# Analysis of Public Perception of Covert Email Tracking

Melanie Chow
*The University of Chicago*

Troy Hu
*The University of Chicago*

Madeline Kim
*The University of Chicago*

Lindsey Ma
*The University of Chicago*

John Schlaak
*The University of Chicago*

Eli Tran-Johnson
*The University of Chicago*

## Abstract

Email tracking is widely used by companies as a means of refining advertisement, informing analytics, and measuring consumer engagement with emails sent to consumers, often without knowledge or consent from the consumer. Previous studies have examined the technical aspects of email tracking, but the research into user perceptions and mental models of email tracking and its privacy implications is currently scarce. In this study, we focused our investigation on user awareness of email tracking and their opinions on the practice of email tracking. We conducted a pilot study and found that most participants were unaware of email tracking, and those that were aware had incorrect or incomplete mental models. Opinions on acceptable email tracking were mostly united in that potentially sensitive data, such as approximate location, were inappropriate to collect, while other information, such as when emails are opened and browser information, received less opposition. Participant reception to email tracking was more favorable in marketing contexts than in others and could be appropriate with some form of consent. Further research in this domain can better inform policies and design principles that equilibrate marketing innovation with privacy and security protection for the consumer.

## 1 Introduction

Email tracking is the practice of using web surveillance techniques in order to gain information about users' email reading behavior, usually surreptitiously and without user knowledge or consent [1, 2]. Marketers, spammers, and hackers, for example, may use email tracking in order to detect when a specific user reads an email, how often they read it, the device(s) they use to read it, and the IP address from which they read it. All of this information is tied to the email address of the recipient, and combined with secondary information and log analysis, this allows senders to create detailed profiles of specific users' behaviors.

There are two primary techniques for implementing email tracking: pixel tracking and link tracking [1]. Pixel tracking takes advantage of the capabilities of HTML formatting in emails. Most email clients will automatically render HTML emails, which allows senders to embed images. The pixel beacon is a small transparent image, usually only 1x1 pixels. The image is stored on a web server associated with the sender, then a sender embeds the image by including a reference URL to the image in the HTML of the email [3]. When the user opens the email to read it, their mail client must send a request to the web server to fetch the image, and that access is logged by the webserver. The sender can later analyze the web server logs to deduce the recipient's behaviors. Pixel tracking does not require any additional user interaction beyond opening and reading the email in which the pixel is embedded, and the pixels are difficult to visually detect because they are tiny and transparent. Furthermore, senders may embed multiple pixel beacons from one or more trusted third parties, effectively allowing any number of parties to collect and analyze the resulting data.

The second technique, link tracking, requires the user to click on a link in the HTML of an email [1]. The link will be unique to the user, so when the user clicks on it the sender will know the user is reading the emails they have sent and has engaged with their contents. This tracking technique is slightly more visible to the user; should they hover over the link, the full URL will be displayed by the browser, and links with long strings of random characters that make the link unique are visually distinctive.

Although web tracking has been the subject of many user studies, academic literature concerning user perceptions of email tracking in particular is scarce [4]. Most papers on email tracking are concerned with the technical aspects of implementation, detection, efficacy, forensic applications, and countermeasures. However, even if a user is aware of web tracking embedded in the web sites they visit, they may not be aware that trackers are also in emails. Email tracking also poses a different privacy risk than general web tracking because the information gained from email tracking is tied to the user's email address, a near-unique identifier for the user [2]. If the user reads an email from multiple devices, senders

can also link information about that user's behavior across devices [1]. The tracking is difficult to block without disabling HTML rendering for emails, which is extremely inconvenient to users who cannot mentally render HTML from plain text in their heads. It is therefore important to gain insights on user perceptions of email tracking and its security and privacy implications.

## 2 Related Work

Prior work on email tracking, online advertising, and participants' perception of advertising provided us with background and motivation for this study. We expand on prior work by combining the three topics above and examining user interaction with and perceptions of email tracking.

### 2.1 Email Tracking Background and Prevention

Research into the technical aspects of email tracking is already abundant, evidenced in part by the many patents filed for technology designed to aid and/or prevent email tracking. There have also been several studies about how to automatically detect email tracking. Pixel-beacon-based analytics constitute a patented technology originally from 2006 for use on websites [5]. Although those tools are intended for use on a standard webpage rather than in an email, such an implementation demonstrates the robustness of pixel tracking systems. Another exemplary demonstration of pixel tracking is embodied by a patented technology originally from 2010 for monitoring the email and website behavior of an email recipient [3]. This technology is email-based and expands on the capabilities of traditional pixel tracking by also establishing a cookie to track the client's website usage.

As previously mentioned, patents have also been registered for the purpose of hindering email tracking. One such patented technology originally from 2005 functions by spoofing an email address to a pixel beacon to trick the tracker into thinking that the fabricated email address is a genuine address from which the recipient has viewed the email [6]. All three of the aforementioned technologies are more than a decade old, but they illustrate the functionality and potential power of email tracking quite well. It is apparent from the intensity of ongoing research to prevent email tracking that this technology is still powerful and pervasive enough to constitute a threat to users' privacy and security. One paper from 2018 focuses on identifying pixel trackers on traditional websites and evaluating the efficacy of various tools for blocking them [7]. While this paper is focused on pixel beacons in general rather than specifically within emails, the authors nonetheless elucidate the power and functionality of this technology. Another paper from 2018 proposes a system for the identification of emails which contain tracking mechanisms via the use of machine learning [8]. It suggests that this tool could be used for a more robust piece of software that would also block those emails once they were identified.

### 2.2 Advertisers and Email Tracking Overview

Web and email tracking are primarily used for targeted/behavioral advertising, which provides the advertiser with the benefits of creating personalized ads that may be more appealing to target customers and the consumer with increased accessibility to web content or newspapers subsidized by ad revenue [9–11]. Third party-services allow the primary websites with which users interact to integrate services such as advertising, analytics, and interactions with social networking sites, but they also introduce privacy concerns through their tendency to track users beyond the primary site they first encountered. Previous studies show that users consistently object to third parties collecting personal data from their browsing history. The policy debate surrounding the privacy and security issues raised by third party web tracking covers effects on the user that can range from discomfort from the feeling of being monitored to physical, psychological, and/or economic harm if the data collected is exploited by a bad actor [12].

Third parties are able to collect from browsing history what a user might classify as very personal data, such as location, financial situation, medical conditions, and employment status. Third party websites can collect these data through several means. A third-party can act as a first-party, such as Facebook, which identifies users in third-party social widgets on its platform to personalize them. Some first-party websites sell identifying information on users to third parties through voluntary 'leaks', which advertisers use to provide more targeted advertising. First parties can also unintentionally provide third parties with identifying information in the URL or page title. Vulnerabilities on a first-party website can also be exploited to gather personal information on a user. Even if a user's browsing history is not itself sufficient to identify a user, the data collected can be matched against a database to re-identify the user [9, 12].

