

## Knowledge Over Control: Understanding and Addressing Privacy Apathy in Harlem through TurboTerms

Tristan Burchett, Leilanie Lewis, Mia Szczesniak, Jayden Wong

### INTRODUCTION

#### Study Background

15,280. That is how many surveillance cameras New York City's Police Department had access to in 2021, equipped with extensive facial recognition tracking.<sup>1</sup> This figure does not even include cameras owned by private businesses, the Metropolitan Transportation Authority (MTA), or personal home cameras. Some pin the total number at over 100,000 given the rapid expansion of MTA's surveillance system on newer subway cars.<sup>2</sup> That is one camera for every 80 New Yorkers. The expansion of surveillance technologies is not the only issue that affects 21st-century New Yorkers; the prevalence of mobile technology is also of great cause for concern. According to a 2019 article in *The Guardian*, "Apple contractors 'regularly hear confidential details' on Siri recordings."<sup>3</sup> Additionally, web browsers often store metadata on one's website usage called cookies, which may seem like a benefit to enhance one's experience on other websites, but often track high levels of data. This data often includes precise location and system configurations. Even newer technologies, such as OpenAI's flagship conversational Large Language Model (LLM) ChatGPT, are not built with privacy in mind.

Thus, we sought to inform the Harlem and Morningside communities on the privacy risks associated with mobile, web, artificial intelligence (AI), and surveillance technologies. This was part of our work with the Center for Smart Streetscapes (CS3) at Columbia University, an engineering and social science research center that works to improve the streets of NYC through advancing technology. We ultimately illustrated that while the community often has general knowledge of the risks surrounding these technologies, they prefer the convenience that comes with less privacy making them more resistant to improving it. As a result, we created an informational and engaging video that summarizes actions users can take as well as creating an actionable solution in the form of a browser extension named TurboTerms that creates tailored summaries of the terms and conditions (T&C), and privacy policies of websites.

---

<sup>1</sup> Amnesty International. "New York Is in Danger of Becoming a Total Surveillance City." Amnesty International, 3 June 2021, [www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/](https://www.amnesty.org/en/latest/news/2021/06/scale-new-york-police-facial-recognition-revealed/). Accessed 10. Aug. 2025

<sup>2</sup> "MTA Will Install Cameras in Every Subway Train Car to Curb Crime, Increase Safety." ABC7 New York, 20 Sept. 2022, [abc7ny.com/post/mta-subway-train-cameras-surveillance-safety/12243165/](https://abc7ny.com/post/mta-subway-train-cameras-surveillance-safety/12243165/). Accessed 10 Aug. 2025.

<sup>3</sup> Hern, Alex. "Apple Contractors 'Regularly Hear Confidential Details' on Siri Recordings." *The Guardian*, 26 July 2019, [www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings](https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings). Accessed 10. Aug. 2025

## **Research Question**

At first, our research question was, “What misconceptions and knowledge gaps exist among Harlem community members regarding how their data is collected, used, and shared by mobile applications and AI?” We initially hypothesized that participants did not know how their private information was stored and that major tech companies often allowed third-party companies access to their personal data. After Field Trip One, our research question changed as individuals knew that their personal information is often used differently than how they would like it to be. Most participants actually lost interest in fighting for their mobile and city privacy. Therefore, we focused on creating a tangible solution to assist them, which would help restore that agency in their privacy, leading to our final research question: “To what extent can we help individuals regain agency in mobile, web, artificial intelligence, and surveillance privacy within Harlem communities?”

## **METHODS**

### **Research Design**

During Field Trip One, we relied on surveys and interviews, ultimately recording 10 responses. These conversations were held at 125th Street and Malcolm X Boulevard. We wished to speak to individuals who would have some initial knowledge surrounding technology, particularly regarding mobile technology and AI software. Consequently, we decided that we should target an area with high levels of consumerism, particularly for those aged 18 to 29. 125th Street and Malcolm X Boulevard and the surrounding area has many shops, a subway station, and a City University of New York campus.

Throughout Field Trip Two we conducted 22 total interviews at Broadway between 112th and 116th Street. We chose this spot because we wanted to conduct interviews with more individuals below the age of 30, a group that we lacked data for after Field Trip One. The area between 112th and 116th Street has many restaurants, food stalls, multiple train stations, and the Columbia University Morningside campus. Adding to our rationale, students use AI technology to assist in studying and answering questions. Additionally, they use AI as a friend or to help with daily tasks. Thus, we concluded that this would be a strong location to conduct interviews.

