Spotlight Report #5: Me2B Alliance Validation Testing Report: Consumer Perception of Legal Policies in Digital Technology

Research Performed by Noreen Y. Whysel, Director of Validation Research, Me2B Alliance

Written by Noreen Y. Whysel, Director of Validation Research, Me2B Alliance

Contributors: Karina Alexanyan (editor), Shaun Spaulding, J.D., New Media Rights (literature review), Julia Little (graphics)

#PrivacyPolicy #TermsofService #TermsofUse

Table of Contents

1 Abstract

Our relationship with technology involves legal agreements that we either review or enter into when using a technology, namely privacy policies and terms of service or terms of use ("TOS/TOU"). We initiated this research to understand if providing a formal rating of the legal policies (privacy policies and TOS/TOUs) would be valuable to consumers (or "Me-s" in our parlance). From our early qualitative discussions, we noticed that people were unclear on whether these policies were legally binding contracts or not. Thus, a secondary objective emerged to quantitatively explore

whether people knew who these policies protected (if anyone), and if the policies were perceived to be contracts with the provider of the digital technology (or "B").

The purpose of a privacy policy is notification and disclosure, not protection. Privacy policies are not designed to protect anyone, they're designed to inform. The TOS/TOU, on the other hand, is an agreement relating to the use of the technology or service and is typically designed to protect the business. Do Me-s understand this?

We conducted ethnographic interviews with six participants living in the United States, during a two-week period from February to March 2021. We followed these interviews with a focus group session of five participants in July 2021 and an online survey of 566 individuals in August 2021. In these studies, we asked participants and survey respondents who they think the privacy policy and TOS/TOU protect and whether they perceived these policies to be enforceable contracts.

The following are the key findings from this research:

- **People don't understand that the Terms of Service is a contract**. 55% of survey participants did not understand that a TOS/TOU is a contract (based on only 45% saying it is one). This has significant legal implications. In particular, a key requirement for legally binding contracts is mutual assent, which means that both parties have a "meeting of the minds"[1] and understand they're entering into a contract. Our research makes clear that is not the case in Terms of Service agreements.[2]

- **Consumers are aware of the existence of legal policies on connected technologies**. Focus group participants said that they know that legal policies exist for connected technologies and that they should read them, but that they largely

ignore them in favor of getting to use the app or website as quickly as possible. The majority recognize cookie consent requests on websites and have some understanding that it relates to data privacy, but doesn't necessarily connect them to a privacy policy. They are aware of TOS/TOU agreements when signing up for a service but often will accept the terms without reading them thoroughly.

- **People have a weak understanding of what the legal policies of digital technologies are or whom they protect**. 66% of survey respondents say that privacy policies protect the business, while only 50% say they protect the consumer. The difference was starker for TOS/TOU, where 68% say they protect the business and only 35% say they protect the consumer. All interview participants say both documents are there largely to protect the digital technology company (the "B") and to enforce "rules" around what a consumer can and cannot do with the technology**.**

- **None of the interview participants were aware of the existence of tools they can use to evaluate legal policies**. They were aware of review sites that evaluate digital products from a consumer perspective, and some of the participants understood what a browser plugin was, and said they use them to block cookies, for example. They were not aware, specifically, of tools that help them understand privacy policies or TOU/TOS documents.

- **Half of the interview participants said that a score wouldn't change their behavior.** Even after we demonstrated rating tools such as TOS;DR and Privacy Badger, participants told us they did not expect to change their behavior, particularly if they were already using a particular digital service. Some said that seeing these ratings would potentially give them pause before using a new (to them) service.

As a result of this collection of research, the Me2B Alliance has decided **not** to pursue a formal legal policy audit service. Instead, we expect to evaluate and perhaps recommend existing services like Privacy Badger, TOS;DR, Mozilla's "Privacy Not Included" program and others.

We hope, however, that the findings in this research can help illuminate and eventually eliminate the pervasive asymmetry in Me2B relationships and be a concrete resource to lawyers supporting Me-s in legal cases relating to digital agreements. Please contact us at admin@me2ba.org if you'd like access to the quantitative data.

2 Introduction

The Me2B Alliance, a nonprofit organization, conducted a qualitative study of consumers' awareness and understanding of the legal policies of online businesses, services and products, namely the Privacy policy and Terms of Service/Terms of Use ("TOS/TOU") agreements. The study explored participants' understanding what these legal documents are, whose interests they protect and whether knowing if these policies are respectful or not would change their online behaviors. The objective was to understand if a legal policy rating would be of use to consumers when deciding whether to enter into a commitment with a technology provider—or even use technology.

2.1 Background

The Me2B Alliance ("Me2BA") is a nonprofit creating a safe and just digital world through standards development and independent technology testing. At the core of our work is our Respectful Technology Specification[3] currently in development,

which provides an objective standard for measuring safe and ethical technology behavior. The Specification consists of a series of tests that evaluate how a connected product or service is behaving towards the people that use it. This helps individuals understand how technology is treating them, and helps businesses build technology that is safe for and respectful to the people that use it.

In particular, the Respectful Tech Specification tests each Me2B Commitment,[4] including whether the notice of the agreement to each commitment is easy for technology users to find and access. Among other things, the set of tests for the each Commitment addresses whether or not the individual has the opportunity to provide permission prior to the sharing, or derivation, of personal and tracking data with a website or mobile app. Viable permission is a core attribute of respectful commitments.[5] Websites typically notify users by asking for permission (often through the browser); mobile apps often reference an individual's existing permission settings, activating a device pop up if permission is needed.

Who are these policies designed to protect?

Most legal policies are written by corporate lawyers, and are therefore designed to protect the corporations who paid for them. We as individual Me-s usually don't have lawyers who specialize in this area, and we aren't writing these kinds of policies for ourselves. And even if we did, we don't have the technological capability to send them to the business at the time of using a service or creating an account. Note, however, that IEEE P7012 "Machine Readable Personal Privacy Terms"[6] is developing a technical interoperability standard that will allow people to have software agents that can send legally binding privacy agreements to the provider (or B)—kind of like a reverse terms of service from the user, asserting specifically what permissions are granted to the business.

Privacy policies are notices provided to users of technology. The practice of privacy policies can be linked to Fair Information Practices Principles (FIPPS) such as these from the FTC (https://en.wikipedia.org/wiki/FTC_fair_information_practice) which expressly includes the practice of notice/notification. The purpose of a privacy policy is notification and disclosure, not protection. Privacy policies are not designed to protect anyone, they're designed to inform.

The TOS/TOU, on the other hand, is an agreement relating to the use of the technology or service and is typically designed to protect the business.

2.2 Literature Review

For a person to have agency in entering into an agreement with a technology product or service, they must be able to find, access and understand these agreements and the policies that explain them. We did a literature review of consumer perceptions of legal policies and evaluated tools like the Privacy Badger[7] and ToS;DR[8] browser extensions to understand if scoring these policies would make any difference in consumer behavior.

In a review of existing research, we found no studies that directly answer whether or not people will change their web activity knowing that legal terms are unfavorable to them. Most studies investigate what extent people will attempt to access a website's legal terms or that people don't read these policies to begin with.[9] Some studies evaluate whether people understand what they have consented to by agreeing to a website's legal terms. However, some reasonable inferences can be drawn based on certain surveys and reports.

The closest study that might shed light on this question is a study conducted by Lior Strahilevitz and Matthew B. Kugler in which they look into the relevancy of reading

privacy policies and what people take away from reading such privacy policies.[10] This study concluded that when people are exposed to varying degrees of specificity and clarity of a website's privacy policy, there was no significant effect on consumers' judgment about what they authorized the website to do. Similarly, exposure to a website's privacy policy did not lead to any significant effects on the individual's perception of the website's intrusiveness. Strahilevitz and Kugler point to the rational thinking of people doing a cost-benefit analysis where privacy sacrifices inherent in their use of certain websites outweigh the costs. One inference that can be made is even if people read a website's privacy policy, they might not have the appropriate knowledge to determine whether the website's data practices are reasonable. Taking this inference one step further, unless a website explicitly says it engages in poor data practices that do not even remotely take into consideration the privacy of the user, people will unlikely know the difference between privacy friendly terms and non-privacy friendly terms.

A Cisco report from 2019 sheds light on people increasingly becoming more aware of their privacy.[11] According to Cisco's report, 32% of all survey respondents across several different countries care about data privacy, are willing to act, and have already taken action to protect their privacy. The most telling result is 87% of responding businesses experienced sales delays to existing or prospective customers caused by their customers' privacy concerns. The report attributes this privacy mindset likely to customers making sure their vendors and business partners have adequate answers to their privacy concerns before doing business together. However, these appear to be business-to-business transactions where customers have stronger negotiating power to encourage their vendors to adopt better data practices, which is quite different from the dynamics involved between an average Internet user and a website/business.

We can conclude from this review that, although privacy is becoming an increasing concern for people, there is little visibility into how or if people are modifying their behaviors when faced with knowledge of a website's poor data practices.

3 Research Design

3.1 Study Objectives

The objective of this study was to conduct qualitative research to understand whether people change their behavior when they understand the legal policies governing their interactions with digital technologies. This was a mixed method (qualitative and quantitative) study, utilizing one-on-one interviews and an online survey. Open-ended interviews were conducted with six adult participants to examine their awareness, understanding and use of the legal policies that govern their interaction with Internet-enabled businesses they interact with on a regular basis, namely privacy policies and TOS/TOU. The online survey was a simple, 3-question survey clarifying online technology consumers' understanding of the impact of these policies on them and the business.

3.2 Research Questions

Three primary research questions guided the development of the research methods:

Part One – Qualitative Study:

1. Do people change how they interact with a website when they are familiar with the legal terms (Privacy policy and/or TOS/TOU) of the website.
2. Does a score grading the Privacy policy and TOS/TOU have value to Me-s (consumers).

