020. On understanding how developers perceive and interpret privacy requirements research preview. In *Requirements Engineering: Foundation for Software Quality: 26th International Working Conference*. 116–123.

[41] Neil Richards and Woodrow Hartzog. 2015. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* 19 (2015), 431–472.

[42] Neil Richards and Woodrow Hartzog. 2018. The Pathologies of Digital Consent. *Washington University Law Review* 96 (2018), 1461–1504.

[43] Neil Richards and Woodrow Hartzog. 2021. A duty of loyalty for privacy law. *Washington University Law Review* 99–1022 (2021), 961.

[44] Neil Richards, Woodrow Hartzog, and Jordan Francis. 2023. A Concrete Proposal for Data Loyalty. *Harvard Journal of Law & Technology* 37, 3 (2023), 1335.

[45] Swapneel Sheth, Gail Kaiser, and Walid Maalej. 2014. Us and them: A study of privacy requirements across North America, Asia, and Europe. In *36th International Conference on Software Engineering*. 859–870.

[46] Sean Sirur, Jason RC Nurse, and Helena Webb. 2018. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*. 88–95.

[47] Felicity Slater. 2022. Enforcing Information Fiduciaries. *Boston University Journal of Science and Technology Law* 28 (2022), 92–132.

[48] Daniel J. Solove. 2012. Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* 126 (2012), 1880–1903.

[49] Daniel J. Solove. 2021. The Myth of the Privacy Paradox. *George Washington Law Review* 89 (2021), 1–51.

[50] Alina Stöver, Nina Gerber, Henning Pridöhl, Max Maass, Sebastian Bretthauer, I. Spiecker, M. Hollick, and D. Herrmann. 2023. How Website Owners Face Privacy Issues: Thematic Analysis of Responses from a Covert Notification Study Reveals Diverse Circumstances and Challenges. *Proceedings on Privacy Enhancing Technologies* 2 (2023), 251–264.

[51] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on Personalized Ads: Nudging Developers About User Privacy. In *17th Symposium on Usable Privacy and Security*. 573–596.

[52] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.

[53] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 114–131.

[54] Mohammad Tahaei, Kopo M Ramokapane, Tianshi Li, Jason I Hong, and Awais Rashid. 2022. Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 33–56.

[55] Mohammad Tahaei and Kami Vaniea. 2021. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–11.

[56] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 367–385.

[57] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. 2021. Defining Privacy: How Users Interpret Technical Terms in Privacy Policies. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 70–94.

[58] Andrew F. Tuch. 2020. A General Defense of Information Fiduciaries. *Washington University Law Review* 98 (2020), 1897–1937.

[59] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2023. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 5–28.

[60] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *ACM SIGSAC Conference on Computer and Communications Security*. 973–990.

[61] Christine Utz, Matthias Michels, Martin Degeling, Ninja Marnau, and Ben Stock. 2023. Comparing Large-Scale Privacy and Security Notifications. *Proceedings on Privacy Enhancing Technologies* 3 (2023), 173–193.

[62] Ari Ezra Waldman. 2018. Designing without privacy. *Houston Law Review* 55, 659 (2018).

[63] Ari Ezra Waldman. 2020. Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'. *Current Opinion in Psychology* 31 (2020), 105–109.

[64] Ari Ezra Waldman. 2021. *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press.

[65] Ari Ezra Waldman. 2022. Privacy, Practice, and Performance. *California Law Review* 110 (2022), 1221–1280.

[66] Wickline vs. State of California 1986. 192 Cal. App. 3d 1630 (2nd Cir. 1986).

[67] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. 2023. Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels. In *32nd USENIX Security Symposium*. 1091–1108.

[68] Leah Zhang-Kennedy and Sonia Chiasson. 2021. "Whether it's moral is a whole other story": Consumer perspectives on privacy regulations and corporate data practices. In *17th Symposium on Usable Privacy and Security*. 197–216.

A Developer Screening Questions

- How many years of experience do you have in mobile app development?
- How many mobile apps have you worked on?
- Consider one mobile app you have worked on. What is the app name?
- Please provide a link to the app in the Google Play Store if available:
- Please provide a link to the app in the iOS App Store if available:
- What was your role in developing this app?
- What kind of company was this app developed for?
  - Big tech company

  - Small tech company
  - Startup
  - Non-tech company
  - Personal Project
  - Other, please describe
- First Name:
- Last Name:
- Email address:
- What is your age?
  - 18 - 24 years
  - 25 - 34 years
  - 35 - 44 years
  - 45 - 54 years
  - 55 - 64 years
  - 65 years or older
- What is your gender?
  - Male
  - Female
  - Non-binary/third gender
- What is your race?
  - Black or African American
  - American Indian or Alaska Native
  - Asian
  - Native Hawaiian or Pacific Islander
  - Other
- Are you of Hispanic/Latino/Spanish origin?
  - Yes
  - No
- Current country of location:
- Current Occupation:

B Developer Interview Script

- Could you tell me about your experience working on app name. What was your role in making that app?
- Was your experience mostly in iOS or Android development? Or both?
- How are privacy decisions managed in your organization and what is your role in that if any?
- Next, could you please pull up the privacy label of your app app name. Can you walk me through this privacy label and explain which of these data practices you think have privacy implications and what those are?
- Are there any things you decided not to collect or things you decided not to do with data because of privacy concerns?
- Now I would like to show you a new privacy regulation that is being considered: Imagine a new privacy regulation is enacted where any party engaging in user data collection is obligated to act in the best interests of those users. Acting in the users' best interest means putting their well-being first. This could look like avoiding opportunistic behavior, reducing abusive design practices, and prohibiting certain forms of data processing and collection, among other things. What do you think acting in a user's "best interest" would look like for your app?
- Let's go back to the privacy label, can you walk me through the label and explain whether you think each element is in the users' best interest? If not, how would you change it?
- Overall, if this regulation were enacted, to what extent would you change your data practices?
- Next, do you think this privacy regulation would be a good idea? Why or why not?
- What could be possible challenges or issues that you would face as a developer or your company would face if there were such a regulation?