Concerns over user security and privacy have inspired policy designed to protect consumers from potential threats posed by the collection and usage of identifying or sensitive data. The Federal Trade Commission (FTC) has been trying to strike a balance between safeguarding user privacy in so much as to protect the user from harmful exploitation of their data, while allowing for product innovation and development, promulgating the following principles: transparency, consumer control, reasonable security, limited data retention, affirmative express consent from the consumer for any changes to privacy policy and for using sensitive data for behavioral advertising. Similarly, European Union members generally require that companies inform the user of their tracking technologies with clear instructions on how to opt out and that the tracking technologies are approved by the appropriate Data

Protection Authority and indicated in the website's privacy policy. Rules and guidance on use of pixels and beacons differ slightly between the U.S. and the European Union, but many of the underlying principles remain the same [10, 13]. One of the issues is that these policies may be difficult to enforce, particularly among third party websites, which tend to be invisible to the user [12]. It is important, therefore, that while innovative policy and protective technologies be developed to counter potential threats from bad actors, users also should be educated about the pervasive use and distribution of their personal data through their browser and email activity, which is the primary motivation for our study on user awareness of these issues.

### 2.3 User perceptions of Online Advertising Tracking

In the past few years, a number of studies have been conducted on users' perception of online behavioral advertising and online tracking. In 2016, Melicher et al. interviewed 35 participants and collected their browsing histories in an attempt to study the perceived benefits and risks of online tracking. The researchers found that participants' general attitudes towards tracking guided their comfort level in tracking situations. At the same time, participants based their tracking preferences/comfort level on specific contexts such as familiarity, control over tracking, and site topic [14]. In a 2012 interview study on 48 participants, Ur et al. found that participants were very concerned about advertising companies collecting their personal information. Participants in their study also had incorrect mental models of advertising networks and did not connect online tracking to such networks [15]. A usability/interview study by Thode et al. also found that cultural contexts may impact perceptions of online advertising tracking; their German participants seemed to be more skeptical and concerned of online tracking than the American participants in Ur et al. [16]. Finally, Agarwal et al.'s interview study on Indian subjects found that users were more significantly concerned about being shown embarrassing ads than third party tracking or OBAs [17]. This result indicates that tracking is not perceived by users to be the most important advertising related concern.

The studies we described above examined users' perceptions of tracking and information collection primarily in the topic of web browsing. However, none of them discussed perceptions of tracking with respect to emails and links in emails. Our study therefore builds upon prior research on online tracking by attempting to answer similar research questions about tracking in the area of emails and email links. Another difference between our study and prior studies is that our study considers tracking with respect to both privacy AND security. The studies above primarily focused on tracking with respect to advertisers. As a result, the researchers above were concerned with users' privacy and their perception of privacy. While advertisers can use email links to track people online, malicious parties (such as phishers) can also benefit from email tracking links.

## 3 Research Questions and Hypothesis

Our overarching research question is how the general public perceives email tracking, refined through several specific research questions:

1. What do people know about email tracking, if anything?
2. Can people identify tracked emails? How do they know?
3. In turn, do people know what kind of information the link senders get when they embed tracking pixels and/or tracked links? Essentially, what mental models do people have of email/link tracking?
4. What are people's opinions of email tracking and possible countermeasures? Sub Questions:
   (a) Do people they think email tracking is useful, fair/unfair? Why or why not?
   (b) Do people think that blocking tools are effective? Why or why not?
   (c) Do people view email tracking as a convenience vs. privacy tradeoff?
5. Do perceptions of email tracking vary by context? The contexts we consider are:
   (a) Demographic contexts such as education level and gender.
   (b) Email types such as work/institutional email and personal email.
   (c) The type of people who send links such as marketers and hackers.

We hypothesize that most of the general public is not aware of what email tracking is, and that those that do, as well as those who are made aware over the course of this study, will perceive email tracking negatively and as an invasion of privacy.

## 4 Methodology

### 4.1 Overview

We conducted an initial pilot study with 2 UChicago students, followed by a second pilot study of 6 participants, which we describe in this paper. Participants recruited for the study completed a pre-screening survey to determine their eligibility. We randomly selected 6 of those who completed the pre-screening and returned consent forms and captured their perception of

email tracking by conducting a semi-structured interviews, one-on-one, with each subject. The semi-structured interview included a hands-on activity within the discussion of email usage, awareness of tracking, and opinions on tracking and consent. For the hands on portion, we sent the participants emails with tracking links and/or pixels, which they would try to determine if they were tracked and voice their reasoning to the interviewer.

## 4.2 Human Subjects and Ethics

Our institution's review board (IRB) approved this study before any research on participants was conducted. Before the interview, we obtained both verbal and written consent from participants to ask them questions about email tracking and to being audio recorded. We only recorded participants' responses and left out any identifiable information. Moreover, audio and notes were only seen by the researchers in this study and stored in an encrypted disk, to be deleted after the completion of the study.

## 4.3 Recruitment and pre-screening Survey

Potential participants were directed to contact the researchers through email and were sent a pre-screening survey to determine their eligibility. This pre-screening survey consisted of a combination of multiple choice and free-form questions on Qualtrics and ensured that the participants we interviewed regularly used email, received at least some marketing and/or spam email in order to provide adequate responses to our research questions, and met these other requirements:

- Be older than 18 years old.
- Be able to send and receive emails.
- Have at least 30 minutes of free time.
- Be able to communicate in English.

Those who met the eligibility requirements and continued on to the interview completed consent forms to participate and to be audio-recorded during the interview. As compensation, we offered those who completed all steps up to and including the interview and hands-on portion a $10 Amazon gift card.

## 4.4 Technical Details

We configured an email tracking server using Postfix[1] and GoPhish. GoPhish[2] is an open-source phishing framework built for internal phishing training. We chose GoPhish because it is lightweight, easy to install and configure, and comes with pixel- and link-tracking by default. It does not ship with any malicious content; email campaign templates and landing pages are configured by the end-user. Its web interface displays and updates results such as email opens, clicked links, and associated GET request information in real time.

The email tracking server was configured to use HTTPS for hosting all pixel beacons and landing pages with a TLS certificate from LetsEncrypt[3]. We only sent tracked emails to participants during the hands-on portion of the interview. No other study-related communications were sent from the email tracking server.

## 4.5 Interview Procedure

All interviews with participants were held in Joseph Regenstein Library or John Crerar Library group study rooms at the University of Chicago (UChicago). We placed a sign on the door asking students not to disturb to reduce the likelihood of an unexpected intruder. We also reserved rooms where participants were able to sit out of view from the doors and/or windows to maintain privacy. The interviews were conducted in an informal, but structured manner. The interviewer had a set of questions to guide the conversation, but the tone was kept casual to keep the participant at ease.