Part Two — Quantitative Study:

1. Do people know whether these documents are contracts, whether they are enforceable and who these policies protect?

3.3 Participants

For the survey, We created a survey on Surveymonkey and ran it on August 5, 2021. 566 people responded, all in the United States. While we did not select for gender balance, 297 female (52.5%) and 269 male (47.5%) respondents completed the survey.

Age ranges included 21.9% aged 18-29, 24.6% aged 30-44, 37.3% aged 45-60 and 16.3% over age 60.

Table 1: Age of Participants

Age	Percent of Total Participants
under 18	0.0%
18-29	37.6%
30-44	43.2%
45-60	12.0%
over 60	7.2%

The majority of respondents, 60.6% were iOS Phone / Tablet users. 34.1% used Android Phone / Tablet, 3.5% were Windows Desktop / Laptopusers and 1.4% were MacOS Desktop / Laptop users. Windows Desktop / Laptop users and 0.3% were MacOS Desktop / Laptop users.

Table 2: Participant Devices

Device	Percent of Total Participants
iOS Phone / Tablet	55.7%
Android Phone / Tablet	40.9%
Other Phone / Tablet	0.0%
Windows Desktop / Laptop	1.2%
MacOS Desktop / Laptop	1.2%
Other	0.9%

Most respondents or 61.8% earned between $25,000-$124,999. 14.4% earned less than $25,000 and 14.8% earned $150,000 or more more than $100,000 and 8.8% preferred not to answer the income question.

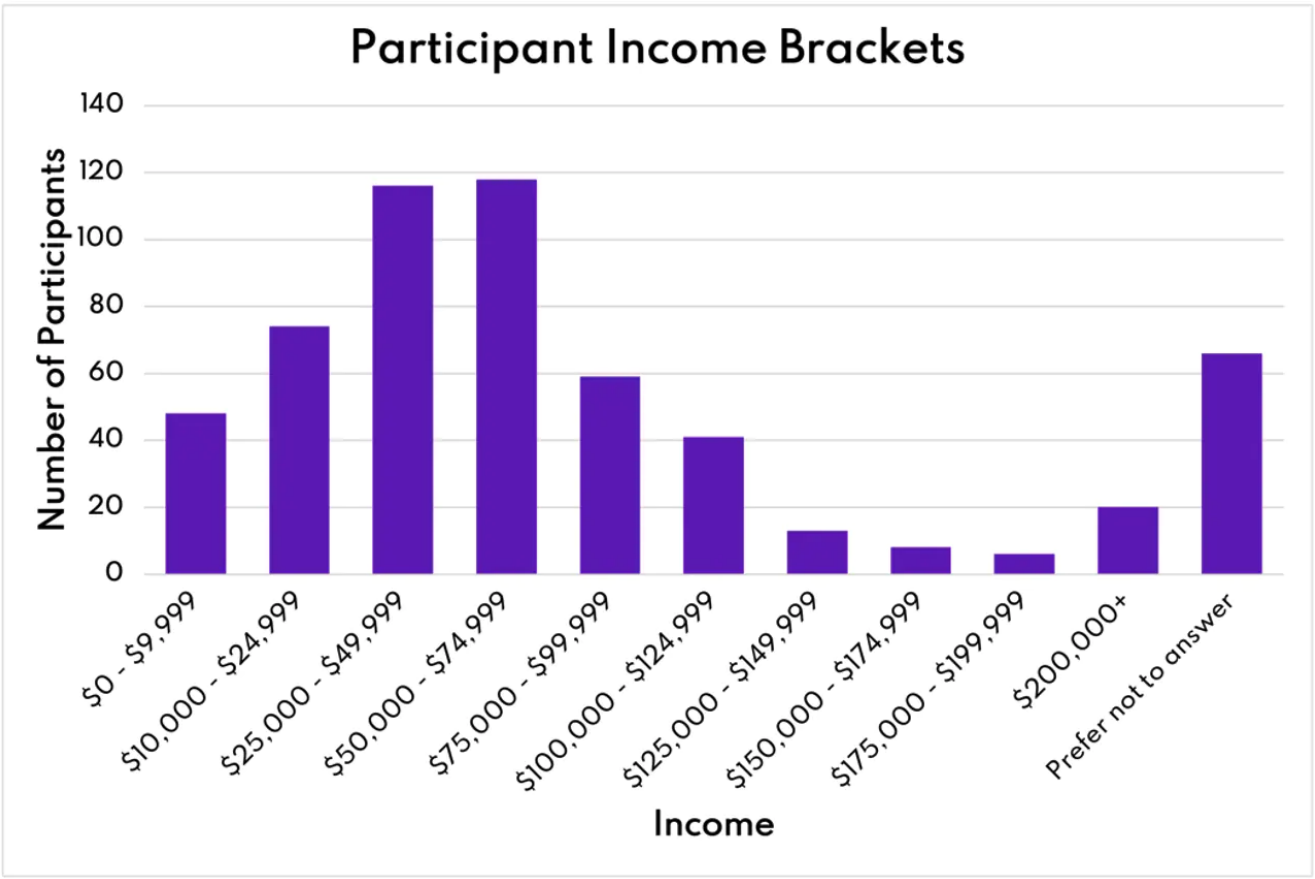


Figure 1: Income Brackets of Survey Participants

Six interview participants from various areas of the United States were selected for

interviews, five women and one man ranging in age from late twenties to mid-fifties. Two of the participants interviewed were African American, one was Latinx and three, including the male participant, were White.

The Participant Snapshots in Appendix A give a sense of each participant's technology use in terms of quantity of products used, the way the products were used, how the participants felt about their technology use, as well as their general comfort level with technology.

Participant recruitment was conducted using an online platform, UserInterviews.com, for the interviews and Surveymonkey.com for the online survey. The UserInterviews platform allows for the creation of a screening survey to find eligible participants. Participants were sought who had a home broadband connection, who regularly used at least two Internet-enabled devices, who did not work in the technology or legal sectors, and who did not live in a large urban center. See Appendix B for the complete screening survey.

Interview participants who qualified after completing the screening survey were then hand-selected by the researcher for participation. The researcher invited participants to maximize diversity of the interviewees along the dimensions of age, ethnic/racial background, and geographical location. Unfortunately, few males responded to the call in the short time that recruiting took place, so there is a gender imbalance, skewing female, with this study.

3.4 Informed Consent

Each participant (interviewee) gave verbal consent to participate in this study. Prior to the start of the interview, Noreen Whysel, the interviewer, emailed a copy of the Me2B Alliance consent form. Then at the time of the interview,

via videoconferencing, she showed the participant a written consent form (see Appendix C).

Participant indicated verbally that they had read the entire consent form, then the interviewer asked if they had any questions and if they agreed to participate in the study. If the interviewee consented, the audio-recording was initiated, and the interviewee was asked to state his or her name and to state, “I agree to participate in this study.”

These audio recordings of participants’ verbal consent were saved as separate audio files and are retained by study personnel. We offered to email a PDF of the conenst form following the survey to all participants.

4 Methods

4.1 Qualitative Research – Interviews and Sentiment Analysis

We conducted the interviews via videoconferencing using Zoom software. Noreen Whysel conducted the interviews. Two additional Me2B volunteers, Lisa LeVasseur and Jeff Orgel, observed an interview on two separate occasions and asked questions of participants at the end of the formal series of questions. Interviews were audio-recorded using Zoom. Each interview lasted approximately 60 minutes.

The purpose of open-ended interviewing was to understand participants’ awareness, understanding and use of legal policies such as privacy policies and TOS/TOU. The Interview Guide (see Appendix D) was used to direct the conversation, though open-ended questions were not necessarily asked verbatim or in the order they appear in the guide. The interviewer(s) also improvised questions

as necessary in order to follow up with topics introduced by the participants.

4.2 Quantitative Research – Online Survey

The survey had two questions, each listing five statements about these online technologies with checkboxes and one open-ended comment box asking participants to explain why they chose the options they did. The respondents selected the statements they agreed with and filled in the open ended comment field to expand on their selections. We also performed a cluster analysis on the open ended responses.

5 Data Analysis

Audio recordings of the interviews were transcribed verbatim. In addition, the interviewer took extensive notes during each interview. The interview responses and recorded conversations are unstructured data comprised of factual statements, as well as opinions and other statements of sentiment or comparison. Indications of positive, neutral and negative sentiment orientation were noted as well as the degree of confidence of the answers by analyzing response time (subjectively), statements such as “I think”, “I’m not sure”, “I don’t know”, etc. and incidents of wavering assertion.

Survey data from the SurveyMonkey projects were downloaded to a Microsoft Excel spreadsheet and analyzed to determine if there were any significant patterns around legal policy awareness and understanding. We further analyzed this data by gender, age, income bracket and U.S. region.

In addition, we used Carrot2 Clustering Workbench (https://search.carrot2.org/#/workbench) using the LINGO algorithm to examine

open-ended comments from the survey responses. The Lingo algorithm creates well-described flat clusters and is available as part of the open source Carrot2 framework. Clustering Workbench processed text content from local files that was uploaded In Excel format.

6 Findings

6.1 Interview Findings

As noted in Section 4 Method, we invited six participants to discuss their awareness and understanding of legal documents including privacy policies and TOS/TOU agreements, We then asked survey participants to select statements from a randomized list to describe the privacy policies and TOS/TOU documents for websites and mobile apps and related evaluation tools.

Participants differed only very slightly in their concern for online privacy or other online treatment. Most were generally accepting of most policy clauses or had one or two they would look for before accepting them. When it came to financial or personal identity information, two described taking extra steps to secure their credit card or other information online, one going as far as to say they might delete their account and open a new one if they were concerned it may have been compromised. Participant 3, who seemed to be the most comfortable with technology among the study particpants, was also the most cynical about how technologies treat consumers and whether legal policies make a difference.

Below are our detailed findings.