C User Survey Questions

Imagine a new privacy regulation is enacted where any party engaging in user data collection is obligated to act in the user's best interest. Acting in the user's best interest means putting the user's well-being first. This could look like avoiding opportunistic behavior, reducing abusive design practices, and prohibiting certain forms of data processing and collection, among other things.

In the following scenarios, assume the company that made the app collects your data and stores your data on their machines.

- Imagine you use a finance app that stores the text messages you send them (including the sender, recipients, and the content of the message) on their machines in order to support some of the app's features. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a finance app that stores information that uniquely identifies your phone on their machines in order to verify your identity. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine your child is using an education app that stores voice recordings on the company's machines in order for their teacher to give them feedback on their speaking skills. Do you agree this data storage in your child's best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine your child is using an education app that stores their username on the company's machines in order for the company to debug issues. Do you agree this data storage in your child's best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree

- Imagine you use a finance app that stores your mailing address on the company's machines in order to prevent fraud. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a medical app that stores the emails you send them (including the email subject line, sender, recipients, and the content of the message) on the company's machines so that your doctor can communicate with you. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a medical app that stores your name on the company's machines in order to include your name on medical documents. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you have asthma and use a medical app that stores information that uniquely identifies your phone on the company's machines in order to enable bluetooth connection with your inhaler. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you have asthma and use a medical app that stores information about your exact location (within 3 square kilometers of where you are) on the company's machines in order to gather data about weather conditions (such as dust information) to provide recommendations on your inhaler usage. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you have asthma and use a medical app that stores information about your approximate location (3 square kilometers or more from where you are) on the company's machines in order to gather data about weather conditions (such as dust information) to provide recommendations on your inhaler usage. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that securely stores your email address on the company's machines in order to send you personalized offers and opportunities. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores information that uniquely identifies your phone on the company's machines in order to send you ads or marketing communications. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores your location (within 3 or more square kilometers from where you are) on the company's machines in order to set up or manage your account with the company that provides the app. Do you this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores your location (within an area of less than 3 square kilometers from where you are) on the company's machines in order to set up or manage your account with the company that provides the app. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that securely stores your financial account details, such as credit card number, on the company's machines in order to access this information conveniently when needed on the company's app. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores information that uniquely identifies your phone on the company's machines in order to verify your identity. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree

  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that securely stores your contact information (such as contact names) on the company's machines in order to authenticate your identity when using the app. Do you this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores your email address on the company's machines in order for the company to contact you in the case of any issue. Do you this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that stores your email address on the company's machines in order to set up or manage your account with the company that provides the app. Do you this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a productivity app that stores your email address on the company's machines in order to inform you of any updates to the company's app if needed by email. Do you agree this data storage in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Which of the following best describes the scenarios discussed on the previous page?
  - The company that made the app collects your data and stores your data on your phone
  - The company that made the app collects your data and stores your data on their machines
  - The company that made the app collects your data and shares your data with third parties
  - The company that made that app collects your data and sells it to third-party advertisers

In the following scenarios, assume that the company that made the app collects your data and shares your data with third parties.

- Imagine you are a college student and use an education app that securely sends your precise location (within 3 kilometers of where you are) to other companies in order to connect you with opportunities nearby on your college campus. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that securely sends your purchase history to other companies in order to prevent fraud. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that securely sends information that uniquely identifies your phone to other companies in order to prevent fraud. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that sends your email address to other companies in order to show you recommended content. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that sends your email address to other companies in order to send you delivery notifications. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Imagine you use a shopping app that sends your email address to other companies in order to set up or manage your account with the company that provides the app. Do you agree this data transfer in your best interest?
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Which of the following best describes the scenarios discussed on the previous page?
  - The company that made the app collects your data and stores your data on your phone
  - The company that made the app collects your data and stores your data on their machines
  - The company that made the app collects your data and shares your data with third parties
  - The company that made that app collects your data and sells it to third-party advertisers

Imagine a new privacy regulation is enacted where any party engaging in user data collection is obligated to act in the user's best interest. Acting in the user's best interest means putting the user's well-being first. This could look like avoiding opportunistic behavior, reducing abusive design practices, and prohibiting certain forms of data processing and collection, among other things.

- To what extent to you agree with the following statement: Enacting this privacy law would be a good idea.
  - Strongly agree
  - Agree
  - Neutral
  - Disagree
  - Strongly disagree
- Please explain why:

- How do you think companies' data practices would have to change to comply with this law?

- How much do you feel you understand what companies are doing with the data they collect about you?
  - A great deal
  - A lot
  - A moderate amount
  - A little
  - None at all
- How concerned are you, if at all, about how companies are using the data they collect about you?
  - Very concerned
  - Somewhat concerned
  - Not too concerned
  - Not at all concerned
- What is your current age?
  - 18-24
  - 25-34
  - 35-44
  - 45-59
  - 60-74
  - 75+
- What is your gender?
  - Man
  - Woman
  - Non-binary person
  - Prefer not to answer
  - Prefer to self-describe:
- Choose one or more races that you consider yourself to be:
  - White
  - Black or African American
  - Native American or Alaska Native
  - Asian
  - Pacific Islander or Native Hawaiian
  - Other:
- Do you consider yourself to be Hispanic/Latino/Latinx?
  - Yes
  - No