We initially followed up on the pre-screening with questions about participants' email usage. Such questions were asked in order to define the contexts in which participants use email. We then had participants complete the hands-on portion. We sent users 4 emails with/without tracking links or pixels: HTML formatting + tracked link + image + pixel, HTML formatting + image + pixel, HTML formatting + pixel, and plain-text with no pixel. For each email, we asked participants whether that email could track them. Given their response, we asked why (i.e. what part of the email led you to come to this conclusion?). After completing the hands-on portion, participants were asked about their perceptions and opinions of email tracking. There were 3 main topics that we touched upon (with two example questions for each topic):

1. Assessment of Awareness/Technical Knowledge. That is, we asked participants what they knew about tracking.
   - "Before coming in, were you aware that how you interact with your emails–whether you've opened them or clicked on any of the links–could be tracked?"
   - "What steps would you take to prevent an outside party from tracking your interactions with an email message?"
2. Opinions on Tracking. We asked participants what they felt and thought about email tracking.
   - "How would you feel in general about some outside party monitoring your activity on the emails they send you this way?"

[1] http://www.postfix.org/
[2] https://getgophish.com/
[3] https://letsencrypt.org/

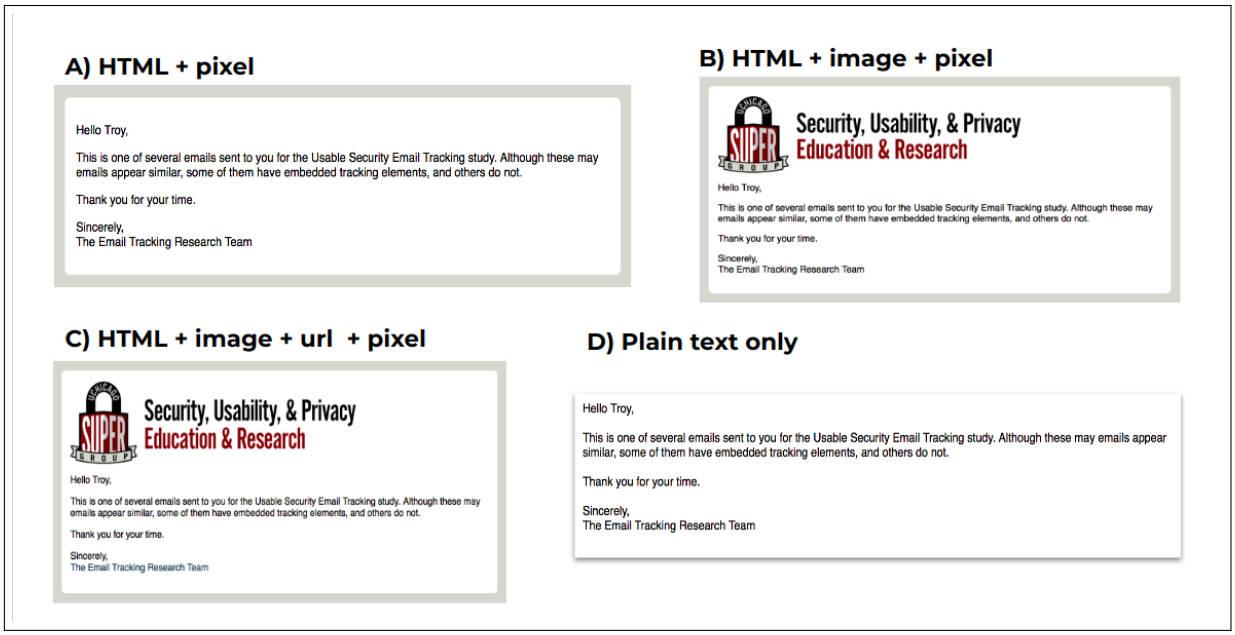


Figure 1: The four emails sent to participants during the hands-on activity.

- "What about for school or for work? Do you make a distinction between when it happens with personal or professional emails?"

3. Consent to Tracking. Finally, we asked what they felt about current consent practices among email trackers.
   - "Do you feel that companies should obtain consent before they track consumers?"
   - "Are there contexts where you do not feel consent would be necessary?"

After the interview was complete, participants were asked to complete a demographic survey, after which they were compensated for their time. Each question in this survey concerning race or gender offered a "Prefer not to answer" option. Upon completion of the study, we deleted all participant data, including those stored on the server purposed for this study on GoPhish, such as server logs and exported campaign files.

# 5 Results

## 5.1 Participant Awareness and Mental Models of Email Tracking

Our participants had varied backgrounds in familiarity with email tracking. Four of our six participants did not know anything about email tracking. The other two participants described either incomplete or incorrect mental models.

When asked to describe their mental models of email tracking pixels, only 2 participants were able to explain their mental models. The other participants either said they were entirely unaware of tracking pixels, or did not know enough about them to describe a mental model.

Participant 5 was aware that email tracking existed, because she has friends who use tools to block email tracking. She did not know any further details about email tracking, but she explained that she associated email tracking with whether an email is personal or not. She thought that personal emails were more likely to be tracked, but not impersonal emails like marketing emails.

Participant 3 was aware of email tracking and explained a mental model that consisted of the frontend and the backend of the email. She thought that email tracking was accomplished by attaching an unspecified tracker to the backend of the email that was not visible to the reader, who only sees the frontend of the email. She thought that this tracker could detect whether or not the email was opened and whether or not the links within it were clicked.

## 5.2 Participants' Ability to Identify Tracked Emails

When participants were shown 4 different emails and asked to identify which of these emails were tracked, none of the participants were able to correctly identify and explain a complete mental model for all four of the emails.

Five of our six participants associated images with tracking. Four of these five participants thought that if an email had an image in it, it was tracked. The other participant that associated images with tracking (Participant 5) thought that images were a sign that an email is not tracked. It follows that Participant 5 was the only participant who thought the plain-

| | Demographics | | | Email Habits | |
|---|---|---|---|---|---|
| Participant # | Gender | Age | Race | Frequency of Receiving Solicited Marketing Emails | Frequency of Receiving Unsolicited Marketing Emails |
| 1 | Female | 18-24 | Asian | Daily | Never |
| 2 | Female | 18-24 | Asian | More than once per day | More than once per day |
| 3 | Female | 18-24 | White | Several times per week | Several times per week |
| 4 | Female | 18-24 | White, Hispanic | More than once per day | Once per week |
| 5 | Female | 18-24 | Asian | Daily | Several times per week |
| 6 | Female | 18-24 | African American | More than once per day | Once per month |

Figure 2: Selected results from the pre-screening and demographics surveys.

text email was tracked, whereas all of the other participants thought the plaintext email was not tracked.