### **Study Protocol**

In Field Trip One, we used a hybrid survey-interview method as we wanted to receive both quantitative and qualitative data for beginning analysis. We created a Google Forms questionnaire using both Likert scales and open ended questions. We created a fifteen question survey, asking about how individuals used AI and social media, their views regarding privacy

policies, if they knew where their personal data and information was collected or used, and demographic questions (see Appendix A). To tailor the development of TurboTerms, we developed a question that asked if individuals read the T&C or privacy policies. In conjunction with our original research task of educating the Harlem community on mobile and city privacy, we asked which educational tool such as a video, comic strip, or poster would be the most engaging.

Although initial analysis was smooth, our main focus shifted, prompting our team to transition to a strictly interview based approach for Field Trip 2. By doing so, we aimed to create a more conversational and a semi-structured twelve question interview protocol, encouraging participants to express their thoughts in greater detail. Instead of relying on structured binary responses, we focused on asking follow-up questions and allowing participants to elaborate in their own words; these new questions elaborated on how participants felt about their privacy on the internet, on different applications, and within their city (see Appendix D). Our question elimination reasoning (Appendix C) and updated protocol (Appendix D) demonstrates that we removed five questions from our first protocol due to redundancy and the insufficiency in adding new knowledge to lead to the development of our intervention. We kept five questions from the original form due to their success in having participants talk about their feelings about surveillance, AI, web privacy, and mobile privacy rather than knowledge that they already deemed common. Within this new 12-question protocol, we added a new question that introduced our TurboTerms prototype which we developed to enable responsibility within the community when it comes to taking initiative over their privacy. This shift led to better results, showing more emotional depth and thoughtful responses that we originally lacked.

### **Procedure**

In order to have the context regarding what the community should know about internet and in-person privacy, we attended mandatory lessons hosted by CS3 researchers about different topics in this domain. We learned about different ways that companies gather our data to sell to other companies for better ads for consumers, how their use of our data can be unethical, and ways that we can protect ourselves. We were originally given the task to create an educational artifact, but we were driven to also do something more hands-on, as reinstating actionability could be more meaningful than only teaching what can be done. Using the information learned within the lectures, we created 20 flyers that we would disperse after interviews were complete amidst both field trips (see Appendix B). Throughout the course of the lecture series, we worked on developing TurboTerms which could shorten the T&C or privacy policies of numerous websites.

In the first two interviews of Field Trip One, one person spoke to the participants and filled out the Google Form, one wrote notes in a separate notebook, and one recorded. After the first two, we decided to do interviews individually. Every participant was asked for consent to the interview being recorded and were promised anonymity. We remained at this site for about

two hours before concluding the first trip, and returned to CS3 where we transcribed the interviews and quantified the survey results. The data from Field Trip One was useful in giving insight on demographics and approximately the amount of people who felt a specific way about using AI, social media, and understanding privacy policies. However, through analysis, we learned that interviews would be more effective in answering our research question. During Field Trip Two, we divided into pairs; one person conducted and recorded the interview, while the other person took notes. We transcribed the second round of interviews and coded them to determine common themes.

### **Objective**

Our objective was to determine the emotions that the Harlem community expressed about their stance in protecting their privacy. Through their responses, we sought to create tools that would both teach and mitigate the harms the community noted toward the specified technologies.

## **RESULTS**

### **Demographics**

We interviewed 27 individuals. Of our participants, nine people identified as African American/African/Black, two identified as Caucasian, seven identified as Asian, four identified as Hispanic/Latino, and five identified with another ethnicity. Amongst the 27 individuals, 15 identified as men and 12 identified as women. In addition, six of our participants were aged 65+ years, 11 were aged 30-45, 10 were aged 18-29.

### **Data Analysis**

A common trend in the data was that 96% of participants, when discussing how much data was collected on them, stated they believed that large companies knew a majority of their personal information. Specifically, one participant mentioned that Google knew “most things” such as “personal info, address,” and “things I google and like” (Participant 17). Notably, one respondent worried that “Google will follow me forever” (Participant 18). Overall, the same 96% also believed they did not have the power to find solutions that could fix privacy issues that plagued their lives.

