The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google

Ehsan Ul Haque
ehsan.ul_haque@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Mohammad Maifi Hasan Khan
maifi.khan@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

Md Abdullah Al Fahim
md.fahim@uconn.edu
University of Connecticut
Storrs, Connecticut, United States

ABSTRACT

This paper investigates how trust towards service providers and the adoption of privacy controls belonging to two specific purposes (control over "sharing" vs. "usage" of data) vary based on users' technical literacy. Towards that, we chose Google as the context and conducted an online survey across 209 Google users. Our results suggest that integrity and benevolence perceptions toward Google are significantly lower among technical participants than non-technical participants. While trust perceptions differ between non-technical adopters and non-adopters of privacy controls, no such difference is found among the technical counterparts. Notably, among the non-technical participants, the direction of trust affecting privacy control adoption is observed to be reversed based on the purpose of the controls. Using qualitative analysis, we extract trust-enhancing and dampening factors contributing to users' trusting beliefs towards Google's protection of user privacy. The implications of our findings for the design and promotion of privacy controls are discussed in the paper.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; **Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

KEYWORDS

Privacy, Trust, Technical Literacy, Privacy Controls, Privacy Choices, Privacy Control Adoption

ACM Reference Format:
Ehsan Ul Haque, Mohammad Maifi Hasan Khan, and Md Abdullah Al Fahim. 2023. The Nuanced Nature of Trust and Privacy Control Adoption in the Context of Google. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/3544548.3581387

1 INTRODUCTION

In 2020, Google's reported revenue was $181.7 billion (USD), 80% of which came from advertising revenue of $146.9 billion (USD) [58]. Notably, Google reportedly has 4.3 billion users worldwide [58], and dominates the search engine market with a whopping 92% market share [64]. With an estimated 4.72 billion Internet users globally [60] and the rise of online marketing and shopping, not surprisingly, the tech companies are increasingly moving towards the Ad revenue-based business model that largely depends on the collection and monetization of user data [4, 17]. Recent years have observed an aggressive growth in data collection as an industry standard practice that has raised serious concerns over the protection of user data privacy [67, 77, 78]. To address these concerns, regulations such as California Consumer Protection Act (CCPA) [71], and General Data Protection Regulation (GDPR) [20] (along with a few others [21, 22]) have been put in place to protect consumer privacy by ensuring fair data collection and usage practices. One of the recommendations proposed by these policies is to require online service providers to offer privacy controls/choices to the users as a means to give them *control over data*, which is aimed at addressing the *lack of control* over personal information [10, 13].

While making privacy choices available serves the purpose of being compliant with the regulatory standards and allows users to personalize their privacy choices, prior research noted that choice architecture can be cleverly manipulated to shift users towards practices that primarily benefit data collection [2], and can influence users' trust towards the provider [61, 74]. For instance, consider the case of Social Networking Sites (SNS), where users are given privacy controls (i.e., disclosure settings) to restrict data sharing with a recipient pool. Nevertheless, despite the disclosure choices, data collection by the SNS providers remains unrestricted. In addition, once information is shared with the recipient pool, these privacy settings do not offer additional control over how the members of the recipient pool can use the shared information. Brandimarte et al. named these controls "Control over sharing of data" (i.e., "sharing" controls) and warned how these controls could mislead users by giving a false sense of *control over data.* Instead, they suggested that greater focus should be given to privacy controls that offer "Control over usage of data" (i.e., "usage" controls) where users can *truly* restrict how collected/shared data can be used [16].

In our study, we used Brandimarte et al.'s conceptualization of categorizing controls based on the underlying purpose of "sharing" vs. "usage". To understand the distinction between "sharing" vs. "usage" controls, one may ask, "Does using the privacy control impact/restrict how the service provider can use shared data?" If the answer to this question is either 'no' or 'not sure,' there is a high probability that the control falls under the "sharing" category. In Google's context, the service provider offers several privacy controls across its platforms. For example, the privacy control *Browser history* offers control over reviewing and deleting browsing history stored on local machines or across synced devices. Note that using

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581387

Google search or Chrome platform allows Google to collect and store users' activity data that can be used to target consumers by providing personalized advertisements or other personalized services. Therefore, even when a user clears browser history, it does not restrict Google from using user activity data for personalization. Instead, the control merely offers users an option to restrict data sharing with third parties (e.g., family members or friends who share a device or someone who uses a synced device and can access the browsing history). Hence, the control does not restrict Google's usage of collected data, indicating 'no' as the answer to the above question for the *Browser history* control. Therefore, it puts the control under the "sharing" category. On the other hand, the purpose of *Ad personalization* control is to restrict Google from using shared activity data to target its users with personalized advertisements, even after acknowledging that Google collects such data (e.g., browsing data). Thus, when *Ad personalization* control is used, it impacts how Google can use collected data, putting it under the "usage" category.

It is important to note that the distinction of "sharing" vs. "usage" can be hard to be perceived by the end-users and can potentially contribute to the company's growth by lowering users' privacy concerns alongside building trust [16, 61, 74]. Prior efforts noted that trust can help mitigate concerns over privacy by giving a sense of belief that a service provider is capable and willing to protect user data [18, 73]. Such a perception of "safety" can be facilitated by the provider's proactive initiative to offer privacy-elevating interventions such as privacy controls [74]. However, a large chunk of prior efforts examined privacy control adoption in the SNS context, where the controls fall under the "sharing" category (e.g., disclosure settings) [3, 13, 57]. Thus, a gap exists in the literature explaining how privacy controls' purpose of "sharing" vs. "usage" affects trust perception among adopters and non-adopters of the privacy controls. Moreover, while research focusing on trust-privacy phenomena underscores the importance of trust in protective privacy behavior, factors that make or break users' trust towards a service provider, especially regarding user privacy protection, remain unclear. In our work, the adoption behavior of the privacy controls is defined based on participants' reporting of the current settings of the privacy controls for their personal computers rather than relying on self-reported behavioral measurement. Participants who changed a particular privacy control's default to one of the other available options are defined as *adopters* of the particular privacy control. Otherwise, participants who reported keeping the default as their current setting are defined as *non-adopters* of the privacy control.