6.1.1 General Questions About Technology Use

General questions were introduced to assess the types of digital technologies each participant used on a regular basis and their level of comfort in discussing their online activity.

6.1.1.1 Interviewer: “How many digital technologies do you use on a regular basis?”

We asked participants to guess how many online accounts they had. Most could not guess a specific number. One said ten to fifteen accounts, but the rest either couldn’t guess, said, ”a lot”, “too many” or thought it could be at least 50 or even a hundred or more.

We introduced a few categories of accounts including email accounts, retail and banking sites, insurance, social media and other publishers, cloud storage, and streaming services and asked participants to list out products and companies in each category. We provided categories both to elicit categories of technologies they had not thought of but also to elicit specific websites and apps to discuss later in the interview. Most discussed online accounts that are primarily for personal use, but some also mentioned software accounts and email they use for work.

Email (Gmail, Outlook, Yahoo!, AOL, etc): Participants have at least one personal email account and one work account. Only one specifically mentioned one personal and one work account, but through later discussions we confirmed that most of the participants also have work accounts.

Social Media (Facebook, Twitter, Instagram, Pinterest, TikTok, etc): Facebook, Twitter and Instagram were the most noted social media accounts. One said they only used Instagram. One said that they use Twitter occasionally but was on Reddit the most. Two have Pinterest accounts. One manages social media for their employer.

Financial Services (bank, investment account, etc.): Four indicated that they have online accounts at a bank or credit card company. Two did not report a financial services account. Insurance Company (medical, dental, auto, home, etc) Four indicated that they have online insurance accounts. Two did not report having an online insurance account.

Cloud storage (iCloud, Dropbox, OneDrive, Google Drive, etc): Five reported that they have cloud storage accounts such as Dropbox, Google Drive, OneDrive, or iCloud or that they had files on their carrier account (Verizon) or associated with their device (Samsung Cloud). The Dropbox user noted that they use it for work.

Conferencing (Zoom, Webex, GotoMeeting, MS Teams, etc): Three discussed conferencing system accounts, mentioning Zoom, Google Meet, Adobe Connect, Group.Me, Slack and Rodeo. While all were accessing Zoom for the interview, one participant does not have a Zoom account and one indicated that they use "whatever everyone is using" and said they don't really notice anymore.

Retail Store (Amazon, Walmart, Target, Walgreens, Nike, etc): All mentioned Amazon, which is not surprising since the testing service, UserInterviews.com pays participants in Amazon credits. Retail sites mentioned include Amazon, Target, Instacart (for grocery delivery from Aldi and Shoprite), Walmart, CVS, Etsy, Lululemon, Poshmark, eBay, Stitchfix, Nine West, Rockbox, Wayfair, Nordstrom, Hay Needle and Michaels. Amazon Prime and Amazon Fresh were also mentioned. "It's surprising how few times I've walked into a store [since 2020]"

Streaming Service (Netflix, Hulu, Spotify, Pandora, etc): Four participants noted they hold accounts with online streaming services, three of whom noted specific video services, including Netflix, Hulu, HBOMax, Disney, and Kanopy, which streams video content to users with a public library card. One participant uses Sirius and Pandora

music streaming services did not mention any video services or subscriptions. Two participants did not mention streaming services.

Publications (newspaper, magazine, etc.): Three participants said that they had an account with news or magazine publishers. Services noted include the Pittsburgh Post Gazette's online newspaper, Associated Press and Amazon News and comic book accounts. One said they did not subscribe to online news, and generally does not pay for news. This participant used to get news related magazines and books if they had a promotional code (e.g., frequent flier miles). The comic book subscriber does not have a paid news account.

> "[N]ormally, I don't don't sign up for anything news related if I have to pay for it."

Online Work Accounts: Five participants indicated that they had email or other online and software accounts for work.

Other Accounts: No responses for "Other"

After discussing account categories, we asked again to estimate how many online accounts they had. Three said they had 51-100 accounts, one said 101-500 and one said they had less than 20. One did not answer. People seem to know that they have a lot of accounts and listing accounts by category allowed them to think about their online accounts in more concrete numbers. Participant 1, an apparel business owner from Washington, DC, identfied less than 15 accounts. We asked this participant to list the accounts and they were able to name thirteen, including two work emails. They said that they normally don't create accounts and will use "guest checkout" on most retail sites. Five of the six participants perceive that they hold a lot of accounts that are saved on company websites or apps.

6.1.1.2 Interviewer: "If you had to guess, about how many digital accounts do

you have in total, including the ones you use regularly and those you use infrequently?"

Most of the participants say that they have more than 50 online accounts. One thought it was likley more than 100. One only has about 10-15 accounts and named 13, confident that that is all they had.

6.1.2 Understanding of Legal Policies

None of the participants were in the habit of reading legal policies on websites or apps, considering them to be too long, legalese or a chore sitting in the way of using the app. One participant, Participant 2, a graphic designer from Kansas City, reads the policies when the technology is for work, but not always when it is for personal use. Generally, the participants consider these policies to be "rules" governing how a company can use their data and how they may use the product.

There was some confusion among one of the participants, Participant 1, about exactly how Privacy policy and a Terms of Use or Service document differ, but this participant ultimately agreed with the others that the Privacy policy governs the technology's use and sharing of personal data and that the TOS/TOU governed the users' behavior. They were in fact very curious about how the privacy policy covers third-party sharing. Participant 2 and Participant 6 were most interested in information about pricing and fees, while Participant 3 was most interested in Android permission settings. One participant said, cynically that the Privacy policy is there so the company can't be sued for not having a privacy policy, alluding to privacy laws like California and GDPR.

Participants were unlikely to cancel an account if there was bad news in the press about a technology they use. In the case of a data breach, they felt the damage was already done (a concept that came up frequently in the interivews). They said they might be safer afterwards given a new focus on security. One participant said they

might close their account if the news was particularly bad, but then possibly open a new one with a different email if the product or service was unique or hard to duplicate elsewhere. On the other hand, good news about a company or product was not necessarily a draw, as one said, it could be a PR ploy.

6.1.2.1 Interviewer: "Do you read the privacy policies or terms of service for online, digital products or services?"

Four of the six participants said they don't read legal policies. One didn't answer. Participant 2 occasionally reviews legal policies for work accounts. When reviewing these policies, this participant said, "When I sign up, I definitely want to know what the company had access to."

> "They are long and legalese and...set up where you have to say you agree, because you can't go to the next step to get your grilled cheese sandwich."

> "Do I feel safe?... I do reviews of a company that I'm signing up for...outside of the website to make sure it's not a scam."

6.1.2.2 Interviewer: "Can you explain the difference is between these documents?"

Privacy policy: Five of the participants defined a Privacy policy as the document stating what user data the technology will save or share. One participant said that a privacy policy is the company's "actual policy for using their site," conflating it with the Terms of Use. This participant continued to assume the privacy policy governed the consumer's use of the product or service rather than how the company will use their data.

TOS/TOU: All but one participant noted that the TOS/TOU (and in one case the EULA) relates to the rules for using the product or service. In all these responses, the participants were clear that an asymmetry between the Me and the B exists: the

company makes the rules, and the user must follow them. One described it as a contract saying that the company has the right to drop you as a user at any time. One participant said that a TOS is associated with payment and includes terms such as 12/months of use "for the term of the account," as well as policies covering free trials and cancelation. Participant 3 was particularly negative, saying that EULA's are "documents you have to stroll to the end to use the product"

On TOS/TOU: "If you violate the terms..incite violent revolution...we can ban you."

On EULAs: "...companies have just thrown random clauses ... to see if anybody challenges them."

6.1.2.3 Interviewer: "Off the top of your head, what are some things you think you might find in a ... "

Privacy policy: Two participants said they would expect to find information about what you can and cannot do on the site and what the site does or does not do. One participant mentioned cookies and said that the privacy policy would indicate if they use third-parties cookies or share data with third parties.

TOS/TOU: Only two participants answered specifically for TOS/TOU. Participant 1 expected to find return/exchange policies and other information about how the vendor conducts business. Participant 4, a university coordinator from Philadelphia, expected to find contact information in the TOS/TOU. In addition to contact information, Participant 2 would expect to find a way to report something that violates the agreement. Participant 5 described entering a radio contest, and noticing that they had a number of "consent to share" checkboxes that were already checked. This participant had to manually uncheck the boxes, but appreciated that it was an option. In a previous contest, this participant ended up having to unsubscribe from a lot of stuff.

"I'd rather not have my info shared if not required, if I had a choice."

"[I] just entered a local radio station contest.... It has all {of the] 'consent to share' [buttons] checked and I had to uncheck all of them. I'm glad they gave me that option. [Another company did that] with another contest and I ended up having to unsubscribe from a lot of stuff."

6.1.2.4 Interviewer: "Are there any specific paragraphs in a privacy policy or terms of service that you tend to look for or read?"

We asked if there are any specific paragraphs that the participant tends to look for and read in a privacy policy or TOU/TOS. Participant 1 is curious about third party sites and whether data is stored by third parties. Participant 2 and Participant 6 look for pricing information. Participant 6 called it the "money aspect." Participant 2 also looks for copyright information since it is a concern at their work. Participant 5 doesn't really read the legal documents, noting that they are more confusing to read than the paper contract you get for car insurance, saying "It's easier to read [the paper document]. It's like bullet points."

Privacy policy: Participant 4 looks for information about protecting credit card information and that they aren't sharing or selling their email. Participant 3 relies on the app level permissions breakdown that Android provides, because it is less difficult to process than the legal forms. This suggests that this participant might be inclined to seek out trusted sources to provide guidance on privacy protections.

"No one has time to read that much drivel, legalese."

TOS/TOU: No Comments

6.1.2.5 Interviewer: "Have you ever tried researching information about a company's terms of use and privacy policy? Did you find what you need?"