Additionally, while all respondents stated they have used AI in the past, ~56% (15/27) would share “personal information” with it. Furthermore, less than 15% of participants felt they had any control over their privacy. An important survey question that was asked during Field Trip One was, “Do you think your entire phone is listening to you?” 60% of participants from Field Trip One responded they did in fact believe their phones and apps are always listening to

them. Further, ~81% (22/27) of people stated that tracking has become so normal that they do not think much of it anymore. In spite of this idea, it was not the sentiment among all respondents with one participant stating that he has control over his data and does not know or care to improve it. Overall, the community sees tracking as something that is omnipresent and difficult to avoid.

When asked about T&C, 85% of respondents said they do not read them. Most described these policies as too long or “impossible to understand.” Participant 17 stated incredulously “40 pages [...] are those expected to be read?” All 27 individuals understood these T&C are important, however it was viewed as more of a burden and tended to be blindly accepted so they could get to their application. Although, 37% of participants did state that they do take action in protecting themselves online, no matter how miniscule they may feel it is. As individuals mention that there is not much you can do to protect yourself against surveillance technologies, 37% took steps like using VPNs and ad blockers, cybersecurity software, declining cookies, and asking apps not to track them.

In conjunction with the creation of TurboTerms, ~96% (26/27) of participants agreed that TurboTerms would be a viable solution to deducing complex T&C statements. This metric informed our development of TurboTerms after Field Trip One and the continual addition of features after Field Trip Two.

Within Field Trip One, we asked individuals about which form of artifact will be most educational for the community to understand what they can do about privacy. All participants agreed that a video would suit them best, as it is engaging and can have the most information.

## **Themes Derived from the Interviews**

### ***Trust***

Individuals lacked trust with technology that consisted of privacy-breaching risks, both online and in the streets. Throughout Field Trip One when individuals were asked, “how concerned are you about your privacy when you’re using your phone and AI,” one stated “...very, very concerned. Very” (Participant 4) articulating their responses strongly expressing their distrust. When asked, “would you tell the AI a secret?” individuals had strong negative reactions as well. The individual’s rationale was usually because they, “...don’t know who’s looking at my data. I don’t know where these data centers might be located. I don’t know if they’re in a country with good privacy laws...yeah, I don’t completely trust them” (Participant 13). This finding demonstrates that people did not feel comfortable with the idea that their personal information could be used in ways they did not intend.

In contrast, participants felt the need to comply with potentially harmful privacy policies. As Participant 1 stated, “[y]ou want to hope that they have your best interests, which is bad,” showing that users often relied on trust out of necessity, even though they knew it may not have

been well intentioned. This reliance on companies and governments to “have your best interest” was closely tied to how people engaged with privacy practices, especially when it came to T&C.

### *Emotions on Privacy*

Although individuals knew that their privacy was being compromised and that their personal data was being used in ways they did not intend it to be, many did not do anything about it. No participant had completely positive input on their security online or in-person. All participants felt indifferent to the idea that they did not have any control, as people believe that it is “...definitely part of what we’ve given up to become a connected society, that’s for sure” (Participant 7). From Field Trip Two, seven participants did not do anything to protect their privacy, due to their lack of interest. Participant 17 stated that they, “do not have a lot of power and I understand that my power is limited to the things I can control. And I think a lot of people try to control things that they cannot control and that leads to deeper issues.” Similar to Participant 17 this notion that individuals did not have much control was common. As individuals felt that their ability was limited, this encouraged them to just let the applications or websites they used utilize their data.

As uncovered in Field Trip Two, despite the common emotion on this issue being apathy, 10 participants took action in protecting themselves online, no matter how miniscule they may have felt it was. As Participant 13 stated, “there’s a certain limit of control that you can have to protect yourself and make sure you’re looking more secure... not as much as I’d like. [Interview question: What do you do to manage your privacy, either online or in the city?] online, like VPN is good, messaging people using something that’s not linked to a Meta, that’s always good as well ....” As individuals mention that there was not much they could do to protect city privacy, these 10 individuals took steps like using VPNs and ad blockers, cybersecurity software, declining cookies, and asking apps not to track them. This demonstrates that there were people that were interested in protecting their privacy, yet people just did not feel like they had the resources to.

