PriBots

Conversational Privacy with Chatbots

Hamza Harkous\textsuperscript{1}, Kassem Fawaz\textsuperscript{2}, Kang. G. Shin\textsuperscript{2}, Karl Aberer\textsuperscript{1}

\textsuperscript{1}EPFL; \textsuperscript{2}University of Michigan

Workshop on the Future of Privacy Notices and Indicators, SOUPS 2016
When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account.

Privacy Policy

Last modified: March 20, 2018 (see archived versions)

Download PDF version

There are many different ways you can use our services — to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better — to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:

- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

We've tried to keep it as simple as possible, but if you're not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a long-time user, please do take the time to get to know our practices — and if you have any questions contact us.

Information we collect
Privacy Notice: Current State

Dual Role:

legally binding

human understandable
Can we split these roles?

Dual Role:

Privacy Notice: Current State

When you use Google services, you trust us with your information. This Privacy Policy is meant to help you understand what data we collect, why we collect it, and what we do with it. This is important; we hope you will take time to read it carefully. And remember, you can find controls to manage your information and protect your privacy and security at My Account.

Privacy Policy
Last modified: March 20, 2018 (view archived versions)

There are many different ways you can use our services – to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better – to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want you to be clear how we’re using information and the ways in which you can protect your privacy.

Our Privacy Policy explains:
• What information we collect and why we collect it.
• How we use that information.
• The choices we offer, including how to access and update information.

We’ve tried to keep it as simple as possible, but if you’re not familiar with terms like cookies, IP addresses, pixel tags and browsers, then read about these key terms first. Your privacy matters to Google so whether you are new to Google or a longtime user, please do take the time to get to know our practices – and if you have any questions contact us.

Information we collect
METHODOLOGY

We conducted an online user study in summer 2009 using Amazon's Mechanical Turk and a tool we developed called Surveyor's Point. Mechanical Turk offers workers the ability to perform short tasks and get compensated. People can place jobs through Mechanical Turk, specifying the number of workers they are looking for, necessary qualifications, the amount they are willing to pay, and details about the task. Mechanical Turk payments are generally calibrated for the length of the task. For our approximately 15-minute study, we paid $0.75 on successful completion.

We developed a custom survey-management tool called Surveyor's Point to facilitate our data collection. Our implementation allows us to show respondents a single question on the screen along with links for switching back and forth between two policies within a single browser window. This allowed us to track the number of users who looked at each policy and the number of times they switched between them. Additionally, Surveyor's Point allowed us to collect the amount of time that users spent reading the policies, as well as information about whether they clicked through to opt-out forms, to additional policy information links, or from a layered notice through to the full text policy.

In preparation for this study we first performed three smaller pilot tests of our survey framework. We ran our pilot studies with approximately thirty users each, across 2-3 conditions. Our pilot studies helped us to finalize remaining design decisions surrounding the standardized short table, refine our questionnaire, and test the integration of Surveyor's Point with Mechanical Turk.

We then conducted our large-scale study and completed the analysis with 764 participants (409 female, 355 male), randomly assigned to five conditions (see Table 1): full policy text, standardized table, standardized short table, standardized short text, and layered text. We dropped 25 additional participants from the study prior to analysis due to incomplete data or for completing the study in an amount of time that indicated inadequate attention to the task (defined as time on task that was two standard deviations lower than the mean). We chose a between-subjects design to remove learning effects and ensure the study could be completed within about 15 minutes. Participants in each condition followed the same protocol; only the policy format differed.

Policies

We selected policies for the study from companies that consumers would conceivably interact with. We narrowed our two systems are linked using a shared key that Surveyor's Point generates on the completion of our survey, which a participant then enters back into Mechanical Turk. This allows us to link an entry in Mechanical Turk with an entry in Surveyor's Point and verify the worker completed the survey before payment.
Figure 1. An example of a standardized table is shown on the left, and a standardized short table on the right. The comparison highlights the rows deleted to "shorten" this version. These deleted rows are listed directly below the table. While both formats contain the legend (bottom right), it is displayed only on the right here due to space constraints.

We have already deployed by major corporations, making them a viable, real world summary format for privacy policies. These policies were stripped of brand information, but the formatting and styles were retained.

**METHODOLOGY**

We conducted an online user study in summer 2009 using Amazon's Mechanical Turk and a tool we developed called Surveyor's Point. Mechanical Turk offers workers the ability to perform short tasks and get compensated. People can place jobs through Mechanical Turk, specifying the number of workers they are looking for, necessary qualifications, the amount they are willing to pay, and details about the task. Mechanical Turk payments are generally calibrated for the length of the task. For our approximately 15-minute study, we paid $0.75 on successful completion.