### 5.3 Participants' Opinions on Consent

Participants' responses to learning about the functionality of email tracking (or, in many cases, to learning about its existence) ranged from shocked and upset to fairly ambivalent. Participant 4 was very surprised and bothered to learn that email tracking was taking place without people's consent, whereas Participant 6 had not known about email tracking, but was not at all surprised to learn that it was happening. Participants generally expressed that they thought some form of consent should be obtained. Participants 1 and 4 both indicated that marketers should at least disclose to consumers that their emails are tracked, though Participant 1 expressed a sentiment shared by Participants 2, 3, and 6 that companies should explicitly ask consumers for consent when they sign up for an email campaign. Participant 5 did not think that companies should have to disclose tracking or obtain consent, saying, "I feel like nobody really notices. I feel like the more data they have, the better for everyone." No participants thought that companies asking for consent would affect the efficacy of their data collection or consumer engagement.

### 5.4 Participants' Opinions on What Data Companies Can Track

Participants had a variety of opinions about what data companies should be allowed to retrieve through email tracking. Participants generally expressed that companies should not collect more information than what they needed. Participant 6 said that she thought consumers should be able to choose what data they shared with companies. Participants were consistently opposed to the collection of location data and IP addresses; Participant 3 was the least opposed, stating that she would be okay with the collection of location data if it was exclusively used for marketing purposes and nothing else. Participants' opinions about the collection of other data varied more. Most participants were fairly ambivalent about the tracking of information like email addresses, whether and when the emails were opened, and whether links were clicked. Participant 6 expressed that she would prefer no data were collected at all, but that she could understand why collecting whether the email was opened might be useful for companies.

### 5.5 Participants' Opinions on Context

An overarching theme in the opinions of all of the participants was context. All of our participants thought that some form of tracking was okay depending on what data was being tracked, and what the purpose of obtaining the tracked information is.

All of our participants mentioned email tracking in the context of marketing emails. Five of the six participants expressed that marketing was the only context in which email tracking should occur. The other participant (Participant 6) thought that email tracking was "bad in all contexts." Three participants also explicitly expressed that tracking should not occur in either personal or professional contexts. Participant 3 thought that it would be a larger invasion of privacy for friends or employees to track emails than for marketing companies to track emails.

In terms of context, many of our participants also mentioned intent. All of the participants who thought marketing emails were okay also said that it would be okay for a company to track their email campaigns, but the information should not be used for any other purpose.

# 6 Discussion

## 6.1 Limitation: Email provider and client interactions

Different email provider services and email client programs have various security and privacy measures that either block or mitigate pixel tracking. This means any information about whether an email was opened may be inaccurate.

### 6.1.1 Gmail

In December 2013, Gmail rolled out its Google Image Proxy feature in order to allow users to securely display all embedded images in emails by default [18]. Gmail users who open emails on the Gmail web application (https://gmail.com) or through the official iOS and Android apps load embedded images through Google Image Proxy. When the user opens an email, the Image Proxy issues a GET request to the tracking server for the pixel beacon, thereby obscuring the user's IP address and user-agent string. This effectively prevents pixel tracking from collecting geolocation, forward, print, operating system, device, browser, and application information from emails read in the official Gmail apps or the web application[19]. Exceptions to image proxying are only available to G Suite administrators, who may whitelist image URLs [20].

Although the Image Proxy cached images for the first months after its roll out [19, 21, 22], it respects no-cache headers as of early 2014 [23]. This means emails opened multiple times will load the pixel beacon multiple times, giving trackers information about how when and how many times an email was opened.

The Google Image Proxy identifies itself in its user agent string, with the client IP address in Mountain View, California.

```
"user-agent"":""Mozilla/5.0 (Windows NT 5.1;
 ↪ rv:11.0) Gecko Firefox/11.0 (via ggpht.com
 ↪ GoogleImageProxy)"
```

### 6.1.2 Yahoo! Mail

Yahoo! Mail implemented an image proxy service similar to Gmail's in 2018, called Yahoo Mail Proxy. Similar to Google Image Proxy, images are only proxied for emails opened in the Yahoo web application (https://mail.yahoo.com) and the official iOS and Android apps [24]. Email marketers have reported that in addition to proxying, the Yahoo mail proxy also caches images, so tracking can only capture unique email opens [25]. The image proxy identifies itself in its user string.

```
"user-agent"":" "YahooMailProxy;
 ↪ https://help.yahoo.com/kb/yahoo-mail-
 ↪ proxy-SLN28749.html"
```

### 6.1.3 Other providers

The following providers do not appear to proxy, pre-fetch, or otherwise interfere with embedded images in emails in their respective web, desktop, or mobile applications. With the exception of ProtonMail, they also load embedded images by default.

- Outlook (https://outlook.com)
- FastMail (https://www.fastmail.com/)
- Yandex (https://mail.yandex.com/)
- ProtonMail (https://protonmail.com/)

## 6.2 Other Limitations

Our participant sample consisted entirely of females, which may biased our results. Future studies should seek to recruit a more representative gender sample. During recruiting, participants were made aware that the study was about email tracking. The participants also learned at the beginning of the interview knew that emails could be tracked. In response to these two limitations, participants may have changed their mental models or opinions of email tracking. Our study also lacked ecological validity in that we did not use deception for the hands-on portion. Email content and subject lines weren't made to "blend in" or meant to attract participants' attention enough to click of their own volition.

## 6.3 Lessons Learned and Future Directions

One of the primary limitations of our pilot study was the limited external validity of our results. As all of our participants were female UChicago undergraduate students, our study sample is likely not generalizable to the rest of the UChicago undergraduate student body, let alone a more general population. Limited resources constrained our ability to expand the scope of our recruitment for interviewees beyond the UChicago campus. Our participants were enlisted primarily through Facebook posts with our flyers to undergraduate class pages, though the gender composition of our sample pool may have been due to chance. In follow-up studies, we will seek to achieve greater diversity among recruited undergraduates. We would post flyers on the UChicago campus at the following locations: undergraduate dormitories (Max Palevsky Commons, Burton-Judson Commons, Campus North and Renée Granville-Grossman Commons), libraries (Regenstein Library, Crerar Library). To attract non-undergraduates, we would post flyers, academic buildings (Biological Sciences Learning Center, Ryerson, Kent, Harper Memorial Library, Cobb Hall, Saieh Hall, and Stuart Hall) to inform potential participants about our study, as well as email the flyer to a variety of academic and extra-curricular list-hosts. Individuals who are not part of the UChicago community may potentially

be reached on other platforms, such as Craigslist, or flyers posted in public spaces around Hyde Park.