While trust has been broadly examined as an antecedent of privacy decision-making, it is not well understood how end-users' technical literacy relates to trust and privacy adoption behavior. In the literature, Malhotra et al. noted that the ability to control and manage privacy plays a vital role in overall privacy decision-making [47]. Moreover, Kang et al. pointed out that technical users have more articulated mental models than their non-technical counterparts, contributing to a deeper and more complete privacy risk-concerns perception [38]. Divergencies in risk-benefit perceptions between the technical and non-technical user groups reported by prior efforts [27, 38] suggest that technical literacy is likely to be a crucial component of the difference in trust perception and overall privacy control adoption behavior, which is yet to be examined in detail. Drawing on this gap in the literature, we incorporated technical literacy as one of our independent variables to observe its interplay in the privacy-trust relationship. To define users' technical literacy level, we used Kang et al.'s *Technical Knowledge of Privacy Tools Scale* (TKPTS) [38]. Kang et al.'s work reported and validated the scale to effectively measure users' technical literacy rather than asking users to self-report their technical literacy level. Based on participants' scores on TKPTS, we categorized them as either *technical* (scoring at least 4 out of 6) or *non-technical* (scoring at most 3 out of 6) participants, while keeping the distribution consistent with the distribution reported in Kang et al.'s work [38].

Overall, in this work, we sought to investigate whether users' adoption behavior of privacy controls varies based on trust perception, the purpose of the controls ("sharing" vs. "usage"), and the technical literacy of participants ("technical" vs. "non-technical"). Towards that, we ask the following research questions:

- **RQ1.** Does the adoption of "sharing" vs. "usage" privacy controls differ based on users' technical literacy?
- **RQ2.** Does trust towards the service provider (e.g., Google) differ based on users' technical literacy?
- **RQ3.** (a) Do technical adopters and technical non-adopters differ in trust perception across the "sharing" vs. "usage" privacy control categories? (b) Do non-technical adopters and non-technical non-adopters differ in trust perception across the "sharing" vs. "usage" privacy control categories?
- **RQ4.** (a) What are the reasons that may enhance/dampen users' trust towards a service provider's (e.g., Google) user privacy protection? (b) Do technical users differ from non-technical users in terms of such reasons?

In order to investigate the above research questions, we designed a user study while choosing Google as our service provider of interest. We elaborate on the reasoning behind choosing Google as the target platform in the Methodology Section (Section 3). In our study, we conducted an online survey among Google users to understand their perceptions of trust and adoption of privacy controls. We performed a quantitative and qualitative analysis of the survey data (N = 209) to shed light on the research questions. Our quantitative results reveal that technical literacy does impact users' trusting beliefs and adoption behavior. While technical and non-technical participants have similar levels of Google's perceived competence, technical participants have a significantly lower perception of Google's integrity and benevolence than non-technical participants. In addition, the interplay between trust and privacy control adoption emerges much more nuanced depending on technical literacy and the privacy controls' underlying purposes. For example, though technical adopters and technical non-adopters do not differ much in their trust perception across the "sharing" vs. "usage" categories, the interactions are significantly different among their non-technical counterparts. Among non-technical participants, adopters of "sharing" controls indicate higher trust perceptions towards Google, while adopters of "usage" controls reveal lower trust perceptions towards Google.

In this paper, we make the following key contributions:

1. We investigate and report how the privacy controls' purpose of "sharing" vs. "usage" impact users' perception of trust towards the service provider based on their technical

literacy level. Notably, our findings hint at how end-users can be misled into overestimating their degree of control over personal data by offering privacy controls ("sharing" vs. "usage"), which can help build trust towards the service providers. In addition, drawing on our findings, we elaborate on the existing power dynamics between the service providers and end-users in the discussion.

2. By leveraging qualitative analysis techniques, we document both trust-enhancing and trust-dampening factors and discuss the relative importance of these factors from the perspective of technical and non-technical participants, which can help guide the design of trust-calibrating strategies.
3. Finally, while answering the research questions, we identify multiple shortcomings of the current state of privacy controls and service providers' practices. We offer concrete suggestions to help service providers strengthen their trust relationships with end-users and potentially increase the adoption of privacy controls.

2 BACKGROUND

In this section, we first review the literature on users' perception of privacy and existing works investigating the adoption of privacy controls in different contexts (2.1). Then, we review the literature on the related constructs, such as technical literacy and trust, and how they affect users' privacy behavior (2.2).

2.1 Privacy Perceptions and Adoption of Privacy Controls

Back in 1991, Goodwin argued that users' control over personal data in a commercial relationship is a crucial component of users' privacy and defined the term"privacy control" as users' control over unwanted presence in the environment (e.g., the Internet) [33]. Hoffman's (1999) subsequent findings support this. They indicated that consumers' ability to control websites' actions to protect their data affects their perception of security and privacy practices [36], which also gives users a feeling of greater autonomy [76]. In the same vein, Chen et al. (2004) observed that consumers typically feel personal information should not be taken without their knowledge and consent, creating concerns about the acquisition of personal information by e-businesses and service providers [19]. Furthermore, such concerns are shown to be correlated with a lack of trust between consumers and e-businesses, exacerbated by the lack of control over personal information being collected [36].