### *Tracking*

Participants reported that they believed large companies tracked most of their personal information. While aware of the associated risks, many participants indicated that they prioritized the convenience and benefits of digital tools over concerns about data privacy. For example, when asked, “Do you manage your privacy at all?” Participant 19 replied “No. I just trust it.” Five participants expressed that this reliance on trust toward companies or governments influenced how they engaged with privacy practices, especially regarding T&C. When asked what the internet knows about them, a participant mentioned that Google knew “most things...personal info, address, things I Google and like” (Participant 17). Additionally, one respondent described the constant tracking by websites such as Google as “definitely problematic

and worrying” (Participant 24). Individuals understood that their activity was being tracked and recorded. Although discomfort was prevalent for more than half of participants, people did not take much action due to the lack of reward they felt they would receive.

### *Surveillance*

Another key theme was the prevalence of excess surveillance. Within Field Trip Two, 11 participants noted the surplus of cameras in the city did not add to their safety. A man in the district office stated that “a lot of cameras are owned by private places” which reduced the validity and safety of them (Participant 24). This was further supported by Participant 13 who said surveillance “creates a degree of self-consciousness.” Individuals felt more watched by all the cameras that were up, rather than protected, also raising questions like who was monitoring them. Participants mention that their trust depended on the institution in charge of the cameras. A recent graduate of Columbia University mentioned that he did not “trust the institution at all. I spent the last year here... if it’s an institution I trust, I’m in a residential building where I know the people, know the security guards, sure, I think that’ll probably make me feel safer. But yeah, it depends on the trust of the institution” (Participant 13). This can raise concern since it calls back to the idea of not knowing who was governing the surveillance cameras, which depleted the amount of trust the community had within their city.

In contrast, several individuals believed surveillance cameras were beneficial, particularly in the realm of safety. Notably, the subject of crime came up in a majority of interviews. For example, a student mentioned that cameras were, “governed by the government or some sort of entity, then at least whatever people are doing, makes our actions traceable” (Participant 12). Individuals felt that this form of monitoring was not excessive and an important asset to the quality of the city. An interviewed assembly member (Participant 19) said that cameras definitely reduce crimes and that CCTV (Closed Circuit Television) was the best option as it was owned by the government and not a private company. It was important to note that his position as an assembly member as part of the government likely influenced his response. He commented that he was more worried about private surveillance companies such as Ring, which were harder to regulate.

### *Terms and Conditions*

One significant problem was that people did not understand the T&C document because it was written with lengthy and obscure legal terms. Five participants actually reported that they read the T&C and privacy policies, one participant sometimes read them; the remaining 21 did not. One participant said “A thousand and one pages to go through where legally, if you’re not a lawyer, you would not understand...” (Participant 4). On the contrary, a different participant mentioned, “at 60, I need to be on top of my game. So yes, I will read the terms” (Participant 1). This shows that the participants realized that the T&C are important, however also agreed that

they are long and complex. Another participant said “I mean I do read [the T&C] when it’s really important” (Participant 5).

Although there was a mixture of citizens that may or may not have read these policies, they all shared the commonality of believing jargon riddled the document, making it hard to read. The same participant who did read the T&C mentioned that “the terms have hitting language. And that’s another reason why it might be discouraging for me not to go through the whole process. But since you said it, I’m going to start doing it” (Participant 1). When she said “hitting language”, this referred to the language that was hard to understand. Individuals feel that the T&C are “...how before they create [an application] they have lawyers write [the T&C]. So the lawyers just kind of [build] in protection from lawsuits” (Participant 7). As these policies were tailored to lawyers rather than the common consumer, people did not feel represented. If individuals did not understand something, then that would discourage them from learning more about what each application was collecting and sharing.

## DISCUSSION

Our findings showed that various individuals felt like their privacy was constantly being invaded, but they also felt powerless to change it; for example, they could not access websites if they did not accept T&C. Even when they cared, they often did not know what to do and felt like their data was already all over the internet and could not control or delete it. This sets the framework to answering our research question, as it illustrated a clear need for technology that was simple, transparent, and built with trust in mind.

Referring back to our research question, apathy was prevalent for all 27 participants. The lack of education on an individual’s rights to their privacy was common within Harlem, which should not have been the case. Individuals should be empowered through their privacy and secure; the fact that all individuals we spoke to expressed discomfort and sadness to their lack of control over something as precious as privacy was alarming. When citizens developed a mistrust in their cities and technologies, then those triumphant feelings to reclaim that agency faded and people lost hope. Our research question touches on why that was, and through our responses, it was because citizens did not know what to do about protecting their privacy. All individuals expressed joy in young citizens like us developing a way for the community to be involved in counteracting this lack of action in protecting privacy.