We developed a custom survey-management tool called Surveyor's Point to facilitate our data collection. Our implementation allows us to show respondents a single question on the screen along with links for switching back and forth between two policies within a single browser window. This allowed us to track the number of users who looked at each policy and the number of times they switched between them. Additionally, Surveyor's Point allowed us to collect the amount of time that users spent reading the policies, as well as information about whether they clicked through to opt-out forms, to additional policy information links, or from a layered notice through to the full text policy.

In preparation for this study we first performed three smaller pilot tests of our survey framework. We ran our pilot studies with approximately thirty users each, across 2-3 conditions. Our pilot studies helped us to finalize remaining design decisions surrounding the standardized short table, refine our questionnaire, and test the integration of Surveyor's Point with Mechanical Turk.

We then conducted our large-scale study and completed the analysis with 764 participants (409 female, 355 male), randomly assigned to five conditions (see Table 1): full policy text, standardized table, standardized short table, standardized short text, and layered text. We dropped 25 additional participants from the study prior to analysis due to incomplete data or for completing the study in an amount of time that indicated inadequate attention to the task (defined as time on task that was two standard deviations lower than the mean). We chose a between-subjects design to remove learning effects and ensure the study could be completed within about 15 minutes. Participants in each condition followed the same protocol; only the policy format differed.

**Policies**

We selected policies for the study from companies that consumers would conceivably interact with. We narrowed our selection to companies that have a privacy policy that is publicly available and has been approved by the industry association it is a part of. We identified the following types of companies:

- Financial services
- Retail
- E-commerce
- Telecommunication
- Social media
- Publishing
- Software
- Health care
- Information technology
- Advertising

These companies were selected because they represent different types of businesses that collect personal information from consumers.

**Standardization**

**Summarization**
Figure 1. An example of a standardized table is shown on the left, and a standardized short table on the right. The comparison highlights the rows deleted to "shorten" this version. These deleted rows are listed directly below the table. While both formats contain the legend (bottom right), it is displayed only on the right here due to space constraints.

METHODOLOGY

We conducted an online user study in summer 2009 using Amazon's Mechanical Turk and a tool we developed called Surveyor's Point. Mechanical Turk offers workers the ability to perform short tasks and get compensated. People can place jobs through Mechanical Turk, specifying the number of workers they are looking for, necessary qualifications, the amount they are willing to pay, and details about the task. Mechanical Turk payments are generally calibrated for the length of the task. For our approximately 15-minute study, we paid $0.75 on successful completion.

We developed a custom survey-management tool called Surveyor's Point to facilitate our data collection. Our implementation allows us to show respondents a single question on the screen along with links for switching back and forth between two policies within a single browser window. This allowed us to track the number of users who looked at each policy and the number of times they switched between them. Additionally, Surveyor's Point allowed us to collect the amount of time that users spent reading the policies, as well as information about whether they clicked through to opt-out forms, to additional policy information links, or from a layered notice through to the full text policy.

In preparation for this study we first performed three smaller pilot tests of our survey framework. We ran our pilot studies with approximately thirty users each, across 2-3 conditions. Our pilot studies helped us to finalize remaining design decisions surrounding the standardized short table, refine our questionnaire, and test the integration of Surveyor's Point with Mechanical Turk.

We then conducted our large-scale study and completed the analysis with 764 participants (409 female, 355 male), randomly assigned to five conditions (see Table 1): full policy text, standardized table, standardized short table, standardized short text, and layered text. We dropped 25 additional participants from the study prior to analysis due to incomplete data or for completing the study in an amount of time that indicated inadequate attention to the task (defined as time on task that was two standard deviations lower than the mean). We chose a between-subjects design to remove learning effects and ensure the study could be completed within about 15 minutes. Participants in each condition followed the same protocol; only the policy format differed.

Policies

We selected policies for the study from companies that consumers would conceivably interact with. We narrowed our two systems are linked using a shared key that Surveyor's Point generates on the completion of our survey, which a participant then enters back into Mechanical Turk. This allows us to link an entry in Mechanical Turk with an entry in Surveyor's Point and verify the worker completed the survey before payment.