Service providers incorporate privacy controls on their platforms to address users' concerns about lack of *control over data* because device-specific privacy-enhancing features are shown to help lower privacy invasion risks [73]. In recent work, Feng et al. found that giving users control over privacy helped reduce perceived intrusiveness and led to a more positive app and brand attitude [29]. It is now a common practice across service providers to integrate privacy controls across their services/websites to offer their consumers choices over data privacy. However, only a limited number of prior efforts examined end-users' adoption of privacy controls. Even then, most works investigated the adoption of privacy controls in the context of Social Networking Sites (SNS). For example, Baruh et al. (2017) found that users concerned about privacy are more likely to use protective measures such as controlling SNS privacy settings [13]. Schwartz et al.'s work (2020) focusing on privacy on Facebook also reflected similar results [57]. Acquisti et al. (2019) investigated users' upstream disclosure choices in SNS settings. They found that when privacy options are given as a choice/control, participants are more likely to choose protective disclosure settings [3]. However, Brandimarte et al. (2013) warned that control over the release of information (such as disclosure settings on SNS) might act as an illusion regarding a company's access to data, leading to a lower perception of privacy risk and concern, and suggested to emphasize on the control over access/usage of the shared data [16]. While choices offered by Google such as *Location history* and *Ad personalization* fit into the "usage" category, to the best of our knowledge, no prior work in the literature investigated the adoption of these controls and how they relate to the perception of trust.

Among the works that look into privacy control adoption in non-SNS contexts, Ketellar (2018) found that privacy concerns allowed users who wanted to prevent being tracked to adjust the settings of their smartphones and IoT devices [31, 40]. Xu et al. (2012) pointed out the importance of investigating privacy in a specific context and suggested that context-specific factors may significantly impact overall privacy behavior as well [75]. In recent work, Balash et al. (2021) investigated users' security and privacy perceptions of third-party application access for Google accounts [9]. They noted the popularity of Google's Single Sign-on (SSO) service in third-party app authorization, which allows these apps to access personal data in Google accounts. Farke et al. (2021) investigated users' perception of the privacy dashboard in the context of Google's "myactivity". They noted that even though these tools are offered to provide transparency of data collection, they end up helping Google in building trust and do not lessen user data collection [28]. Though not focused on privacy control adoption, these works underscore the need for an in-depth investigation of trust and privacy adoption in this context.

2.2 Technical Literacy, Trust, and Privacy Behavior

In 2015, Ion et al. noted differences in safety perception and behaviors among technical and non-technical participants[37]. Kang et al. (2015) also identified a gap in the mental models of technical and non-technical participants. They showed that technical participants had a more complex and sophisticated mental model regarding data security and privacy and a better understanding of privacy risk-benefit perceptions compared to non-technical participants [38]. Prior efforts further indicated a connection between technical knowledge, privacy concerns, and behavior. In 2004, Malhotra et al. noticed that users' ability to understand and manage privacy plays a vital role in their privacy protection strategies [47]. The ability to understand privacy was found to be affected by users' lack of technical literacy among Facebook users as well [25]. It is evident in the literature that technical literacy does play an important role in privacy decision-making among Social Networking Site (SNS) users [13, 25, 63, 72]. Technical literacy was found to affect users' perceived vulnerability, influencing their perceived

ability to control information sharing alongside elevating their perception of privacy [68]. In contrast, some works suggested that, while technical literacy impacts users' level of privacy concern and intention to take privacy protective measures, it does not affect the actual privacy behavior [13]. Kang et al. also observed a discrepancy between users' technical literacy and privacy-protective measures [38]. These mixed results indicate that, while technical literacy affects users' perception of privacy, how their interaction changes across different platforms and contexts needs to be clarified. Therefore, it is crucial to consider technical literacy, privacy perceptions, and trust factors while studying technology adoption and privacy behavior.

A vast body of work looked into the effect of trust on privacy behavior. In online privacy contexts, users' belief in a service provider's trustworthiness often comes from their perception of the provider's willingness to protect user data, facilitated by providers' privacy-enhancing interventions (e.g., privacy controls) [74]. Availability of privacy interventions assures consumers that the vendor site is safe [50] and reduces consumers' perceptions of privacy invasion risks and concerns [18, 73, 74]. Unfortunately, inappropriate trust can lead to risky privacy decisions as well. For instance, Balash's work in the context of Google identified inappropriate trust towards third-party services authorized with Google's SSO services [9].

Works looking at trust in the context of data breaches also portray trust as a crucial antecedent of service adoption and perception of privacy. Users' trust towards a breached entity decreases significantly upon publication of the breach information [7, 8, 11, 65]. In the context of social networking sites (SNS), Antoci et al. showed that a breach in trust often leads to reduced usage of services [6]. A similar reduction in usage or even complete avoidance was noticed after a trust breach in the context of online shopping as well [65]. As trust is shown to be a significant antecedent of service usage, breached entities often rely on trust-repair activities such as persuasive apology [8] and compensation [48] in order to rebuild the trust relationship with consumers. Further, actively communicating breach information to the consumers and subsequent actions to protect users from further breaches pose higher behavioral integrity perception among the users and help maintain trust [7].