As previously mentioned, our focus shifted from the public’s knowledge because citizens already knew that their personal information was not localized; it was stored and sold to other companies outside of what they interacted with online for more personalized advertisements or stronger technology to be released. Nonetheless, citizens did not know as much about small actions they could take to limit tracking of their person, which partially contributed to their apathy. Additionally, all participants collectively agreed that city privacy was hard to manage as the surplus of cameras will always exist. Connecting to our research question, as a team we could



start small; starting with tackling internet safety to make privacy measures more noticeable, consequently leading to more citizens in the city doing more to protect themselves online.

### **Initial Assumptions**

Initially, we assumed that our first location, 125th St and Malcom X Blvd, would give us a large pool of data to work with; varying from 18 to 65+. However, this assumption was disproved as 90% of our participants were aged 30+ during Field Trip 1, and all were well versed with social media. As the main problem was citizens not feeling safe putting their information into the web due to not knowing if their privacy was being maintained, individuals were just as skeptical as we assumed.

We also believed that individuals would be more alarmed and did more to protect their online identity. This consensus was unfortunately counteracted by the large amount of apathy met with many of our interview questions. Moreover, we believed that community members would be more closed off to the idea of using AI due to their lack of knowledge on privacy protections. This assumption still stands; although our focus shifted from that, the remaining participants who did not do anything to protect privacy were because they did not know where to start, as T&C and privacy policies are too long and they just did not believe their efforts would change anything.

### **Interventions**

#### ***Artifact***

As mentioned prior, after Field Trip One, our data showed the community expressed strong opinions on the best educational artifact being a video. As part of our engineering fulfillment, we scripted and recorded our video artifact about ways individuals can protect their data while browsing the internet. Although it contained elements to quickly explain tracking tools used by internet companies and ways to subside them, we wanted to create something that was more actionable for the user.

#### ***TurboTerms***

TurboTerms was built to address the barrier between a user's privacy and their general knowledge. During engineering sessions at CS3, we worked on an extension that detects terms and privacy documents on websites and instantly summarizes them into concise bullet points. TurboTerms helps users understand what they are agreeing to, including what data is being collected, who it is being shared with, and what rights they may be giving up.

The initial version of TurboTerms (created before Field Trip Two) can be viewed in Appendix D, and additional developments have been made in the time since. Version 1.0 (Appendix D) contained links to all subpages on the given website relating to T&C, with some keyword searches including “terms,” “conditions,” “terms and conditions,” and “privacy policy.” Version 1.1 (not shown) included some new features to enhance the interactability of the extension, including a tab to ask questions directly about the T&C and a dropdown menu where users can input their familiarity around online privacy that informs the T&C summaries. These features were implemented due to the community’s desire for clarity and interactive features. Version 1.2 (not shown), while not including any major UI updates, included a major step in enhancing the security of TurboTerms. It stored the OpenAI API key used to create summaries and answer questions as a Cloudflare secret environment variable, as opposed to insecurely storing it as a global variable within the extension’s JavaScript.

### **Limitations**

Our largest limitation was the initial survey-interview method. The survey format, by nature, constrained responses to binary or limited options, which restricted the depth of information collected. Additionally, some survey questions were repetitive, reducing overall efficiency with participants speaking too fast on open-ended questions. Through the hybrid survey-interview structure, the emotional tone and depth of participants’ feelings about digital privacy were not able to be adequately captured. For example, when asked, “What do you think are the best ways to educate the community about privacy and phone security?” some responses were vague or difficult to interpret: such as “real person,” “deal with your issues in public?”, “what is outcome,” or simply “n/a” because we could not capture what they were saying. As a result, while we were able to collect enough quantitative data to analyze, much of the rich qualitative insight we hoped to gather was missing.

Although we were able to acquire data during Field Trip One, we did not talk to anyone under the age of 30, which did not give us the variety of answers we were hoping for. Additionally, we conducted 22 interviews, although we encountered five people under the age of 18; due to underage consent concerns, their responses were scrapped from analysis. Additionally, our lack of numeric data outside of demographic questions in Field Trip One made initial analysis somewhat difficult, although as our sample size grew bigger, we were able to draw conclusions off of more subjective data.