While we could only recruit a limited number of subjects for our interviews, the hands-on portion could potentially be performed independently from the interview, followed by an online survey. Such a design allows for the recruitment of many more participants on large platforms such as Amazon Turk, with a greater likelihood for capturing a more generalizable sample. The separation of the interview and hands-on portion also eliminates potential confounds introduced by these two activities into each other's results. During our second-round pilot study, we found that the hands-on section may have produced a learning effect during the interview section, where participants may have modified their answers to interview questions based on information they gathered from the hands-on activity. One solution could be to move the hands-on activity after the assessment of the participants' technical knowledge; however, the interview questions could in turn influence participant responses during the hands-on activity. It may be best, therefore, to conduct these two activities separately with two independent samples.

A learning effect may have also occurred during the hands-on portion itself, where some participants seemed to change or base their answers on previous emails they had seen. The emails were very similar in design, which may have contributed to the learning effect. While the emails could be redesigned to no longer resemble each other or to show a pattern, doing so would introduce an additional confound. These issues could be mitigated or eliminated altogether by sending participants only one or two of the four emails, in which case, it would be ideal to recruit many more participants, possibly through an aforementioned mass-recruitment platform such as MTurk or Prolific.

Additionally, some of our interview questions hindered effective communication with our participants. Some questions were too long, some questions were worded badly, and some questions were confusing. For instance, question C from section VI of the interview (see appendix for interview script) asked participants if they felt that "the efficacy of the company's outreach would be affected by waiting to obtain consumers' consent, as opposed to paper mail, where companies would not be able to obtain information about the response of the consumer." We noticed that participants were confused by the wording of this question, and that its sheer length made it too hard to follow. We intended to ask participants if they felt that asking for consent would reduce the effectiveness of consumer engagement for companies. We therefore propose an improved question: "If a company first has to ask for consent to collect data, do you think this reduces consumer engagement?" However, we ultimately believe that we should remove this question, because not only is it irrelevant to our research question, but also because it does not provide any meaningful answers. The question ultimately asks users to evaluate the effectiveness of a marketing strategy from a business's point of view. Any answer would effectively be baseless and useless unless the participant was in the marketing industry, and were talking in the scope of a specific type of company.

When conducting our interviews, we also noticed that some questions were either redundant, or were useless based on the individual's response. For instance, we asked users how they think emails are tracked, as well as their opinion on email tracking, even if the individual did not know email tracking existed (which was the case for most of our participants). These questions are poorly ordered because if a user does not know that email tracking exists, it may be hard to get a nuanced opinion of email tracking, as well as an educated response to how email tracking works. As a result, we can improve our interview script by only asking certain questions, or by slightly changing the question wording based on previous responses, such as asking "Based on what you just learned about email tracking, could you tell us more about your initial thoughts?" if users did not know email tracking existed. Additionally, we noted that our questions may be biased/leading due to the negative connotations with "tracking," in email tracking, as opposed to a more positively worded "data analytics" or "data driven engagement." It may therefore be helpful to also test out different wordings with a study to see if we get different results or opinions, which is discussed in more detail later.

Lastly, the study could further be improved by editing our interview questions to account for a larger sample size–such as making our questions easier to code for. Since we had a pilot study with 6 participants, we did not code their responses due to the inability to draw (and infer) universal patterns. It was also difficult to code these items due to the nature of our questions, as almost all of the questions were open ended. Therefore, it might be helpful to also run a small study on our questions and ask participants if they believe a question can be answered in a yes-or-no question. For instance, we simply gave participants a list of information that could be obtained through email tracking. Given that we want to explore user's mental models, this may be improved by asking a series of yes-or-no questions, such as if a participant thinks location can be detected through email tracking, if browser model can be detected, etc. This is an improvement as it allows us to see what participants think could be detected based on his or her mental model of email tracking. In summary, an interview model facilitating more simplified, streamlined answers from participants would by easier to code and would yield clearer results to address our research questions.

Although we had an initial pilot study with two participants to test our questions, we did not have enough time and resources to iterate and improve our questions further. Especially as we refined our research questions and made improvements, it would have been nice to test our questions again. Therefore, in the future we can improve our questions by recruiting participants solely for refining the questions. More specifically, we can ask these participants to read the

questions, and tell us what they think each question means. We can try seeing if our question wording "led" participants to a certain response by asking different participants questions with different leadings (eg. email tracking vs data analytics) and seeing if that dramatically affected response or opinion. In addition, we can also ask if anything, or any word (eg. efficacy), was unclear or ambiguous.

## 7 Conclusion

We conducted a pilot study on user perceptions of email tracking due to the current lack of literature on the topic. We found that although web tracking has been explored in many user studies, research on email tracking, especially on user perceptions, is scarce. We believe that user perceptions on email tracking is important to explore because it introduces privacy risks that are different from other forms of tracking. Since email tracking is difficult to disable and difficult to definitively detect, email tracking raises the question of whether individuals can adequately give informed consent, and if users can opt-out. We therefore ran a pilot study in order to explore the feasibility of our methods in evaluating user perceptions on email tracking. We ran this study with 6 participants, and found that most participants had little to no awareness or understanding of email tracking, but that participants generally did have issues with sensitive data being collected without their consent, such as location. We also found that participants were more open to their data being tracked in marketing contexts than in others, such as professional contexts, but still felt that it was important for companies to disclose whether they were tracking emails. From this pilot study, it seems apparent that consumers have little awareness about the widespread practice of email tracking, although they have strong opinions about the ethics of it. Further research in this area could confirm this trend and potentially inform marketing companies or policymakers on future decision making in the realm of email tracking.

## References


[1] B. Bender, B. Fabian, S. Lessmann, and J. Haupt, "E-mail tracking: Status quo and novel countermeasures," *ICIS 2016 Proceedings*, Dec. 11, 2016.

[2] D. Martin, H. Wu, and A. Alsaid, "Hidden surveillance by web sites: Web bugs in contemporary use," *Commun. ACM*, vol. 46, no. 12, pp. 258–264, Dec. 2003, ISSN: 0001-0782. DOI: 10.1145/953460.953509.

[3] A. Knox, L. Knox, and J. Hart, "Method and system for monitoring email and website behavior of an email recipient," U.S. Patent 7680892B2, Mar. 16, 2010.

[4] Ermakova, Tatiana, Fabian, Benjamin, Bender, Benedict, Klimek, and Kerstin, "Web tracking - a literature review on the state of research," *Handle Proxy*, Jan. 2018.

[5] C. Wong and B. M. Error, "Multi-party web-beacon-based analytics," U.S. Patent 8365150B2, Jan. 29, 2013.