While the relationship between trust and privacy behavior is investigated in the literature, it is unclear whether such an effect of trust is related to end-users' technical literacy. Additionally, prior efforts that investigated trust (e.g., McKnight's trust conceptualization [50]) primarily studied trust perception towards the service provider (i.e., trustee) attributed by the service consumer (i.e., trustor). However, trusting a service provider may not fully correspond to the same level of trust in using their services. For example, despite having trust towards the service provider (e.g., Google or Amazon), consumers reported having lower trust in using their product (e.g., Smart Personal Assistants (SPA) such as Google Home and Amazon Alexa) in specific ways (e.g., using the SPA for online shopping) [1]. Furthermore, Metzar showed that trusting a service provider is more strongly influenced by the entity's reputation (i.e., the brand trust) rather than their actual security and privacy practices [51]. Thus, trust towards a popular (with brand popularity) service provider (e.g., Google) may not align with users' trust perception towards the same provider's approach to protecting user privacy. Towards this vein, using qualitative analysis techniques, we look at factors affecting users' trust in the service provider's privacy protection and how technical literacy impacts the interplay of such factors.

3 METHODOLOGY

In this study, we choose Google as our service provider of interest based on the following key considerations. **First,** *The juxtaposition of privacy control offering and the data-centric profit motive*: On one hand, Google is the most used search engine, with over 92% market share [64], that provides most services without monetary charge while offering several privacy and security choices to give users control over their privacy and data sharing preferences. On the other hand, Google monetizes users' data and depends on Ad revenue via Google Ad Services, which leverages user information (e.g., search history, click behavior) to deliver targeted advertisements. Given the popularity of Google services combined with Google's data-centric business model, it is particularly intriguing to see how trust impacts Google's privacy control adoption depending on users' technical literacy. **Second,** *The availability of offered privacy controls across both "sharing" and "usage" categories*: Literature that investigated privacy control adoption often do so in the context of Social Networking Sites (SNS) where the offered privacy controls are disclosure settings (i.e., restrict content sharing with a recipient pool) that fall under the "sharing" category [16]. However, keeping the research questions in mind, we needed a service provider that offers privacy controls across both "sharing" and "usage" categories. Google offers both "sharing" controls, such as *Browser history* and *Cookies*, and "usage" controls, like *Ad personalization* and *Location history*. These key factors led us to select Google as our service provider for the study.

3.1 Purpose of Privacy Controls: "Sharing" vs. "Usage" of Data

In this work, we group privacy control into two groups based on the intended purpose of the controls. First, based on Brandimarte's conceptualization[16], we identify a group of privacy controls that enable users to customize whether Google can use collected data for personalization purposes (referred to as "usage" controls from here on). Second and finally, there is another group of controls that allow users to block sharing of data with third parties (e.g., either friends/family members or third-party websites) but does not affect or restrict how Google can use the collected data (e.g., for personalization) (referred to as "sharing" controls from here on). *Note that the word "control" in this paper refers to "privacy controls/choices" offered by service providers rather than indicating control variable or control group.*

Regarding grouping controls by the intended purpose (i.e., "sharing" vs. "usage" of data), it is important to note that, though nuanced, there is a clear distinction between these concepts. Specifically, the choice/control architecture that provides control over the "sharing" of data does not necessarily give users control over how the collected data can be used. For example, in the case of SNS, users are often given disclosure settings that allow users to restrict sharing of collected data to a limited recipient pool (e.g., shared with friends). However, once collected by the SNS, even if not shared

Privacy Control	Control Purpose	Reported Measure	Default Setting	Privacy Conservative Settings (Ascending order of Strictness)
Browser history	Sharing	Usage frequency	N/A	N/A
Cookies	Sharing	Current setting	Block third-party cookies in Incognito	1. Block third-party cookies 2. Block all cookies
Location history	Usage	Current setting	Allowed with auto-deletion off	1. Allowed with auto-deletion on 2. Paused/Turned off
Ad personalization	Usage	Current setting	Disabled	Enabled

Table 1: Privacy controls and available choices/options

with third parties, it can be misused by the service providers, violating privacy. Further, even when a user restricts sharing, the information that has already been shared with other third parties can still be used in ways that violate privacy. Despite this limitation, service providers often provide "sharing" controls, which can be manipulative and benefit companies rather than the users in terms of privacy [69]. Brandimarte considers these as 'Illusory of control' that can lead to lower privacy risk perception and potentially impact users' trust [16]. Therefore, a privacy control that gives users control over how the data, once shared/collected, can be "used" is much preferred for privacy protection as users can potentially review and restrict the usage of their shared information.

We chose four privacy controls from Google platforms due to two primary considerations. First, the distinction between somewhat illusory "sharing" controls and more preferred "usage" controls motivated us to investigate how they impact the trust-privacy relationship. Second, we limited participants to two controls each to keep the survey length reasonable and elicit thoughtful responses. As our goal was not to directly compare controls to one another but to investigate whether and how controls' purposes may relate to users' trust-privacy considerations, looking at a subset of controls was considered adequate for this study.

To investigate the effect of the purpose of privacy controls, as samples of "sharing" controls, we chose *Browser history* and *Cookies*. These controls are offered in Google's Chrome platform. *Browser history* allows users to review and delete history and browsing data and allows control over sharing the history data across synched devices and with other users in case of shared devices (e.g., family, friends, colleagues). However, when a user clears the browser history, while it clears the search history from the local browser or synched devices, it does not remove the user activity data that is available to Google, which Google can still use for personalization or other targeting purposes. Moreover, once users allow browsing history to be saved, they have no control over how the shared information can be used. For example, a family member or friend who shares the device with or uses a separate but synced device may be informed of sensitive personal information by looking at the browsing history, violating personal privacy. *Cookies* control offers choices for users to allow or block websites to save cookies into the browser (can be either marketing, functional, or statistical cookies; Google's definition of the control does not differentiate across the types of cookies). Similar to *Browser history*, while blocking cookies may help restrict data sharing with a third-party, data collection and usage by Google are not affected. Further, similar to the disclosure settings on SNS sites (that allow sharing of content to specific user groups), this control enables users to choose websites that will be allowed to save cookies. However, once the cookies are allowed, user data is collected by these cookies. Although users can remove cookies from the browser to discontinue future data collection if they change their minds, users do not have any control over how the websites use the collected data (e.g., allowing third-party cookies may introduce cross-site tracking), and, importantly, how Google can use the collected data. Hence, these controls serve the purpose of "sharing" control rather than a "usage" control.