In regards to questions, in the future, we can pinpoint more forms of AI. We only referred to generative AI, like ChatGPT and Google Gemini. However, there is AI in numerous applications; shortening search results for users in Google, recommending new artists in Spotify, even ticketing drivers in bus lanes within the city. Getting more insight into how individuals felt about this could have helped us grasp the relationships individuals may have with AI.

Additionally, asking them specifically where they thought information went and how it was used would also have been useful, as it could have provided credibility to our intervention as a lot of these answers were buried into the T&C that people refused to read, potentially jeopardizing their internet safety.

## CONCLUSION

Privacy is a valuable asset to being human; as large companies and governments thrive and start tracking individuals closely, it almost strips the freedom and security from people. Unfortunately, a main cause of this is the lack of transparency between governments, large corporations, and their consumers, meaning that we as CS3 researchers must do more to bridge that gap between the community and their knowledge of privacy. Through involving our citizens, our research revealed this sense of security consistently being ignored. Our data demonstrated a significant disconnect between individuals' awareness of digital privacy risks and their willingness to do something about protecting their privacy. Recognizing these challenges, we developed our browser extension TurboTerms, directly inspired from what we heard in our interviews.

For our engineering teams and the CS3 community, this means focusing on tools and education that help people better understand and control their data, such as our browser extension TurboTerms. Stronger attempts to protect an individual's data need to be made. As of right now judging by the various responses, any hope in this has been reduced. Thus, it is our job as researchers to develop methods to teach the community the importance of keeping their privacy in mind. TurboTerms is a strong foundation to begin with as it successfully simplifies what they should know and what they are agreeing to, although more can be done to grant the agency of privacy, security, and anonymity back to the community.

**APPENDIX A**

## Field Trip One Questionnaire:

Hello we are (My name is \_\_\_\_ and I'm a high school student doing a research program (at Center for Smart Streetscapes with Columbia University) focused on educating people about misconceptions and knowledge gaps within personal data that may be collected, used, and shared by mobile applications and AI. Do you have 5 minutes for us to answer a few questions? You are allowed to skip any questions you don't feel comfortable sharing or opt out of this interview at any time. Also, do you consent to being recorded? Your information will be anonymous.

|   |   |
|---|---|
| How many apps do you think are tracking your location right now?  | Open-ended  |
| Have you ever felt that your phone was listening to you?  | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• Other</li> </ul>  |
| Have you ever used AI(artificial intelligence)  | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• Other</li> </ul>  |
| Do you mind telling AI a secret or something personal about you?  | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• Other</li> </ul>  |
| How concerned are you about your privacy when using your phone through certain apps or artificial intelligence? | Multiple choice <ul style="list-style-type: none"> <li>• Very concerned</li> <li>• Somewhat concerned</li> <li>• Not concerned</li> <li>• Neutral</li> <li>• Other</li> </ul> |
| Do you believe you have control over your privacy online?   | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• Somewhat</li> </ul>   |

## PRIVACY

13


|  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• No</li> <li>• I'm not sure</li> <li>• Other</li> </ul>                               |
| Do you know that certain apps or AI programs could be using your personal information about you to improve their systems in the future?                          | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• Other</li> </ul>                        |
| Do you read the terms and conditions policy when you download an app?  | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• Sometimes</li> <li>• Other</li> </ul>   |
| Would you ever use a browsing extension that will summarize the terms and conditions of an app or website to tell you in easier terms if your data is protected? | Multiple choice <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> <li>• I'm not sure</li> </ul>                 |
| What do you think the internet knows about you?  | Open-ended  |
| What do you think are the best ways to educate the community about privacy and phone security?   | Open-ended  |
| What gender do you identify as?  | Open-ended  |
| What is your race/ ethnicity?  | Open-ended  |
| Do you mind sharing your age?  | Multiple choice <ul style="list-style-type: none"> <li>• Under 18</li> <li>• 18-29</li> <li>• 30-64</li> <li>• 65+</li> </ul> |
| Any questions? comments? or concerns? Is there anything else you think I should have asked you?  | Open-ended  |

## APPENDIX B

## Flyers

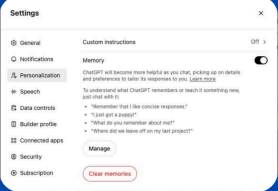
## Privacy in AI

Do you know where your data goes each time you use an AI tool?