Participant 6 and Participant 1 discussed their experiences with retail websites. Participant 6 had an unfortunate incident with a company that offered to send a free blender but reneged on the offer. They looked up the company information after they had been "wronged." Participant 1 had an account at AliBaba but "does read policies on Chinese websites" and will create an account if the merchandise is good. This participant said some sites will allow guest checkout and will use that if they won't be making future purchases there.

6.1.2.6 Interviewer: "Let's say one of your services was featured in the news. Would reading news about a company that shows they care about privacy make you feel more secure using them?"

Participants were mixed on this question. While two said it would make a positive impression if the news were good, two said a definitive no, and one hesitant no. Participant 2 said it depends on where the report appeared, citing news media bias. This participant would look at other sources, before changing their behavior. Participant 6, who was hesitant admitted that this kind of news "goes in one ear and out the other." Participant 5 discussed the hacking of Target as an example of bad news about a company. Participant 3 was the most cynical, stating that companies have PR agencies to manipulate the news, and mentioned confirmation bias and zero day exploits. They concluded that "you have to accept that nothing is perfect."

> "Not to be a conspiracy theory, crazy-hat [person], but...paid advertising can say anything."

6.1.2.7 Interviewer: "Would reading negative news make you want to stop using it?"

The general feeling was that if there was negative news it would really depend on the source and whether it was a serious breach of data security. Then, they would

consider closing their account. While Participant 4 might remove credit card info and keep using the site, Participant 5 was fatalistic. In that case, "the damage was already done" and "[the business] would probably be more secure afterward." Participant 3 said if it were "hysterical headlines in your news feed" they would ignore it, but if there was a technical document describing the issue, they might cancel the account.

Only Participant 5 would probably cancel their account and could describe situations where they did act on it. Participant 2 said that if it was a breach, they might cancel an existing account and open a new one.

> "There are some things you can only get on Etsy."

Three participants expressed negative sentiment about privacy policies terms. Participant 5 and Participant 6 suggested that the terms can be misleading. Participant 6 said the terms for canceling their daughter's Kindle Fire were vague and that the fine print put around the free trial was misleading. Participant 5 said that Geico asks for seemingly irrelevant information on its insurance quote form. Participant 5 went as far as to say that you have no choice if you want to use the service, which was a common response. Participant 3 complained that a music app wanted 24/7 access to the camera and microphone, even though they do not use voice activation. They thought it was "weird" that larger, well-known apps would do that. Participant 1 answered this question, not about legal policies, but about FAQs on a site that they described as "sketchy."

> "I googled something, I think for some type of DSLR. I went on one of these sketchy [Google links]. Clicked on it and read the FAQ, researched reviews on the company. In the reviews I found not only is it a third-party site, it's not a real company."

"When you install a music app and it wanted access to camera or 24/7 microphone and I don't plan to use voice activation. It would be weird on larger well-known apps."

Two participants said no, reading news about a company would not necessarily make them stop using it, or that they could not think of any services that whose privacy policy made them decide not to use it.

6.1.2.8 Interviewer: "Have you ever received a notification about an update to a privacy policy (or TOS) that made you consider changing the service? Did you delete your account?"

Four participants said they have received policy update notices.

6.1.3 Awareness of Legal Policy Protections

Participants were asked to describe in their own words what a privacy policy and TOS/TOU are for. Five responded. There was general agreement that both documents protect the B more than the user. Most said that these policies are primarily to inform the Me and protect the B. The general sense is that they are rules the user must abide by.

6.1.3.1 Interviewer: "What do you think the privacy policy is for?"

Two participants were negative about both documents. Participant 3 called a privacy policy "legal cover" for the company. These responses may indicate a sense of a power imbalance.

"I have no choice but to agree."

"It doesn't protect me. I can't select the parts I agree with."

6.1.3.2 Interviewer: "What do you think the TOS/TOU is for?"

Participant 2 said the TOS/TOU were "for" the user in the sense that agreeing to the

terms gets you access. What rights do you have? Are they protecting your rights/giving you rights/protecting you? Two participants suggested that they are protected by privacy policies if it allows them to change their settings.

"I feel protected if I can change/edit settings."

"You agree to these policies or you have the right to not use the platform."

6.1.3.3 Interviewer: "Do legal policies protect you as the consumer? How?"

Four participants gave a qualified Yes to this answer. Participant 1 said they do protect the consumer but "it's on me to read them and absorb them and figure it out." Participant 5 said they protect consumers "maybe a little bit." This participant also had doubts, saying, "They all do share your information." Participant 3 was the most negative and did not think people really had a chance against companies like Google, even if their policies are clear.

Participant 2 was much more willing to accept that the companies are collecting data to make the experience better for users, saying that the act of accepting these policies is "kind of an intimate experience." They appreciate when their personal and financial information are protected.

Participant 3 on whether privacy policies protect them (as a Me):

"Ostensibly, yes. In reality, good luck."

"Do you have the time and money and army of lawyers to go against Google?"

Privacy policy: Participant 1's answer to this question clarifies some earlier confusion about what these policies cover. This participant explained, erroneously, that a privacy policy outlines what you can and cannot do on the site and TOS/TOU

was how to use the site. After hearing how the Me2B Alliance defines these documents in the next section, Participant 1 said it was clearer.

TOS/TOU: None of the comments to this question were specifically about the TOS/TOU.

6.1.3.4 Interviewer: "Do legal policies protect the organization? How?"

Privacy policy: All participants answered this question in the affirmative. Companies are protected by the privacy policy. Participant 2 mentioned GDPR (though didn't recall the name of the regulation) as the reason we are seeing cookie notices. This participant said that their understanding is a company can get sued if they don't have a privacy policy. Participant 3 called it "legal cover for what they track and sell," saying that while it does allow a better experience it "allows them to sell and monetize whatever they want." Participant 1 continued to suggest that a privacy policy allows a company to sue a user who uses the content without permission.

TOS/TOU: Three participants said that the organization is protected by the TOS/TOU because they can ban or delete an account of a user who isn't following the rules. This protects the integrity of the service and builds the trust of the user population. Participant 1 was unclear if the TOS/TOU protects the company, since their understanding was that the terms document was more "how to" than rules. They made more sense later when we defined the documents.

Participant 3 felt that the TOS/TOU protects the company in extreme cases where a bad actor can be banned. They described services where users are banned for promoting violence or hate speech. They said that sometimes these companies may be accused of censorship but that terms may be written so that they can remove a user for any reason, which further protects the company from lawsuits.

Participant 6 was also negative, mentioning a situation where a company may force you into paying for a service and make it difficult to get out of the agreement, including terms that are written such that, "you have to keep paying them" and cannot tell your bank to stop payment. This is described as Forced Continuity in Harry Brignull's website DarkPatterns.org. "If someone is using the platform for malicious activities and making the org or platform look bad, they should have the right to delete their account if that person is doing bad things."

6.1.3.5 Interviewer: "Have you seen cookie notices?"

Five participants answered this question. They all have seen cookie notices.

> "I do see them. When they pop up, it says 'Accept all cookies.'"

6.1.3.6 Interviewer: "Do you know what they are?"

Participant 2 found them particularly irritating, saying that, "It would be better if all of them were by default. I wouldn't have to do more work."

6.1.3.7 Interviewer: "Are these [cookie notices] legally binding?"

Responses to whether these policies are legally binding were mixed. Four participants were unsure and of the two participants who answered confidently, one said yes, and the other said No. Participant 1 says that if you click OK to consent to a policy it is now binding.

Participant 3 did not think they could be prosecuted.

> "I haven't read a court case...where a cookie was used as evidence."

6.1.3.8 Interviewer: "Are they related to the privacy policy?"

Five participants said that cookies are related to the privacy policy and were confident in their response. The sixth, Participant 5, said that they are probably not

related to the privacy policy “because they are stored on my computer, not at Amazon.” Participant 6 seemed to abstract the privacy policy and the cookies from each other saying that the policy is related to “something I signed up for” while cookies are a “generalization”.

6.1.4 Understandability of Me2BA Definitions for Privacy policy and Terms of Service/Use

The interviewer read the following working definitions of Privacy policy and Terms of Service/Tems of Use to get the participants reactions.

Privacy policy: Public promise of how the technology and the company will treat you and your data. Enforceable by the FTC in the US.[12]

Terms of Service/Terms of Use: The two-party contract that you are signing that both parties will abide by. Enforceable by the court of law.

6.1.4.1 Interviewer: Does this change your understanding of either of these documents at all?

Privacy policy: Four participants reacted positively to the Privacy policy definition. They found it simple, understandable, but Participant 3, who was favorable of the definition and Participant 5 who was unfavorable both wondered if it would be enforceable. Participant 5 said that “If I start getting emails from a company I never did business with, I won’t know who they got [my data] from” and wouldn’t know if it is possible to sue. Participant 2 and Participant 6 found the definition protective of the consumer. Participant 2 called it a “promise”.

TOS/TOU: Four participants reacted to the Me2BA definition for TOS/TOU, three negatively. The concern was that the Me2BA definition was idealistic on one hand and scary on the other. Participant 3 and Participant 6 found the idea of a binding agreement frightening. Participant 3 called it a “hostage situation” and thought it

would be difficult for a new service to open their customer relationship with such an agreement. They also said that TOSs and EULAs have been challenged in court and "have been found to be unenforceable in Europe". At best, they said they are "idealistic."

On enforceability, Participant 5 didn't think the company would ever enforce the TOS/TOU and that it would be difficult to prove it was violated.

6.1.4.2 Interviewer: Does any of this change your understanding of these policies?

Five participants responded. Two said that it did not change their understanding. Participant 1 was not aware of the limited enforceability of the policies and assumed that both were enforceable agreements. Participant 2 said that the Me2BA definition of the TOS/TOU made it seem two-sided, but felt it was one-sided from the consumer's point of view, ie. covering actions by the consumer that could affect their ability to use a product. Participant 3 objected to the Me2BA definition stating that there are "no two parties".