For the "usage" controls, we chose *Location history* and *Ad personalization* controls present on the Google Account platform. *Location history* control entitles users to allow or restrict Google from using shared location data (e.g., through Google Maps, mobile devices) for purposes such as creating personalized maps and recommendations based on visited places. Similarly, *Ad personalization* control allows users to opt in or out from receiving targeted advertisements that leverage data shared with Google. Importantly, by using Google services (e.g., maps), certain user data is already collected. For example, when a user uses Google Maps, travel data is already available to Google. Likewise, browsing in Chrome allows the collection of information that may be used for targeted Ads. However, controls such as *Location history* and *Ad personalization* give users the option to choose how Google may use the shared personal data. Hence these controls fall under the "usage" controls category and intuitively give users more power over their data.

Table 1 shows the privacy controls, the purpose they serve, reported measures from the participants, their default settings (if applicable), and the conservative settings for the controls (if applicable).

3.2 Variables in the Study

Technical Literacy. To avoid participants' self-report of their technical literacy level, we used the Technical Knowledge of Privacy Tools Scale from Kang et al., who showed the scale's effectiveness in determining the technical literacy of users while considering it as a binary variable to distinguish between technical vs. non-technical participants. Kang et al. validated the scale's reliability by combining multiple data sets in both online and in-person setups and found the mean correctness: technical, $M = 4.27$; non-technical: $M = 1.53$ [38]. As such, we considered technical literacy as a binary variable, where a participant scoring equal to or higher than 4 out of 6 was defined as a technical (T) user ($M = 4.5, SD = .73$) and scoring between 0 to 3 was defined as a non-technical (NT) user ($M = 1.7, SD = 1.1$). The mean differences across the two

groups were consistent with the distribution reported in Kang et al.'s work [38]. The scale items are reported in the Appendix A.2.

Trust towards Google. McKnight et al. (2002) conceptualized trust as an interaction between three specific dimensions: *competence* - the ability of the trustee to do what the trustor needs; *benevolence* - trustors' belief that trustee cares and belongs motivation to act on trustors' interest; *integrity* - trustee's honesty in keeping their promise to the trustor [50]. To understand users' perception of trust towards Google, we used McKnight et al.'s Technology Trusting Belief scale (7-point Likert) [50], which consists of these three dimensions *Integrity, Competence*, and *Benevolence*. Numerous prior works in privacy literature used this scale to measure the constructs of trust [26, 41, 42]. We calculated Cronbach's alpha to measure the internal validity of the items and found high-reliability scores for the constructs (integrity: $\alpha = 0.92$; competence: $\alpha = 0.89$; benevolence: $\alpha = 0.89$). The scale is presented in the Appendix A.2.

We further asked study participants to briefly explain the factors (both positive and negative) behind trusting or distrusting Google's privacy protection. Participants' comments were used to perform qualitative analysis to understand users' trust perception towards Google's privacy protection.

Adoption of Privacy Controls. We asked participants to report the current settings of the privacy controls of their personal computers. For the study, we defined *adopter* of a privacy control as someone who changed the control's default setting to suit specific needs, even if the changed setting is not towards stricter privacy. The reason for considering participants who changed the default to a less strict setting also as adopters is their active role in customizing the control, which can be attributed to their conscious privacy-convenience tradeoff calculations (we refrained from judging whether a decision was right or wrong).

For the binary control *Browser history*, as there are no settings to enable or disable, adoption is defined by the frequency of proactively using the feature(i.e., clearing browser history). Thus, a person who *clears browser history* in their browser once every week is considered more proactive than someone who usually does it once a month or once in three months. For the control, proactiveness has three levels *using within a week*, *within a month*, and *within three months*.

3.3 Participant Requirement

Participants were recruited from Amazon's Mechanical Turk (MTurk) platform. Recently, there has been criticism regarding the quality of data from MTurk [66]. Despite the criticism, MTurk is a widely used platform for online surveys in usable security and privacy [15]. Moreover, to ensure the quality of data and to elicit thoughtful responses, we have taken several precautionary steps: First, to restrict multiple attempts to figure out the eligibility criteria, we asked participants to enter their MTurk ID (A unique identifier assigned by Mturk to each Mechanical Turk worker) prior to seeing the prescreening questions and kept a database of unique MTurk IDs to cross-check if an MTurk worker has attempted the prescreening questions before. This approach also enabled us to prevent bots from taking the survey. Second, we asked participants multiple attention-check questions throughout the survey and removed the responses from participants who failed to answer one or more of these questions correctly. Third, we recruited participants who had completed at least 1000 Human Intelligent Tasks (HITs) and had a HIT approval rate of 95% based on recommendations from prior works [70].

We restricted the participation eligibility to those at least 18 years of age, currently living in the United States, and proficient English speakers (as the survey was conducted in English). As the study focused on Google's privacy control adoption, the eligibility for the study required participants to use Google Chrome for their daily internet browsing alongside having a personal Google Account. In addition, as certain company/business protocols may override users' innate account settings behavior to protect the company's data privacy and security, we only considered participants who had a personal home computer and personal Google Account that they did not use for business/company purposes and asked them to report settings from their personal computers.