OpenAI says: "We may share your Personal Data [...] with government authorities, industry peers, or other third parties..."

### AI OR SPY?




Share less  
Use privacy tools  
Check AI policies

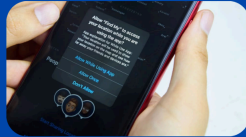


## Mobile Privacy Concerns


Warning your data may be getting shared without your knowledge




How many apps do you think track your location right now?



Tracking **METHODS**:  
location, Wi-Fi,  
motion sensors,  
Bluetooth,  
advertising IDs



turn off tracking  
Reset Advertising ID  
use tools such as Exodus  
Privacy  
just be aware of these issues



Apps often include third-party tools that can record your screen, take screenshots, or upload photos without notifying you. Even if an app's privacy policy seems clear, you may not be protected from what third-party code inside the app does.

**APPENDIX C**

## Question Revisions for Field Trip Two:

**QUESTIONS THAT WERE REMOVED**

As we originally went the survey and interview route, some questions were close ended, and others were open ended. The mixture led to repetitive questions leading to an insufficient pool of answers; some of the questions did not lead to new information, however only added to what we knew. So, below are some questions that were in our original intervention.

**How many apps do you think are tracking your location right now?**

This question was removed because this touches more on knowledge and less on personal feelings. Also, people were saying many numbers without proper reason; as if they were shooting a number because they felt they had to.

**Have you ever felt that your phone was listening to you?**

This question was removed since there was a question asked later asking “What do you feel the internet knows about you?” which we felt was more effective and widespread, as we noticed that some individuals did not have their phone on them.

**How concerned are you about your privacy when using your phone through certain apps or artificial intelligence?**

This question was removed due to its redundancy, as well as because it is in survey format. This question will have more impact if we ask if they feel they have control over their privacy, since from there it will reveal how concerned they are.

**Do you know that certain apps or AI programs could be using your personal information about you to improve their systems in the future?**

This question was removed since the majority of participants, to our surprise, already deemed this common knowledge. However the mundane reactions of this outcome was what really turned our focus around.

**What do you think are the best ways to educate the community about privacy and phone security?**

This question was removed since it was too open-ended that we did not get the answer we were looking for (video, comic strip, memes, etc.). However, when prompted, the majority of participants said video, so this will be our artifact of choice due to how expressive and informative participants expressed it could be.

## REVISED INTERVIEW QUESTIONS

### Mobile Privacy

- 1) **What do you think the internet knows about you?** *(Originally, this question was at the end, which made it redundant and useless. However, placing it at the beginning is a good icebreaker and a question to ease into the rest of the interview.)*

### Artificial Intelligence

- 2) **Have you ever used AI(artificial intelligence) such as ChatGP or Google AI? Why or why not?** *(This question changed as we ask for them to share any specific circumstances or reasons for their usage of AI)*
- 3) **Would you tell an AI a secret? Why or why not?** *(This question was kept since it was a specific twist to really see how closely people rely on AI, as well as how they perceive it.)*

### Web Privacy

- 4) **Do you read the terms and conditions policy when you download an app or use a website and if so why? Or why not?** *(This question is useful for our web browser, as it give insight into how people perceive the terms and conditions/privacy policies)*
- 5) **We are working on a browser extension that would summarize the terms and conditions of an app or website to tell you in easier terms if your data is protected. Would you use this?** *(This question directly helps with input on our future intervention, as community involvement is important)*
  - a) *Show picture: Do you understand what this is and should we edit it in any way?*

### Surveillance

- 6) **Do security cameras make you feel safer?** *(This question was added since we needed more insight on city technology that potentially made citizens uncomfortable)*
- 7) **What do you do to manage your privacy (either online or in-person) if at all? Why?** *(This question was added since our question touches on this topic, however there was a lack of interview questions which directly add to the question.)*
- 8) **Do you think you have control over your privacy online and through surveillance cameras? Why?**  
*(This question was kept since it sums up how much agency the participant feels they have over their privacy as a whole, which directly touches on our research question.)*
- 9) **Any questions? comments? or concerns? Do you have anything else you want to share?** *(This question was kept to make sure everything that could have been said, has been said.)*



PRIVACY

17

**Demographics**

**10) What is your gender identity?**

**11) What is your race/ ethnicity?**

**12) What is your age?**

**APPENDIX D**

## Final Field Trip Two Protocol:

**Hook:** Hello we are [NAMES] and we are high school students doing a research program with Columbia focused on educating people about misconceptions and knowledge gaps within personal data that may be collected, used, and shared by mobile applications and AI. Do you have 10 minutes for us to ask a few questions?