[6] G. Khalsa and D. Morss, "Method and apparatus for simulating end user responses to spam email messages," U.S. Patent 8874658B1, Oct. 28, 2014.

[7] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Tracking the pixels: Detecting web trackers via analyzing invisible pixels," *CoRR*, vol. abs/1812.01514, 2018. arXiv: 1812.01514.

[8] J. Haupt, B. Bender, B. Fabian, and S. Lessmann, "Robust identification of email tracking: A machine learning approach," *European Journal of Operational Research*, vol. 271, no. 1, pp. 341–356, 2018, ISSN: 0377-2217. DOI: https://doi.org/10.1016/j.ejor.2018.05.018.

[9] J. Estrada-Jiménez, J. Parra-Arnau, A. Rodríguez-Hoyos, and J. Forné, "Online advertising: Analysis of privacy threats and protection approaches," *Computer Communications*, vol. 100, pp. 32–51, 2017, ISSN: 0140-3664. DOI: https://doi.org/10.1016/j.comcom.2016.12.016.

[10] F. Gilbert, "Beacons, bugs, and pixel tags: Do you comply with the ftc behavioral marketing principles and foreign law requirements?.," *Journal of Internet Law*, vol. 11, no. 11, pp. 3–10, 2008, ISSN: 10942904.

[11] L. Lubbe and M. Oliver, "Beacons and their uses for digital forensics purposes," in *2015 Information Security for South Africa (ISSA)*, Aug. 2015, pp. 1–6. DOI: 10.1109/ISSA.2015.7335074.

[12] J. R. Mayer and J. C. Mitchell, "Third-party web tracking: Policy and technology," in *2012 IEEE Symposium on Security and Privacy*, May 2012, pp. 413–427. DOI: 10.1109/SP.2012.47.

[13] A. Esteve, "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA," *International Data Privacy Law*, vol. 7, no. 1, pp. 36–47, Mar. 2017, ISSN: 2044-3994. DOI: 10.1093/idpl/ipw026. eprint: http://oup.prod.sis.lan/idpl/article-pdf/7/1/36/14043496/ipw026.pdf.

[14] W. Melicher, M. Sharif, J. Tan, L. Bauer, M. Christodorescu, and P. G. Leon, "(do not) track me sometimes: Users' contextual preferences for web tracking," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 2, pp. 135–154, Apr. 1, 2016. DOI: 10.1515/popets-2016-0009.

[15] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, "Smart, useful, scary, creepy: Perceptions of online behavioral advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, Washington, D.C.: ACM, 2012, 4:1–4:15, ISBN: 978-1-4503-1532-6. DOI: 10.1145/2335356.2335362.

[16] W. Thode, J. Griesbaum, and T. Mandl, ""i would have never allowed it": User perception of third-party tracking and implications for display advertising," in *ISI*, 2015.

[17] L. Agarwal, N. Shrivastava, S. Jaiswal, and S. Panjwani, "Do not embarrass: Re-examining user concerns for online tracking and advertising," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13, Newcastle, United Kingdom: ACM, 2013, 8:1–8:13, ISBN: 978-1-4503-2319-2. DOI: 10.1145/2501604.2501612.

[18] J. Rae-Grant. (Dec. 12, 2013). Images now showing, Official Gmail Blog, [Online]. Available: https://gmail.googleblog.com/2013/12/images-now-showing.html (visited on 06/07/2019).

[19] (Jun. 4, 2014). How are gmail opens reported within email analytics? Help – Litmus, [Online]. Available: https://litmus.com/help/analytics/understanding-gmail-opens/ (visited on 06/07/2019).

[20] (). Set up an image URL proxy whitelist - g suite admin help, [Online]. Available: https://support.google.com/a/answer/3299041?hl=en (visited on 06/07/2019).

[21] R. Kulka. (Dec. 7, 2013). How gmail's image caching affects marketing and email tracking, E-Mail Marketing Tipps, [Online]. Available: https://www.emailmarketingtipps.de/2013/12/07/gmails-image-caching-affects-email-marketing-heal-opens-tracking/ (visited on 06/07/2019).

[22] S. Bauers. (Dec. 16, 2013). Cache busting gmail's new image caching, Red Ant, [Online]. Available: https://redant.com.au/how-we-do/cache-busting-gmail-new-image-caching/ (visited on 06/07/2019).

[23] M. Nutt. (Mar. 9, 2014). Real-time content and re-open tracking return to gmail | movable ink blog, MoveableInk, [Online]. Available: https://movableink.com/blog/real-time-content-and-re-open-tracking-return-to-gmail/ (visited on 06/07/2019).

[24] Z. Sheehan. (Mar. 19, 2018). How yahoo's image caching will impact your email marketing metrics, Return Path, [Online]. Available: https://blog.returnpath.com/how-yahoos-image-caching-will-impact-your-email-marketing-metrics/ (visited on 06/07/2019).

[25] B. Specht. (Mar. 12, 2018). Yahoo! mail introduces image caching—what marketers must know, Litmus Software, Inc. [Online]. Available: https://litmus.com/blog/yahoo-mail-introduces-image-caching-what-marketers-must-know (visited on 06/07/2019).

# A Appendix - Study Materials

# The University of Chicago

"What Do You Think Of Email Tracking?"

**Volunteer for a University of Chicago research study in which you can help us better understand perceptions of emails and tracking.**

Participants will take a prescreening survey about their email usage. Based on their survey responses, they will interviewed about their experiences with email and perceptions of email tracking. The prescreening survey will take 5-10 minutes and the interview will take 15-20 minutes.

If interviewed, participants will be compensated with a **$10 Amazon gift card** for their time.

To participate, you must:

- Be older than 18 years old
- Be able to send and receive emails
- Have at least 30 minutes of free time
- Be able to communicate in English

If you are interested in participating in this study, please follow this link to fill out the prescreening survey:

https://bit.ly/2Qh5BSc

**UNIVERSITY OF CHICAGO**
**CONSENT FORM FOR RESEARCH PARTICIPATION**

**Study Title: How does the general public perceive email tracking?**

**Principal Investigator: N/A**

**Student Researcher: John Schlaak, Madeline Kim, Melanie Chow, Lindsey Ma, Troy Hu, Eli Tran-Johnson**

**IRB Study Number: N/A**

We are students at the University of Chicago, in the Department of Computer Science. We are planning to conduct a research study, in which we invite you to take part. This form has important information about the reason for doing this study, what we will ask you to do if you decide to be in this study, and the way we would like to use information about you if you choose to be in the study.

**Why are you doing this study?**
You are being asked to participate in a research study about people's perceptions and knowledge of email tracking.
The purpose of the study is to describe the public perception of email tracking. We wish to learn what people already know about email tracking, whether they can identify tracked emails, and what information they think email senders can get from tracked emails.