6.1.5 Importance of Reading Legal Policies

6.1.5.1 Interviewer: "Do you think it is important to read legal policies before signing up for an account?"

Five participants think it is important to read legal policies before signing up for an account. Participant 1 said it is important "but not mandatory" and Participant 2 said it is important but "I know a lot of people don't look through it because it is very lengthy." Participant 5 called them "legalese" and "vague" and felt it would be better if it were written in a "common language".

Participant 3 bluntly stated that you don't have to read the policy, "If you have to use the platform, if it's mandatory," or "if you want to do modern banking." Their

nearest Bank of America ATM is 15 miles away, so they would have to use the website or app to manage their account.

"You don't want to live in a food desert. I live in a Bank of America desert."

6.1.5.2 Interviewer: "Why? Or Why not? Could they be important to you?"

Participant 6 noted that popular culture provides examples of why it is important to read legal policies. They described an episode of South Park where one of the kids "...didn't read it and ended up in a kind of hell." Some examples of why it is important to read legal policies are,

"If you abuse how you use Amazon and vice versa, you can go to court."

"If something goes wrong, you want to be protected."

"So that I know what I'm getting into, what I'm going to be charged, and if they are going to sell my data."

Participant 6 offered examples of why people don't read legal policies: instant gratification, living in a consumer society, and being in a hurry.

6.1.6 Awareness of Privacy/TOU Management Tools

6.1.6.1 Interviewer: "Did you know there are plugins that read privacy policies? If so, do you use them? Which ones?"

Five participants have heard of browser plugins, generally as tools that improve your internet experience or as Participant 1 said "make it better to do anything in regard to the internet or a specific [site or task], but none had heard of plugins that specifically address the content of legal policies.

"Couldn't you just block cookies on your browser?"

6.1.6.2 Interviewer: "If you are aware of plugins and don't use them, why don't you use them?"

We offered to do a walkthrough for each participant of ToS;DR ("Terms of Service; Didn't Read" is a play on "TL;DR: Too Long Didn't Read" in internet parlance) to see if it would be possible to filter for people who use privacy browser extensions and plugins. All participants agreed to view these services. We were hoping to create a control group of people who don't use legal policy extensions, but while Participant 3 uses script blockers and other chrome extensions, neither they nor any other participants had heard of browser-based privacy or other legal policy tools. It could be interesting to do a larger survey of people who use these extensions and those who do not.

All participants were curious about browser extensions that address legal policies and agreed to do walkthroughs of TOS;DR and Privacy Badger. Participant 1's reaction was the strongest: "That is amazing!" Yet, they weren't sure it would stop them from shopping on a site. Participant 4 wouldn't necessarily stop using the service (mentioning YouTube) but that "it might make me more careful."

Participant 2 would want to look at other rating sites. Their concern is who is doing the reports since some can be biased. "Knowledge is power," and knowing what you are getting into yourself into is important but was doubtful to this participant that it would make a difference overall.

> "I would wonder if the trackers it is blocking disrupts my experience on the website. If it doesn't, I would definitely use the plug-in. I'd disable it one time and then renew it later. "

Of the six participants, Participant 2, the graphic designer, was the most curious about the interface on TOS;DR and Privacy Badger. The color coding made sense for

TOS;DR, but the Privacy Badger stop icon and cookie icon were hard to distinguish.

> "Red means bad. Green means 'I want.' If I have these [cookies] blocked, I only see red: It looks bad."

6.1.6.3 Interviewer: "Are you comfortable using a site that uses trackers?"

Participant 1 doesn't like trackers. They see ads following them around various sites and called it disturbing. "It can freak you out a little bit. I don't like it, but I don't stop using them."

6.1.7 Scoring Legal Policies

In lieu of asking about independent scoring, such as the ratings provided by the Electronic Frontier Foundation's Privacy Badger or Consumer Reports, we asked participants if knowing that a policy is good or bad would change behavior and if so whose opinion would you trust to make that decision. The interviewer allowed questions and responses to arise organically and where relevant suggested discussing concepts such as independent agency, rating service, friends, certification, etc.

From prior responses it seems like it would be very unlikely if users would change their behavior if presented with these scores. Some already have a personal policy of not signing onto a service at first and mentioned behavior like blocking trackers on unfamiliar sites and unblocking trackers as they gained comfort. The scores are seen as "nice to know" and useful in combination with other rating services like consumer ratings or other reviews.

Participant 5 answered this question directly and would trust a rating service, but wouldn't stop using the service even if the score was bad. They noted that "Amazon got an E [TOS;DR's lowest rating] and I'm still going to use it." They said they would

only change their behavior if the government enforced a minimum score.

> "I don't think it [a score] would influence my behavior. It would be nice to know."

6.1.7.1 Interviewer: "Do you ever talk to people about these policies?"

Five participants said that they don't talk to people about legal policies. Participant 1 said it is not a natural conversation. Participant 6 said they probably should have that conversation with their spouse. Participant 2 would talk about it at work because it was something they had to include on their own website, and said they might talk to people about the plugins we demonstrated. Participant 3 is usually the person that people go to to ask about these kind of things, but their former supervisor was "more into this than I am."

6.1.7.2 Interviewer: "If you knew that a policy was good or bad, would it affect your decision to use the digital technology?"

Three participants said that knowing there was a legal rating would change their behavior and three said it would not. Participant 4 said it would make them more aware when using a site and already uses service without logging in if login isn't necesary. Participant 1 said it would probably be more useful to have a rating for a site they never used before. While Participant 6 said that there are certain things [sites] they wouldn't give up and that having something like a rating would be "super beneficial." Participant 4 and Participant 2 mentioned practical changes like not having a credit card saved to the account or changing privacy settings. Participant 5 was the most negative. They've already bought things from Amazon for years, which means the damage and privacy violations are already done.

> "Having a list like this would be helpful. I can think of scenarios where it would stop me from using the site or give me the the go ahead and go."

6.1.7.3 Interviewer: "Whose opinion about whether a policy is good or bad

would you trust?”

Participants indicated that they would trust an independent rating, particularly if it was objective and had no ulterior motive, such as a not-for-profit organization. Participant 4 mentioned Better Business Bureau and Consumer Reports, followed by their own family. Participant 6 trusts restaurant scores, indicating that they would be open to government involvement. Participant 5 from previous questions seemed to want to look to government regulation to solve the problem rather than trust a score.

> “I would trust TOS;DR or Privacy Badger more than a friend. That’s their job, what they are actually built to do.”

6.2 Survey Findings

6.2.1 June 2021 Study

We conducted an online survey in June 2021 asking the following questions:

1. Which of the following are true about a privacy policy on a website or mobile app?
2. Which of the following are true about the terms of service or terms of use on a website or mobile app?

Each question had eight options including both positively and negatively stated phrases, as well as two options that offered combinations:

- “It protects me”
- “It protects the business”
- “It does not protect me”
- “It does not protect the business”
- “It is a contract”

- “It is not a contract”
- “It is enforceable”
- “It is not enforceable”
- “It protects me and the business”
- “It does not protect me or the business”
- “None of these”

This study was found to be flawed with just over 6.1% of responses including contradicting phrases, for example, where a participant selected both “It protects me and the business” and “It does not protect me.” Also, because we included a “None of These“ option on both questions, there was a risk that it could be selected along with a positive phrase. In drafting the survey, we felt this was acceptable as long as an answer was required. If we did not require an answer, it would be difficult to know if a question with no options selected was inadvertantly skipped or if the participant felt that none of the answers were true. However, on reviewing the results, we decided to run a new survey that eliminated potentially contradictory selections.

6.2.2 August 2021 Study

In our August study, we dropped the negatively stated options. Instead, we asked participants to indicate whether the policy protects them, protects the business, whether it is a contract and whether it is enforceable. A fifth answer “None of these” was provided in case the respondent believed none of these to be true. (Appendix E)

1. Which of the following are true about a privacy policy on a website or mobile app?

- It is legally binding
- It protects me

- It protects the business
- It is a contract
- None of these

Please describe why you answered this question the way you did.

2. Which of the following are true about a terms of service or terms of use on a website or mobile app?

- It is legally binding
- It protects me
- It protects the business
- It is a contract
- None of these

Please describe why you answered this question the way you did.

This shorter survey offered clearer insights. The following table shows response rates for each option.

Table 3: Response rate for each option in the survey

	Privacy policy	TOS/TOU
It protects me	49.7%	34.8%
It protects the business	67.5%	67.7%
It is a contract	38.5%	45.2%
It is enforceable	29.3%	33.7%
None of these	7.7%	9.9%

Just under 40% understood the privacy policy to be a contract (39%), and just under

a half said that a TOS/TOU is a contract (45%). This is a huge finding considering that the TOS/TOU is indeed a contract. Fewer indicated that these documents are enforceable with 29% for Privacy policies and 34% for TOS/TOU selecting "It is enforceable."

On privacy policies:

> "I can leave it any time. It is not a contract."

> "I'm not sure if it is a contract because I'm not sure if it's signed by both parties."

> "It is a contract part of the EULA that guarantees certain actions that the business may do with one's content, which may release them from certain responsibilities, but does not necessarily assure protection for end users."

On TOS/TOUs:

> "[Not a contract] Because it doesn't have my signature."

> "I don't think it is a contract and I don't really think it is legally binding and it's just something businesses put in place."

> "Good lawyers can get around the excessive verbiage, so I don't know if it's really legally binding."

More than two thirds of the respondents selected "It protects the business" for both the privacy policy and the TOS/TOU, while less than half selected "It protects me" for either policy. More people selected "It protects me" (about 50%) in regard to privacy policy than TOS/TOUs (35%). This data indicates that the Privacy policies and TOS/TOUs are thought to favor business interests with more perceived protection to the consumer by privacy policies.

"It provides limited protection for both sides."

"I just don't believe they would have our best interest in mind."

"[T]he only thing I know for sure is that I'm not protected."