Challenges

- one size fits all
- user education
Privacy Choice: Current State
Privacy Choice: Current State

fragmented ecosystem
difficult to find
Conversation-first Interfaces
The Future of Conversational UI Belongs to Hybrid Interfaces

2016 is the year of everything conversational. Messaging apps are taking over the world and app store rankings with incredible retention and engagement rates. Every community, marketplace, on-demand service, dating app...
PriBots: Conversational Privacy Bots
PriBots: Conversational Privacy Bots

Appeal to new tech adopters
PriBots: Conversational Privacy Bots

Appeal to new tech adopters

Appeal to existing users

Message
PriBots: Conversational Privacy Bots

Appeal to new tech adopters

Appeal to existing users

An intuitive way to
1. communicate privacy policies
2. adjust privacy preferences
1-Communicating Privacy Policies
Hello there! I'm a bot that you can chat with about our privacy policy. You can ask me questions like: "Does your app share my location?"
What is this Privacy Policy for?

This privacy policy is for this website [www.website.com] and served by [COMPANY NAME] and governs the privacy of its users who choose to use it.

The policy sets out the different areas where user privacy is concerned and outlines the obligations & requirements of the users, the website and website owners. Furthermore the way this website processes, stores and protects user data and information will also be detailed within this policy.

The Website

This website and its owners take a proactive approach to user privacy and ensure the necessary steps are taken to protect the privacy of its users throughout their visiting experience. This website complies to all UK national laws and requirements for user privacy.

Use of Cookies

This website uses cookies to better the users experience while visiting the website. Where applicable this website uses a cookie control system allowing the user on their first visit to the website to allow or disallow the use of cookies on their computer / device. This complies with recent legislation requirements for websites to obtain explicit consent from users before leaving behind or reading files such as cookies on a user’s computer / device.
Timing

At-setup
Timing

At-setup

Hello there! I'm a bot that you can chat with about our privacy policy. You can ask me questions like: "Does your app share my location?"

On-demand

Do you share my location with other companies?

No, your location is kept within our servers.
Feedback

- **implicit**: sentiment analysis
- **explicit**: structured messages
- gathering users’ concerns
Voicing User Concerns

Providers traditionally say what they want
Voicing User Concerns

Providers traditionally say what they want

Users’ concerns might not be covered
Voicing User Concerns

Providers traditionally say what they want.

Users’ concerns might not be covered.

PriBots activate the two-way channel.
2- Setting Privacy Preferences
Service and platform-dependent interface
Service and platform-dependent interface

Tradeoffs for simplicity: try finding this setting on Mobile Web version
Who can see my birthday?

All your friends can view your birthday. Do you want to change this?

Yea. Restrict it to myself.

Done! I made your birthday invisible to friends.
Unique interface with all functionalities
Ability to suggest adjustments to the user (combining notice and choice/preferences)
System Architecture

User Input

Analysis & Classification
System Architecture

User Input → Analysis & Classification → Query

Query Yes → Structured Query
Query No → Statement
System Architecture

User Input → Analysis & Classification → Query

Yes → Structured Query → Retrieval Module

No → Statement

Result → Confident?

Yes → Answer Formulation in NL

No → Fallback Answer Generation

Knowledge Base

Answer Formulation in NL

Fallback Answer Generation
System Architecture

User Input -> Analysis & Classification -> Query

- Yes: Structured Query -> Retrieval Module
- No: Statement

Structured Query -> Yes: Retrieval Module -> Result
- No: Confidence? -> Yes: Answer Formulation in NL
- No: Fallback Answer Generation

Result

Confidence?

Augment the Knowledge Base

- Amendments/Improvements
- Knowledge Base
- Feedback DB
- Analytics

- unanswered queries
- frequent questions
- user sentiments

Feedback

Amendments/Improvements

Analytics

DB

Analytics

Amendments/Improvements
Challenges
Mature User Understanding

- Text processing
- Question answering
- Domain-specific datasets and ontologies
- Graceful fallback
Legal Challenges

- Inherently error prone: are they legally binding?
- Accounting for false-positives and false-negatives
- The case of 3rd party PriBots: defamation possibilities?
Trusting the Machine

- rule-based vs. AI-based
- user backlash?
- regulate the confidence level
PriBots’ Personality

- positive tone $\rightarrow$ higher trust
- diversified content $\rightarrow$ reduced habituation
Deployment

Suitable for Voice Assistants

provider

3rd parties
What’s Next?

Privacy as a Dialogue
Rule-based Prototype
System Implementation
User studies
Questions/Feedback?

hamza.harkous@gmail.com
hamzaharkous.com
Image/Media Credits

- Zara Picken: slide 12
- Egor Kosten: slide 24
- Alex Prokhoda: slide 6
- Freepik: slide 23
- Geoff Keough: slide 14
- Victor: slide 12