**Beginning of the interview:** You are allowed to skip any questions you don't feel comfortable sharing or opt out of this interview at any time. Also, do you consent to being recorded? Your information will be anonymous.

**1) What do you think the internet knows about you?**

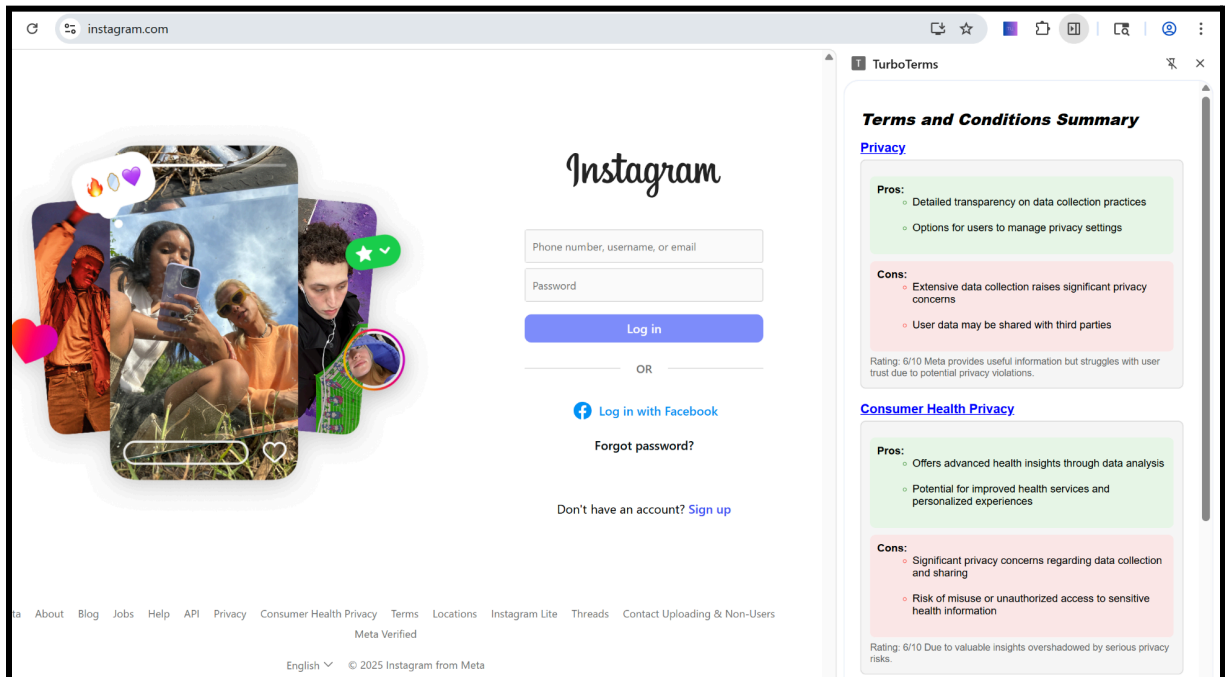
**2) Have you ever used AI(artificial intelligence) such as ChatGPT or Google AI? Why or why not?**

**3) Would you tell an AI a secret? Why or why not?**

**4) Do you read the terms and conditions policy when you download an app or use a website and if so why? Or why not?**

**5) We are working on a browser extension that would summarize the terms and conditions of an app or website to tell you in easier terms if your data is protected. Would you use this? (*printed picture of extension shown below*)**

***Photo Shown to Participants:***



**6) Do security cameras make you feel safer?**

**7) What do you do to manage your privacy (either online or in-person) if at all? Why?**

**8) Do you think you have control over your privacy online and through surveillance cameras? Why?**

**9) Any questions? comments? or concerns? Do you have anything else you want to share?**

**Demographics**

**10) What is your gender identity?**

**11) What is your race/ ethnicity?**

**12) What is your age?**

**Under 18 / 18-29 / 30-45 / 46-64 / 65+**