Female respondents were more likely than males to indicate that a Privacy policy "Protects me" (56% of females and 43% of males), and that "It is a contract" (41% of females and 36% of males) and that "It is enforceable" (31% females and 28% of males). Other responses were similar across genders

8% selected "None of these" for Privacy policies and 10% selected "None of These" for TOS/TOU, indicating they do not believe it protects them or the business and that it is neither a contract nor enforceable.

We also looked at combinations to see if there are any patterns.

Table 4: Privacy policy: Response Rate for Combined Options

	It protects me	It protects the business	It is a contract	It is enforceable	None of these
It protects me	**49.7%**	29.7%	19.2%	17.2%	0.2%
It protects the business	29.7%	**65.7%**	29.2%	24.6%	0.4%
It is a contract	19.2%	29.2%	**38.5%**	20.7%	7.7%
It is enforceable	17.2%	24.6%	20.7%	**29.3%**	0.4%
None of these	0.2%	0.4%	0.0%	0.4%	**7.7%**

Table 5: Privacy policy: Correlation between pairs of responses

	It protects me	It protects the business	It is a contract	It is enforceable	None of these
It protects me	1.000	-0.126	0.001	0.115	-0.275
It protects the business	-0.126	1.000	0.168	0.246	-0.373
It is a contract	0.001	0.168	1.000	0.426	-0.229
It is enforceable	0.115	0.246	0.426	1.000	-0.158
None of these	-0.275	-0.373	-0.229	-0.158	1.000

We looked at combinations of examples to see if there is a correlation between any of the statements. For example, if respondents believed that a document is a contract, do they also believe it provides protection to both parties? Below are some of the more interesting combinations; however, none showed a particularly strong correlation.

38.5% selected “It is a Contract” only 20.7% selected both “It is a Contract” and “It is enforceable.” Overall, only 29.3% selected “It is Enforceable”, which is 9.2% fewer than those who selected “It is a contract.”

Less than one third (29.7%) selected both “It protects me” and “It protects the business.” Only a fifth or responses (20.0%) selected “it protects me” but did not select “It protects the business.” 36.0% selected “It protects the business” but did not select “It protects me.”

Table 6: TOS/TOU: Response Rate for Combined Options

	It protects me	It protects the business	It is a contract	It is enforceable	None of these
It protects me	**34.8%**	22.3%	16.9%	14.6%	0.7%

It protects the business	22.3%	**67.7%**	32.9%	27.2%	0.5%
It is a contract	16.9%	32.9%	**45.2%**	24.1%	0.5%
It is enforceable	14.6%	27.2%	24.1%	**33.7%**	0.5%
None of these	0.7%	0.5%	0.5%	0.5%	**9.5%**

Table 7: TOS/TOU: Correlation between pairs of responses

	It protects me	It protects the business	It is a contract	It is enforceable	None of these
It protects me	1.000	-0.055	0.049	0.126	-0.186
It protects the business	-0.055	1.000	0.099	0.199	-0.430
It is a contract	0.049	0.099	1.000	0.376	-0.258
It is enforceable	0.126	0.199	0.376	1.000	-0.193
None of these	-0.186	-0.430	-0.258	-0.193	1.000

More people (45.2%) selected “It is a Contract” for TOS/TOU than for Privacy policies. Slightly fewer (33.7%) said “It is Enforceable”.

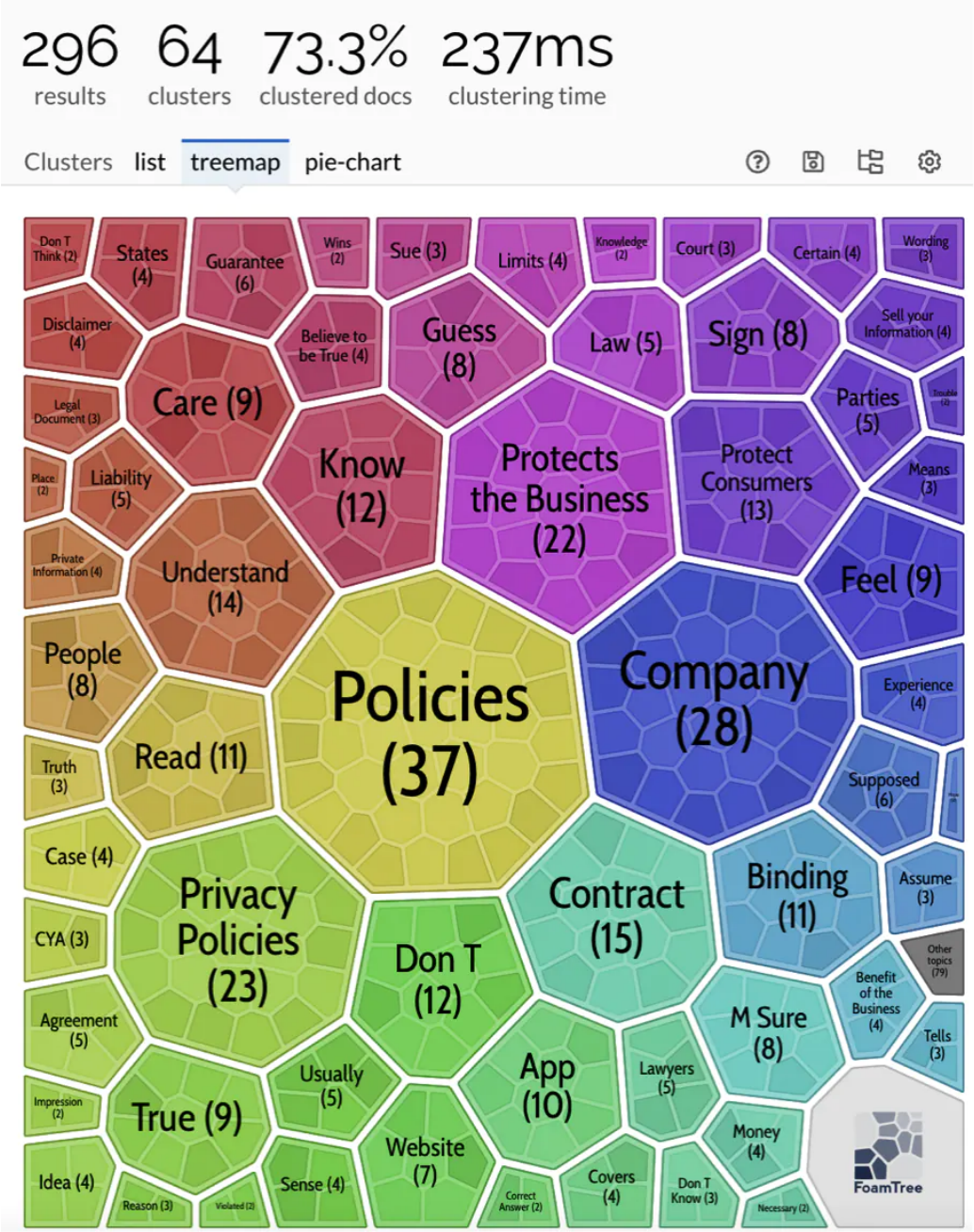
Those who felt it protected the business were divided over whether it also protects them (29.7% for privacy policies and 22.3% for TOS/TOU) and whether it was a contract (29.2% for privacy policies and 32.9% for TOS/TOU) or enforceable (24.6% for privacy policies and 27.2% for TOS/TOU).

Fewer participants (38.4%) selected “it protects me” for the TOU/TOS than for a privacy policy. Roughly the same number selected “It protects the business” (65.7% for privacy policies and 67.7% for TOU/TOS). For TOS/TOU, 12.5% selected “it

protects me” but did not select “It protects the business”, nearly half the number for privacy policies (45.3% selected “It protects the business” but did not select “It protects me” for TOS/TOU.

For a deeper look, we used the Carrot2 Clustering Workbench program to identify word clusters for each question. And highlighted common themes in the responses.

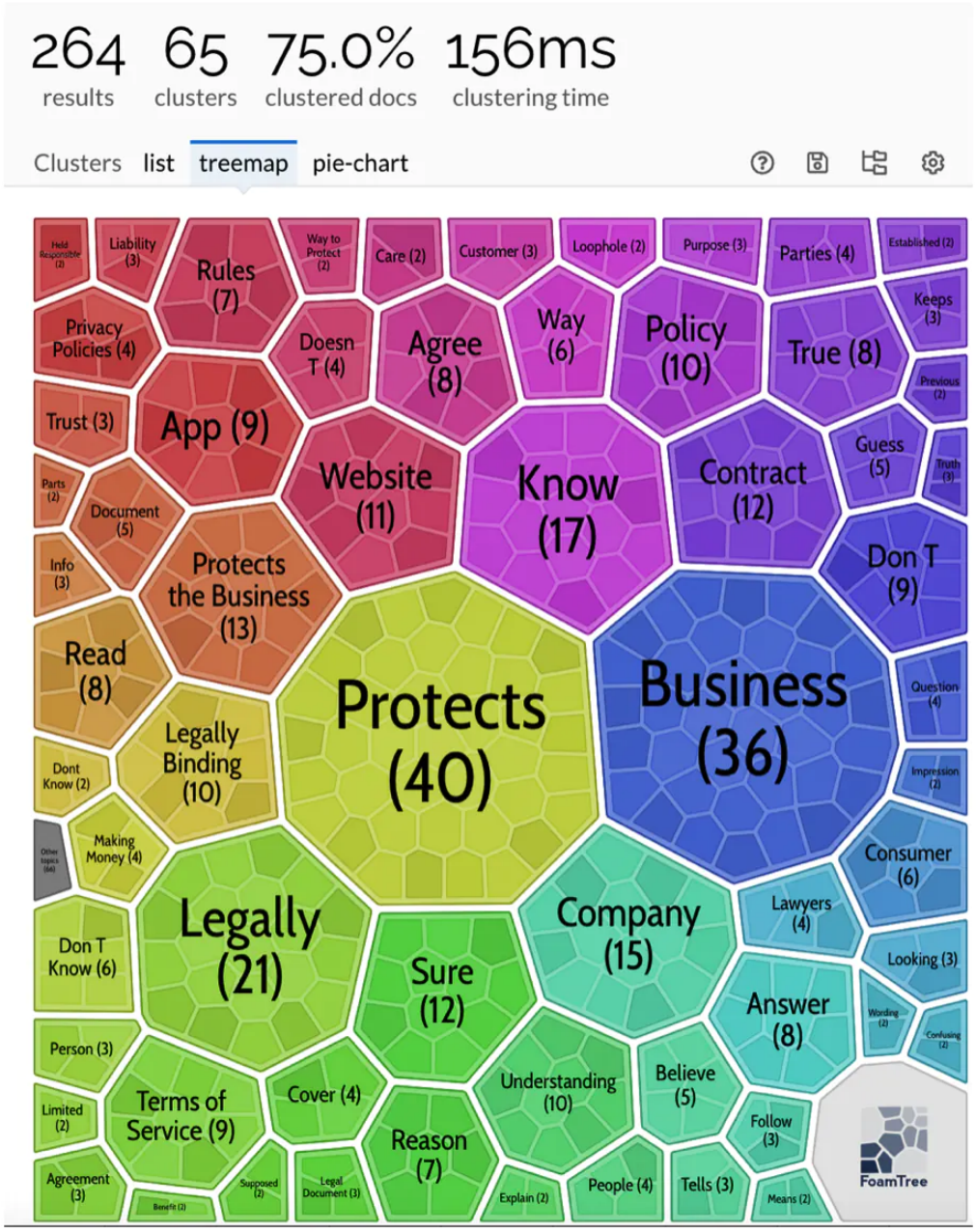
The following image indicates the prevalence of various terms and phrases for privacy policies:



The top clusters were Policies (37), Company (28), Privacy Policies (23) and Protects the Business (22), which is logical since the question was to describe why the participant answered the way they did about privacy policies. Using the term “privacy” or references to protecting the business/company or the individual would be expected. It is interesting that the phrase Protects the Business (22) appears more frequently than Protects Consumers (13).

Several clusters indicate uncertainty: While 14 of the comments that contained the term “Understand” or “understanding” were positive, as in “This is what I understand,” and clusters containing “feel” (9), “guess” (8), “supposed” (6), and variations on “not sure” or “unsure” (11).

For TOS/TOU, we found the following clusters:



The top clusters were Protects (40), Business (36) and Legally (21), Company (15), Protects the Business (13) and Legally Binding (10) which is again logical since the question was to describe why the participant answered the way they did about TOS/TOUs and whom they protect and whether they were enforcable. Again Protects the Business (13) appears more frequently than phrases indicating protection of the individual consumer. In fact “protects consumers” did not appear in the responses, while “protects me” appeared only once. There were six instances indicating that both parties were protected by TOS/TOU, but “Both” was not one of

the clusters.

Like with the privacy policy cluster analysis, many responses for the TOS/TOU indicate uncertainty: Eleven of 17 instances of “know” contained variations of the phrase “don’t know,” such as “don’t really know.”

7 Conclusions and Recommendations

7.1 Key Findings

Are consumers aware of legal documents on connected technologies?

Consumers are aware of the legal policies on connected technologies but see them as things they should read and understand but that are ignored in favor of getting to the app or website as quickly as possible.

Do consumers understand accurately what these documents are for and whom they protect?

Not all participants that we interviewed had a good understanding of what privacy policies and TOS/TOU agreements are or whom they protect. Some attributed policies of use, which they called “rules” to the privacy policy as well as the terms of use. Both those with a good and poor understandings of these policies say that the policies are there largely to protect the digital technology company and to enforce rules around what they can and can’t do with the technology. Our cluster analysis uncovered some uncertainty in the responses.

Are consumers aware that these documents are contracts?

In the survey 39% erroneously believed that a privacy policy is a contract and only

45% believed that a TOS/TOU is a contract. None of the interview participants indicated an awareness that the privacy policy or TOS/TOU outlined a contractual obligation. They understood the Privacy policy as a promise not to share data, but they were skeptical. As for the TOS/TOU, they understood these as “rules” that they have to abide by. It was understood more as potentially punitive than as mutually agreed terms.

Do consumers use or are they aware of tools to evaluate legal documents?

None of the participants were aware of the existence of tools they can use to evaluate legal policies. They were aware of review sites that evaluate digital products from a consumer perspective, and some understand what a browser plugin is, but tend to use them to block cookies or extend the functionality of an existing program. The interviewer demonstrated two browser plugins, including TOS;DR (tosdr.org), an independent user rights initiative that evaluates Terms of Service, and Privacy Badger (privacybadger.org), an open-source browser extension that blocks cookies, created by the Electronic Frontier Foundation.

Would consumers alter their behavior knowing what these documents mean?

Results from TOS;DR and Privacy Badger on various websites suggested by the participant were of great interest to the participants. Some said that it would potentially give them pause before using a new website, though most are cautious with new technologies anyway. However, half of the participants said that it is unlikely that knowing a site’s score would change their behavior, especially if they are a current customer of that site. They were not surprised that sites like Amazon or Facebook received low scores and suggested of these sites that “the damage is already done.”

7.2 Recommendations

Should the Me2B Alliance create a scoring system for legal policies?

Given that consumers are not likely to change their behavior even if they know a site has a poor score for its legal policies it is difficult to justify creating a legal policy rating service. Alternatively, Me2B Alliance may wish to consider partnering with organizations like TOS;DR that do this type of rating.

8. Appendix A: Participant Snapshots

Below are brief snapshots of the Me-s who participanted in interviews and/or focus groups for this research. We have excluded names (even psuedonyms) and demographic information to protect the privacy of these individuals and prevent a biased reading of their responses to questions. Since we are aware that profile building technology can potentially reverse-engineer personally-identifiable information about an individual from the collection of online accounts they hold, we are careful to not only exclude names and demographic information, but also to exclude the names of specific companies and technologies. Instead, we list the number and category of accounts and services held by each participant.

Participant 1	Snapshot: Cautious Consumer
	Estimated that they have 10-15 total accounts and was able to name 13. This participant was the most cautious of this group. They seemed at first to be unclear on the difference between privacy policies and TOS/TOUs but as the interview went on it

became clear that they are aware of them and are curious about third party cookies and sites. Participant 1 skims legal policies when “forced to read them” before signing up, and researches unfamiliar sites. This was the only participant who expressed confidence that deleting their account was a likely response, if something bad, like theft, abuse or racism was reported in connection to the business.

Quotes: Aware of and favorable of plugins because “They make it better to do anything in regard to the Internet....”

Devices regularly used: Computer, webcam, mobile device, four different web browsers.

Key connected products and services discussed: Several email account providers including two provided by the employer, one cloud-based file storage service, one social media account, and one mobile wallet account that they said they had subsequently deleted.

Participant 2

Snapshot: The Skimmer

Estimated having somewhere in the range of 51 to 100 accounts. Skims privacy policies and terms of service for items specific to the use of their financial information. This participant mentioned two cases that would make them rethink using a particular digital technology: security breach and sharing of credit card

information. Used the term “virtual footprint” when describing what the privacy policy allows companies to track.

Quotes: “I do think it’s on me to read them [privacy policies and terms of use] and absorb them and figure them out.”

Devices regularly used: Computer with webcam, mobile phone, tablet device, and two web browsers.

Key connected products and services discussed: One personal and one work email account, an online chat tool, one streaming media service and several online retails sites for household items and clothing.

Participant 3

Snapshot: Too Many Accounts

Selected the option for between 51 and 100. This participant stood out for the sheer number of products and services they could name at once that they use. Understands clearly that they all track users but is carefree about most of it. Answered questions gleefully and with wry cynicism at times.

Quotes: On EULAs: “documents you have to scroll to the end to use the product. Random clauses thrown in that no one ever challenges it.” On TOS/TOU: “If you violate the terms, incite violent revolution, we can ban you.”

Devices regularly used: One home computer with webcam, one mobile phone,

one tablet computer, and two web browsers

Key connected products and services discussed: Two personal email accounts and one work email account. a personal online database, online auto service, two online social media accounts (one disengaged a while ago), three online banking or trading accounts, multiple credit cards, medical, dental, auto, insurance accounts. For work, three cloud-based file storage accounts and three conferencing accounts. Three media streaming accounts, three video game accounts and other entertainment/media accounts.

Participant 4

Snapshot: Secret Shopper

Savvy about privacy and tracking cookies, even though they don't feel very informed about or understand well the subtleties and legalese of the digital agreements. Frequently interrupted to apologize for not answering the questions but tended to have more interesting responses. While enumerating accounts, this participant remarked that it "feels way more than expected." Does not use cloud-based file storage accounts except for phone backup. Rarely creates accounts at online stores, other than one major retailer, which they use a lot.

Quotes: "I always forget my password...so I just do the option where you enter as a guest... I do it over and over."

Legal documents "are very long and legalese." "It's set up most of the time

where you have to say you agree, because if you don't, you can't go to the next step to buy your grilled cheese sandwich or whatever, so you just click accept."

Devices regularly used: Two personal computers with webcam, one mobile phone, two tablet computers, three web browsers.

Key connected products and services discussed: Two personal and one work email accounts, several work software accounts, three social media, several financial accounts including credit cards, checking account, investment, and insurance accounts, one cloud-based file storage service, two online conferencing accounts and one that they use without an account. several online retail accounts ("If I buy anything I create an account."); Two media streaming accounts. Several mobile apps, one local newspaper account and one restaurant loyalty program.

Participant 5

Snapshot: Tech Savvy

Estimated having over 101-500 online accounts, many of which use a federated ID to access rather than creating separate accounts. "[There are] too many to count." Skims online legal policies. Handles a lot of visual assets at work so is most interested in copyright. Very interested in pricing and fees. Skeptical of bias in news media and does not pay for news.