**What will I do if I choose to be in this study?**
If receiving this form, you have been taken the pre-screening survey and are eligible to participate in the study. Before proceeding, we will need this consent form signed. If given consent, in the interview we will ask you questions about your perception of email tracking. As part of this procedure, we will send you a few sample emails, some of which are tracked by us. You will be asked to analyze the emails. We will also evaluate your email configurations and whether or not they are more prone to tracking or not. Apart from this hands-on portion of the interview, you will be asked several questions about your knowledge and opinions of email tracking, as well as its privacy implications. At the conclusion of the interview, we will erase any identifying data we received from tracking your emails. If you feel uncomfortable at any time during the interview process, you may terminate your participation in the study immediately. You will still be compensated for your time if you choose to do so.

**Study time:** Study participation will take approximately 20 to 30 minutes in one session.

**Study location:** All study procedures will take place at the Joseph Regenstein Library. Specifically, its upper level study rooms.

We would like to audio-record this interview to make sure that we remember accurately all the information you provide. We will keep these tapes in an encrypted disk and they will only be used by the researchers of this study. If you prefer not to be audio-recorded, we will take notes instead.

We may quote your remarks in presentations or articles resulting from this work. A pseudonym will be

used to protect your identity, unless you specifically request that you be identified by your true name.

**What are the possible risks or discomforts?**

To the best of our knowledge, the things you will be doing have no more risk of harm than you would experience in everyday life.

As with all research, there is a chance that confidentiality of the information we collect from you could be breached – we will take steps to minimize this risk, as discussed in more detail below in this form.

We will temporarily have possession of some information about user IP addresses, browser configurations, and other such data that could potentially constitute a privacy breach if people outside of our group got hold of it.

You may be uncomfortable with some of the questions and topics we will ask about. If you are uncomfortable, you are free to not answer or to skip to the next question.

**What are the possible benefits for me or others?**

Taking part in this research study may help you be more aware of email tracking--particularly that it exists, as well as ways to detect if you are being tracked. For us, we may be able to learn new things that will help others. For example, we may be able to help others prevent their emails from being tracked by exploring popular email configurations and tracking implications on user privacy and security.

**How will you protect the information you collect about me, and how will that information be shared?**

Results of this study may be used in publications and presentations. Your study data will be handled as confidentially as possible. If results of this study are published or presented, individual names and other personally identifiable information will not be used.

To minimize the risks to confidentiality, we will store all data in an encrypted disk, limit access to your information, and anonymize your information.

We may share the data we collect from you for use in future research studies or with other researchers – if we share the data that we collect about you, we will remove any information that could identify you before we share it.

If we think that you intend to harm yourself or others, we will notify the appropriate people with this information.

**Financial Information**

Participation in this study will involve no cost to you. You will be compensated at a rate of $12 per hour if interviewed.

**What are my rights as a research participant?**

Participation in this study is voluntary. You do not have to answer any question you do not want to

answer. If at any time and for any reason, you would prefer not to participate in this study, please feel free not to. If at any time you would like to stop participating, please tell me. We can take a break, stop and continue at a later date, or stop altogether. You may withdraw from this study at any time, and you will not be penalized in any way for deciding to stop participation.
If you decide to withdraw from this study, the researchers will ask you if the information already collected from you can be used.

**What if I am a University of Chicago student?**
You may choose not to participate or to stop your participation in this research at any time. This will not affect your compensation for the study, or your class standing or grades at University of Chicago.

**What if I am a University of Chicago employee?**
Your participation in this research is in no way a part of your university duties, and your refusal to participate will not in any way affect your compensation for the study, or employment with the university, or the benefits, privileges, or opportunities associated with your employment at University of Chicago.

**Who can I contact if I have questions or concerns about this research study?**
If you have questions, you are free to ask them now. If you have questions later, you may contact the researchers at usablesecurity@gmail.com.

If you have any questions about your rights as a participant in this research, you can contact the following office at the University of Chicago:

Social & Behavioral Sciences Institutional Review Board
University of Chicago
1155 E. 60th Street, Room 418
Chicago, IL 60637
Phone: (773) 834-7835
Email: sbs-irb@uchicago.edu

**Consent**
I have read this form and the research study has been explained to me. I have been given the opportunity to ask questions and my questions have been answered. If I have additional questions, I have been told whom to contact. I agree to participate in the research study described above and will receive a copy of this consent form.

**Optional Study Elements**

**Consent for use of contact information to be contacted about participation in other studies**
Initial one of the following to indicate your choice:
_____ (initial) I agree to allow the researchers to use my contact information collected during this study to contact me about participating in future research studies.
_____ (initial) I do not agree to allow the researchers to use my contact information collected during this study to contact me about participating in future research studies.

_____
Participant's Name (printed)

_____ _____
Participant's Signature Date

**Pre-Interview Screening**

Introduction: Thank you for your interest in our study! To determine your eligibility for the study, we ask that you complete this brief survey. Please answer each question truthfully and to the best of your ability--we are not looking for a specific set of answers in eligible participants--and we will contact you with next steps. Regardless of whether you are invited to participate, the information you share with us will be de-identified and will only used for the analyses of our study. We will not share your information with any entity not directly involved in the administration of this study.

1. Please enter your name (*required)
    a. Question type: free-form
2. Please enter your email address and/or daytime phone number (*required)
    a. Question type: free-form
3. Are you over 18? (*required)
    a. Yes
    b. No
4. Are you currently enrolled as student (undergraduate or graduate) at the University of Chicago? (*required)
    a. Yes
    b. No
5. You must be comfortable communicating in English in order to participate in this study. Please indicate that you meet this requirement:
    a. I understand, and I am proficient in English (listening, speaking, reading)

***These questions apply to your use of email overall (i.e., including all email accounts), not any specific email account you may own.

6. Do you use email as a form of communication? (*required)
    a. Yes
    b. No
7. How often do you use email (receiving and sending)? (*required)
    a. Never
    b. Once per month
    c. Once per week
    d. Several times per week, but not daily
    e. Daily
    f. More than once per day
8. Do you receive marketing emails? (*required)
    a. Yes
    b. No
9. How frequently do you receive marketing emails? (*required)
    a. Never
    b. Once per month
    c. Once per week

    d. Several times per week, but not daily
    e. Daily
    f. More than once per day
10. Do you receive marketing emails from senders that you do not recognise/have never interacted with before? (*required)
    a. Yes
    b. No
11. How frequently do you receive these unsolicited marketing emails? (*required)
    a. Never
    b. Once per month
    c. Once per week
    d. Several times per week, but not daily
    e. Daily
    f. More than once per day
12. Do you receive spam emails? (*required)
    a. Yes
    b. No
13. How frequently do you receive spam emails? (*required)
    a. Never
    b. Once per month
    c. Once per week
    d. Several times per week, but not daily
    e. Daily
    f. More than once per day

Message upon completion: Thank for completing this survey. We will reach out to you shortly from usablestudy@gmail.com. Feel free to use this email address to contact us with questions and concerns.