In addition, to ensure that participants' technical literacy came from their self-promoted proactive technology usage, alongside the intention to avoid any confounds of computer science-related educational background on technical literacy, we restricted participants to those who did not have any computer science education background and measured their technical literacy afterward using the instrument from Kang et al.'s work (2015) [38].

Lastly, we restricted participants to those who use Windows personal computers and Android smartphones to avoid possible confounding effects due to different operating systems pointed out in earlier effort [14].

3.4 Survey Flow

After giving consent, participants first answered the prescreening questionnaire to measure their eligibility. If found eligible, participants were randomly assigned to one of the two groups based on the purpose of the controls: "sharing" or"usage". Next, participants reported their behavior for the controls they were assigned to, where each participant reported adoption behavior for the two privacy controls of the assigned purpose. After the group assignment, participants' technical literacy and trust in Google were measured first (Likert scale and qualitative response). Next, participants were asked to report their current settings for their assigned controls. We asked privacy control-related questions last to avoid biasing and raising concerns about Google (which might have affected their trust ratings).

For the controls where current settings were measured, we showed participants step-by-step instructions (with proper images) on how to go to the specific settings page and report the current settings to assist them in reporting. Finally, the survey ended with participants answering the demographic questionnaire. Survey instruments and questionnaires are presented in the Appendix.

Survey took about 20 minutes to complete ($M = 19.48, Mdn = 15.28, SD = 14.38$), and eligible participants were compensated $3 for completing the survey. The survey was hosted on the university's Qualtrics server and was approved by the university Institutional Review Board (IRB).

3.5 Survey Data Analysis

We recorded a total of 215 responses for the main survey. Among them, 6 participants (2.79%) failed at least one of the three attention

check questions. We removed these responses from the data. These led us to our final data set of 209 valid responses. Among them, 105 participants were in the "sharing" group, and 104 were in the "usage" group. Scores from technical literacy items indicated that there were 65 (34 in "sharing" group, 31 in "usage" group) technical participants (Scoring 4 or higher out of 6) and 144 (71 in "sharing" group, 73 in "usage" group) non-technical participants (scoring 3 or lower out of 6) in the data set.

Assumption tests showed that data violated the normality assumption (normality transformation techniques also failed). In addition, the specific group sample size for individual controls (e.g., the number of technical adopters of a specific control) was low for some cases. Due to these observations, as suggested in literature [43, 53, 56], we used nonparametric tests for significance testing, e.g., Mann-Whitney U tests (for two samples) and Kruskal-Wallis tests (for more than two samples; posthoc results are reported). Bonferroni corrections were made for any post hoc comparisons (for Kruskal-Wallis tests) as needed. We used a p-value < .05 to indicate statistical significance. We calculated and reported effect size (r) for Man-Whitney tests using $r = \frac{Z}{\sqrt{N}}$ formula [30]. Data were analyzed using SPSS.

For qualitative data analysis, we used a bottom-up inductive coding approach [52] to code the responses to the open-ended question. Initially, two researchers coded each statement independently by reading through all the comments. Then both coders met and decided on the final codebook. Afterward, both coders sat together to resolve the conflicts between the codes. After the conflicts were resolved, both coders independently updated their codebooks. Inter-rater reliability (IRR) for each question was calculated using Cohen's Kappa, which ranged from 0.7 to 1, indicating "substantial" or "excellent" agreement between the coders [44].

4 RESULTS

Among the 209 responses, there were 112 males (53.6%), 95 females (45.5%), one other, and one participant who chose not to answer. Participants' age ranged from 22 to 70 years ($M = 38.52, SD = 10.43$). Group-wise demographic breakdown of the participants is presented in Table 5 in the Appendix A.2.

Mann-Whitney U test showed no significant differences across the groups regarding age ($U = 6088.5, p = 0.154$) and technical literacy scores ($U = 6129, p = .12$). In addition, a chi-squared test showed no significant differences in terms of gender across the groups ($\chi^2(1) = 1.402, p = 0.236$). Based on this, we concluded that the groups are demographically similar.

Between the technical and non-technical participants, a Chi-squares test showed a significant difference in gender ($\chi^2(1) = 5.989, p = 0.014$). Further analysis showed that 66.2% (43/65) technical participants were male compared to 47.9% (69/144) non-technical participants across all platforms. However, technical and non-technical participants did not differ in age ($U = 4858, p = 0.66$). Hence, our recruitment method yielded more male participants than female who scored highly on the technical literacy scale.

4.1 Adoption of the Privacy Controls (RQ1)

The adoption rate of the privacy controls varied across the controls. Figures 1 and 2 summarize participants' responses for the "sharing" vs. "usage" controls, respectively. Importantly, for all three of the controls with a default setting (except *Browser history* that does not have a default value), the majority reported having the defaults as their current settings. For example, 53.3% (56/105) participants kept the current setting for *Cookies* control as "Block third-party cookies in incognito," which is the default setting. Similarly, for the *Ad personalization* control, 70.2% (73/104) reported having it turned on. On the other hand, there was no setting to turn on or off for the *Browser history* control. Among the participants, 34.3% (36/105) mentioned using the feature within a week, which was the most frequent among the options. Hence, we conclude that *most participants are likely to keep the defaults as their current settings for the chosen privacy controls in our study.* **(Finding 1)**

Looking closely into the adoption rate across the technical literacy levels gave us an understanding of how privacy controls are adopted among the technical and non-technical participants. Figures 3 and 4 portrays the results for the "sharing" vs. "usage" controls, respectively.