Quotes: "When I sign up, I definitely want to know what the company had access to."

Devices regularly used: Two personal computers, one mobile phone; one web

browser, “Several” email accounts including a personal account, a work account and a student email account.

Key connected products and services discussed: Four social media accounts, one airline, one credit union, four credit cards including two affiliated with retail loyalty programs. Health insurance, HSA and IRA investment accounts. Three cloud-based file storage accounts, two of which are unused. Four online retail accounts.

Participant 6

Snapshot: Avid Online Shopper

Has hundreds of online accounts and five different emails. Noted that their list of passwords is huge. Read about 2%. Ambivalent about privacy policies and TOS/TOU, but not naïve. Has had an experience where a company offered a free blender on signup but never sent the blender. But won’t necessarily delete an account when something bad happens. Referring to a favorite site, they said sometimes there is only one place where you can get something you need.

Quotes: “There are certain things that I won’t give up.”

Devices regularly used: Two personal computers with webcams, two browsers, one mobile phone, three tablet computers.

Key connected products and services discussed: One personal and one work

email accounts, two social media accounts, two cloud-based file storage accounts, several online retail accounts, two music streaming accounts, one news account, two online money transferring services, a dog walking service.

9. Appendix B: Screener Survey

Question 1 (Pick one)

Do you have reliable Internet service in your home?

- Yes (accept)
- No (reject)
- Not sure (reject)

Question 2 (Pick one)

What kinds of computing devices do you frequently use?

- Computer (accept)
- Smartphone (accept)
- Tablet (accept)
- Smart TV or Smart DVD/Blueray player (accept)
- Connected device (accept)
- Connected wearable (accept)
- Smart speaker or personal assistant (accept)
- Other (accept)
- None of the above (reject)

Question 3 (Pick one)

In which of the following sectors do you work?

- Banking or finance (accept)
- Business management (accept)
- Healthcare (accept)
- Law (reject)
- Manufacturing (accept)
- Retail/Wholesale (accept)
- Technology (reject)
- Media (accept)
- Education (accept)
- Other/none (accept)

Question 4 (Pick one)

Do you live or work in any of the following locations? Austin, Boston, Chicago, Los Angeles, New York City, Raleigh-Durham, Redmond (WA), San Francisco Bay Area, Seattle?

- Yes (reject)
- No (accept)

10. Appendix C: Informed Consent

Informed Consent

Me2B Alliance

CONSENT TO ACT AS A RESEARCH SUBJECT

Treatment of consumers by Internet-enabled businesses

Me2B Alliance is conducting a study to understand the concerns of people who use connected products or services. Noreen Whysel will lead the study. You have been asked to take part because you are a consumer or user of connected products and services. There will be approximately 10 participants in this study over a one-month period.

If you agree to be in this study, the following will happen to you:

You will be asked a series of questions about your technology use and your feelings related to your technology use. The interview will last about 40 minutes. It will take place over videoconference and it will be recorded. The interview will be conducted by Noreen Whysel, and one additional Me2B volunteer may observe.

There will not be any direct benefit to you by participating in this study. There will be no cost, and you will be compensated for your participation. The investigator may learn more about how people want to be treated by Internet-enabled businesses.

Participation in this research is entirely voluntary. You may refuse to participate or withdraw at any time. You will not be compensated if you withdraw.

Audio recording:

Audio recording you as part of this project will help our research team better analyze your responses. We will not retain any video recording or imagery of your likeness. We will take the following steps to ensure your privacy:

Except to confirm your consent, we will not record any names, personal data,

or obviously identifying characteristics. If recorded, such information will be permanently deleted using audio editing software.

All identifying details will be concealed in the presentation of data.

The researcher will remind you when you are being recorded.

The audio recording and original transcript will not be made available to anyone outside our research team.

Risks: There is the possibility of loss of confidentiality. However, research records will be kept confidential to the extent allowed by law. Because this is an investigational study, there may be some unknown risks that are currently unforeseeable.

Ms. Whysel has explained this study to you and answered your questions. If you have other research related questions or problems, you may reach Ms. Whysel at noreen.whysel@me2ba.org.

11. Appendix D: Interview Guide

General Questions:

1. How many digital technologies do you use on a regular basis?
2. How many social media accounts do you use?
3. Do you have online accounts at any of the following types of services? (ask about the category first to prompt for the abundance of accounts, then use examples in they are slow to answer)
    a. Email (Gmail, Outlook, Yahoo!, AOL, etc)
    b. Social Media (Facebook, Twitter, Instagram, Pinterest, TikTok, etc)

c. Financial Services (bank, investment account, etc.)
d. Insurance Company (medical, dental, auto, home, etc)
e. Cloud storage (iCloud, Dropbox, OneDrive, Google Drive, etc)
f. Conferencing (Zoom, Webex, GotoMeeting, MS Teams, etc)
g. Retail Store (Amazon, Walmart, Target, Walgreens, Nike, etc)
h. Streaming Service (Netflix, Hulu, Spotify, Pandora, etc)
i. Publications (newspaper, magazine, etc)
j. Other

4. If you had to guess, about how many digital accounts do you have

 None

 1-20

 21-50

 51-100

 101-500

 More than 500

Understanding of Legal Policies

First I am going to ask you some questions about your interaction with the legal policies of your online accounts. Please answer to the best of your understanding and feel free to ask me to clarify any questions that you don't understand.

1. Do you read the privacy policies or terms of service for online, digital products or services?
2. Do you know what the difference is between these documents?

3. Off the top of your head, what are some things you might find in one of these documents?
4. Are there any specific paragraphs in a privacy policy or terms of service that you tend to look for or read?
5. Another way to ask: Have you been ever tried researching information about a company's terms of use and privacy policy? Did you find what you need?
6. Would reading news about a company that shows they care about privacy make you feel more secure using them?
7. Have you ever read a privacy policy (or TOS) that made you decide that you didn't want to use the website after reading it?
8. Do you recall receiving a notification in email or paper post about an update to a privacy policy (or TOS) that made you consider changing the service?

Awareness of Legal Policy Protections

Next, I'd like to understand why you companies have these policies. Again, there is no judgement. All answers are good answers.

1. What do you think the privacy policy is for?
2. What rights do you have? Are they protecting your rights/giving you rights/protecting you?
3. (Who are legal policies for?)
4. Do legal policies protect you as the consumer? How?
5. Do legal policies protect the organization? How?
6. Privacy policy
7. Terms of Service/Terms of Use
8. Have you seen cookie notices?
9. Are these legally binding?

10. Are they related to the privacy policy?

Introduce the definitions

Privacy policy: Public promise of how the technology and the company will treat you and your data. Enforceable by the FTC in the US.

Terms of Service/Terms of Use ("TOS/TOU"): The two-party contract that you are signing that both parties will abide by. Enforceable by the court of law.

Does any of this change your understanding of these policies?

Importance of these policies

1. Do you think it is important to read them before signing up for an account?
2. Why?
3. Why not?
4. Could they be important to you?

Awareness of Tools

1. Did you know there are plugins that read privacy policies?
2. If so, do you use them?
3. If you are aware of plugins and don't use them, why don't you use them?
4. Would you like to see a couple of these tools?
    a. If so, walk through ToS;DR (tosdr.org) and Privacy Badger (privacybadger.org)
    b. Filter for people who do use them
    c. Control group of people who don't

Trusted Opinions

1. Do you talk about legal policies with anyone?
2. Whose opinion would you trust to make a decision about whether to use a digital technology? (The following could be allowed to arise organically and then suggested: independent agency, rating service, friends, certification, etc.)

12. Appendix E: August Survey Questions

Which of the following are true about a privacy policy on a website or mobile app? (Select all that apply)

- ☐ It is legally binding
- ☐ It protects me
- ☐ It protects the business
- ☐ It is a contract
- ☐ None of these

Please describe why you answered the way you did. (open text box)

Which of the following are true about a terms of service or terms of use on a website or mobile app? (Select all that apply)

- ☐ It is legally binding
- ☐ It protects me
- ☐ It protects the business

 It is a contract

 None of these

Please describe why you answered the way you did. (open text box)

Footnotes:

1. Mutual Assent. Legal Information Institute, Cornell Law School. Web. https://www.law.cornell.edu/wex/mutual_assent
2. Note that the author of this report is not a lawyer. Additional legal research may be prudent.
3. See "Flash Guide #2: What is the Me2B Respectful Tech Specification?" https://me2ba.org/flash-guide-2-what-is-the-me2b-respectful-tech-specification/
4. See "Flash Guide #8: Digital Me2B Commitments and Deals", https://me2ba.org/flash-guide-8-digital-me2b-commitments-deals/
5. See "Flash Guide #9: The 10 Attributes of Respectful Me2B Commitments", https://me2ba.org/flash-guide-9-the-10-attributes-of-respectful-me2b-commitments/
6. IEEE P7012 – Machine Readable Privacy Terms Working Group. Web. https://sagroups.ieee.org/7012/
7. Privacy Badger. https://www.privacybadger.org
8. Terms Of Service; Didn't Read. https://www.tosdr.org
9. McDonald, Aleesia M. and Tom Lowenthal. 2013. "Nano-Notice: Privacy Disclosure at a Mobile Scale." Journal of Information Policy, Vol. 3 (2013), pp. 331-354 Penn State University Press. https://www.jstor.org/stable/10.5325/jinfopoli.3.2013.0331
10. Matthew Kugler & Lior Strahilevitz, "Is Privacy policy Language Irrelevant to

Consumers?," 45 Journal of Legal Studies S69 (2016).

11. Cisco. (2019). Consumer Privacy Survey. Cisco Cybersecurity Series 2019—Data Privacy. https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

12. Privacy and Security. Federal Trade Commission. Web. https://www.ftc.gov/tips-advice/business-center/privacy-and-security

---