**Interview Questions**

Interview Type: Semi-Structured Interview
Estimated Time: 20 minutes, maximum 30 minutes
Location: Regenstein Group Study Room (TBD)

I. Introductions:
   A. Greet interviewee and thank them for coming in
   B. Introduce yourself
      1. I'm _____, and I'll be holding a brief 20 minute interview with you as part of a study we're conducting on campus.
   C. Give brief explanation of the purpose of the study:
      1. We are looking at how much people in general are aware of the tracking that occurs when they interact with their emails and their opinions on the use of tracking.

II. Email Usage (Pre-Screening Follow-Up)
   A. You said in your response to the pre-screening survey that you use your email <frequency given in survey>. Is this still true?
      1. Do you manage multiple accounts?
      2. Do you use these accounts for different contexts, like school, work, or personal use?
         a) Note these responses for future questions on privacy across contexts
      3. Does your usage of these accounts vary, or do you use them all about the same?
         a) Note these responses for future questions on privacy across contexts
   B. (If they receive marketing emails)
      1. In the pre-screening survey, you said that you receive marketing emails <frequency given in survey> and unsolicited marketing emails <frequency given in survey>. Is this still true?
      2. On which email account or accounts do you receive the most marketing emails?
      3. What do you normally do with these emails?
      4. (Allow for any clarifying questions and respond accordingly)

III. Hands-On Portion (Ask these set of questions for each email sent. Make sure to note which email you are asking about during the interview.)
   A. (Ask participant to open the emails we sent to them)
   B. Do you think this email is being tracked or not tracked?
   C. What about the email informed you about (answer from part B)?
      1. Ask: "Why?" for each aspect.

IV. Assessment of Awareness/Technical Knowledge
   A. Do you think that any of the emails you've received could track you?
   B. Do you know how your emails could be tracked?

1. If no: provide brief explanation of pixels and link tracking. Allow for clarifying questions.
    a) Pixel tracking: An image is embedded in the HTML of an email. It is usually small (1 px wide and 1px tall) and transparent so the user does not see it. The image is hosted by the sender's web server at a unique URL; when a user opens the email and loads the image, it must contact the web server to download the image. The web server logs information about the URL requested and the client who requested it.
    b) Link tracking: Links in the email are personalized by embedding additional information to make the link unique to the email (or the email address of the recipient). When a user clicks on personalized links, the web server logs information about the URL requested and the client who requested it.
    c) In both cases, web servers will store the requested URLs, IP addresses, timestamps, and user-agent strings (which give browser and operating system information). The URL can be correlated with the email/recipient in order to associate web server log information with recipient information.
    d) Graphic to aid explanation: https://www.ceralytics.com/wp-content/uploads/2018/10/how-email-tracking-works.jpg
2. If yes: probe for an explanation from the participant. Provide clarification when asked.

C. What steps would you take to prevent an outside party from tracking your interactions with an email message?

V. Opinions on Tracking
   A. How would you feel in general about some outside party monitoring your activity on the emails they send you this way?
   B. Some examples of information that could be obtained through tracking include IP address, email address, email client, browser, operating system, date and time email was opened, rough geographic location, whether the email was read and/or any links clicked; how much information would you find acceptable to be obtained if an outside party were to track you?
   C. Would you feel differently depending on who sent you the tracking email? For example, if it were an advertiser for a company you buy from online or a subscription service versus someone or some entity you haven't directly interacted with before?
   D. What about for school or for work? Do you make a distinction between when it happens with personal or professional emails?

VI. Consent to Tracking
   A. Do you feel that companies should obtain consent before they track consumers?
   B. Are there contexts where you do not feel consent would be necessary?
   C. Some companies may find that using email tracking is necessary to measure consumer engagement with their advertisement materials. Do you feel the efficacy of

the company's outreach would be affected by waiting to obtain consumers' consent, as opposed to paper mail, where companies would not be able to obtain information about the response of the consumer?

D. Do you feel that there could be a compromise between tracking for advertising or marketing purposes and consumer privacy?

Demographics Survey: http://uchicago.co1.qualtrics.com/jfe/form/SV_2mn8tS4VMTfaMrX

**Post-Interview Demographic Survey**
Survey distributed at: http://uchicago.co1.qualtrics.com/jfe/form/SV_2mn8tS4VMTfaMrX

Introduction: Thank you for participating in our study! As a final step, we ask that you complete this brief to aid us in better understanding patterns that may occur across various demographics. The information you share with us will be de-identified and will only used for the analyses of our study. We will not share your information with any entity not directly involved in the administration of this study.

1. Please enter your name (*required)
    a. Question type: free-form
2. Please enter your email address and/or daytime phone number (*required)
    a. Question type: free-form
3. Please select the age category that best describes you (*required)
    a. 18-24
    b. 25-34
    c. 35-44
    d. 45-54
    e. 55-64
    f. 65-74
    g. 75-84
    h. 85+
4. Please select the option that best describes the education level that you have reached (more information on each of the categories can be found at https://www.bls.gov/emp/documentation/nem-definitions.htm#education): (*required)
    a. No formal educational credential
    b. High school diploma or equivalent
    c. Some college, no degree (excludes currently working towards a college-level degree, in which case, select “High school diploma or equivalent”)
    d. Postsecondary nondegree award
    e. Associate’s degree
    f. Bachelor’s degree
    g. Master’s degree
    h. Doctoral or professional degree
5. Please select the gender identity that best describes you: (*required)
    a. Female
    b. Male
    c. Non-binary
    d. Other
        i. Free-form option
    e. I prefer not to answer
6. Do you identify as latino or hispanic? (*required)

    a. Yes
    b. No
    c. I prefer not to answer
7. Please select the racial identity or identities below that best describe you. These categories were drawn from the 1997 Office of Management and Budget (OMB) standards on race and ethnicity (*required)
    a. American Indian or Alaska Native *(a person having origins in any of the original peoples of North and South America (including Central America) and who maintains tribal affiliation or community attachment)*
    b. Asian *(a person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam)*
    c. Black or African American *(a person having origins in any of the Black racial groups of Africa)*
    d. Native Hawaiian or Other Pacific Islander *(a person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands)*
    e. White *(a person having origins in any of the original peoples of Europe, the Middle East, or North Africa)*
    f. I prefer not to answer

Message upon completion: Thank for completing this survey and for participating in our study. Feel free to use this email address to contact us at usablestudy@gmail.com with any questions and concerns.