For the "sharing" controls, non-technical participants were found to use/change the current settings more frequently than technical participants. For example, 48.3% (29/60) non-technical participants mentioned using the *Browser history* control within a week, compared to 25% (7/28) technical participants. However, the difference was not found to be significant. Similarly, for the *Cookies* control, 42.3% (30/71) non-technical participants kept the default setting "Block third-party cookies in incognito" compared to 76.5% (26/34) technical participants. Post-hoc tests showed that non-technical participants were significantly more likely to change the default settings than technical participants ($\chi^2(1) = 10.89, p = 0.001$, corrected $p = 0.008$). Further, non-technical participants (36.6%; 26/71) used the conservative option "Block third-party cookies" significantly more compared to the technical participants (8.8%; 3/34) ($\chi^2(1) = 9.0, p = 0.003$).

Among the "usage" controls, we did not find any significant differences between the technical and non-technical participants for the *Location history* control. Overall, 27.4% (20/73) of the non-technical participants kept the defaults compared to 54.8% (17/31) of the technical participants. Likewise, for the *Ad personalization* control, the default usage was about the same between technical and non-technical groups (about 70% for both groups). Based on our data, we conclude that, *among the four controls, non-technical participants significantly differ from technical participants in changing the default settings for the Cookies control only.* **(Finding 2)**

4.2 Trust Perceptions towards Google (RQ2 & RQ3)

4.2.1 Trust difference between technical vs. non-technical participants (RQ2). Regarding trust towards Google's competence, technical ($M = 5.6, Mdn = 6, SD = 1.1$) and non-technical participants ($M = 5.73, Mdn = 6, SD = 1.0$) did not differ significantly. Overall, participants' high ratings of competence score toward Google ($M = 5.69, Mdn = 6, SD = 1.01$) indicate that they felt Google has the competence to provide effective services.

However, regarding perceptions of Google's integrity and benevolence, technical and non-technical participants significantly differed. Technical participants ($M = 4.3, Mdn = 4.33, SD = 1.4$)

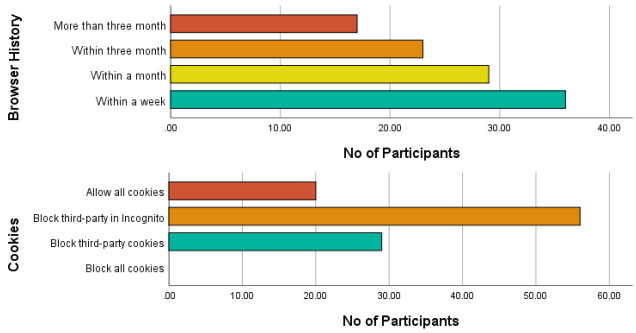

Figure 1: Participants' adoption rate of the "sharing" controls

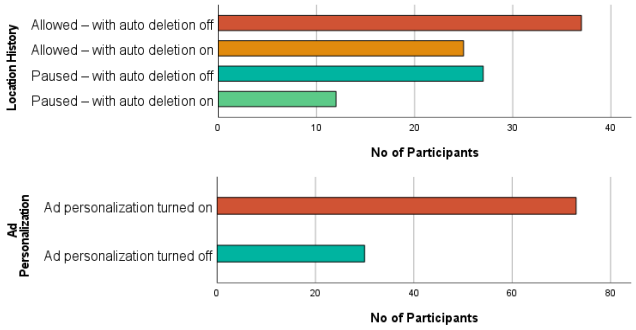

Figure 2: Participants' adoption rate of the "usage" controls

rated significantly lower compared to non-technical participants ($M = 4.8, Mdn = 5, SD = 1.3$) towards Google's integrity ($U = 3672, p = 0.012, r = 0.17$) (e.g., Google is truthful in its dealing with me). Similarly, technical participants ($M = 3.9, Mdn = 3.67, SD = 1.5$) gave significantly lower benevolence rating to Google than non-technical participants ($M = 4.6, Mdn = 4.67, SD = 1.3$) ($U = 3432, p = 0.002, r = 0.21$) (e.g., Google acts in my best interest).

Based on our analysis, we conclude that *Technical participants differ significantly from non-technical participants in their perceptions of integrity and benevolence of Google. However, both groups agree on Google's high competence.* **(Finding 3)**

4.2.2 Trust difference between adopters vs. non-adopters across technical literacy levels. (RQ3). As trust is often found to be an influential factor in privacy decision-making [12, 13, 32], we wanted to see whether being an adopter of privacy control is associated with trust perceptions towards Google.

Among *technical participants,* trust (towards Google as a service provider) was not found to be associated with being an adopter for any of the four controls, indicating that technical adopters of the privacy controls do not show a significant difference in trusting Google compared to technical non-adopters (RQ3(a)). This result hints at the likelihood that trust in Google as a service provider may not be the most compelling reason for technical participants to change their choices from default settings.

We conclude that *Technical adopters and non-adopters of Google's privacy controls (both "sharing" and "usage" controls) do not differ significantly regarding trust ratings towards Google.* **(Finding 4)**

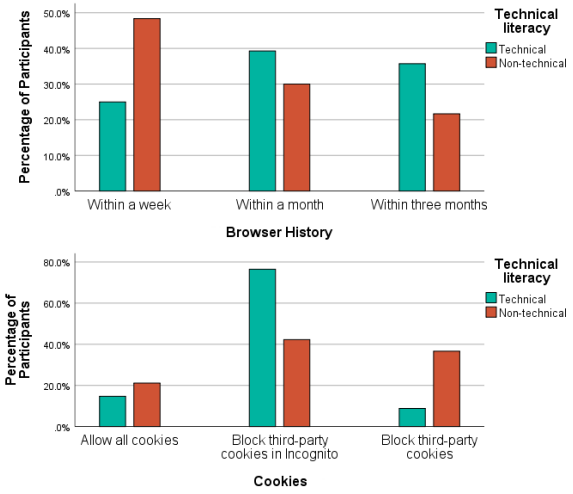

Figure 3: Adoption of the "sharing" controls between technical and non-technical participants

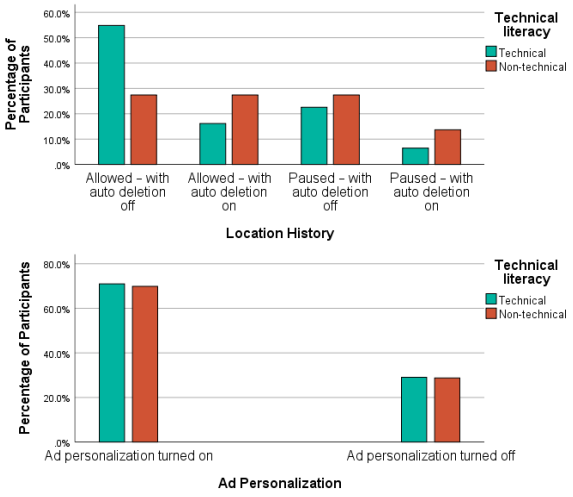

Figure 4: Adoption of the "usage" controls between technical and non-technical participants

For *non-technical participants,* trust was found to be associated with the adoption of several 'sharing" and "usage" controls. Specifically, differences in benevolence and integrity were found between non-technical adopters and non-adopters.

Among the "sharing" controls, we noticed a significant trust difference for the *Browser history* control, but not for the *Cookies* control. For the *Browser history* control, users who proactively (e.g., reported using these features weekly) deleted their browsing data felt high integrity and benevolence (benevolence: $M = 4.6, Mdn = 4.67, SD = 1.3$) of Google compared to those who barely used these features (e.g., reported using the feature within three months) (benevolence: $M = 3.7, Mdn = 4, SD = 1.1$). This finding may indicate that trusting Google lets these non-technical users use the "sharing" controls at a higher rate.

Non-technical Participants				
Control Purpose	**Privacy Control**	**Trust Integrity**	**Trust Competence**	**Trust Benevolence**
Sharing	Browser history (post-hoc: within a week vs. within three months)	$U = 100.5, p = 0.048,$ $r = -0.37$	*NS*	$U = 95.5, p = 0.033,$ $r = -0.39$
Sharing	Browser history (post-hoc: within a month vs. within three months)	*NS*	*NS*	$U = 57.5, p = 0.05,$ $r = -0.43$
Usage	Location history	*NS*	*NS*	$U = 408.5, p = 0.047,$ $r = -0.23$
Usage	Ad personalization	$U = 368.5, p = 0.029,$ $r = -0.25$	*NS*	$U = 329, p = 0.008,$ $r = -0.31$

Table 2: Signi cant associations between trust and adoption of the privacy controls. The symbol *NS* indicates non-signi cant results

Hence, we conclude that *Non-technical adopters of the "sharing" controls pose higher trust (integrity and benevolence) towards Google compared to non-technical non-adopters of such controls.* **(Finding 5)**

Among the "usage" controls, adopters of *Ad personalization* (benevolence: $M = 4.14, Mdn = 4, SD = 1.3$) and *Location history* controls (benevolence: $M = 4.6, Mdn = 5, SD = 1.3$) indicated lower benevolence (also integrity for *Location history* control) ratings towards Google compared to the non-adopters of *Ad personalization* (benevolence: $M = 5.1, Mdn = 5.33, SD = 1.3$) and *Location history* controls (benevolence: $M = 5.3, Mdn = 5.33, SD = 1.4$), respectively. The result may indicate that, for the "usage" controls scenario, participants who trust Google less (in terms of integrity and benevolence) adopt these controls to restrict usage of collected data for external/personalization purposes at a higher rate (e.g., use of location tracking for personalizing recommendations or third-party tracking for personalizing Ads). Summary of these findings with significance statistics are presented in Table 2, and the descriptive statistics of the significant associations are informed in Table 6 of the Appendix A.2. We conclude -

Non-technical adopters of the "usage" controls pose lower trust (integrity and benevolence) towards Google compared to non-technical non-adopters of such controls. **(Finding 6)**

Among non-technical participants, the directionality of trust changes between adopters vs. non-adopters of "sharing" vs. "usage" controls. For "sharing" controls, adopters indicate higher trust (integrity and benevolence) in Google, whereas, for "usage" controls, adopters indicate lower trust (integrity and benevolence) in Google. **(Finding 7)**

Overall, we observed that trust works as an crucial antecedent for the non-technical users' adoption decision of Google's privacy controls, but not so much for technical users. While these findings complement the literature by echoing that trust is crucial in privacy decision-making, our findings highlight a much more subtle effect of trust based on technical literacy.

4.3 Factors A ecting Trust Towards Google's Privacy Protection (RQ4)

To identify the factors that contribute to (dis)trusting a service provider (i.e., Google) from the perspective of privacy protection, we asked participants to explain their reasoning behind their attribution of trust towards Google's privacy protection. Findings of our qualitative analysis are presented below (sample comments are presented with minor corrections to address typos as needed, T and NT indicating comments from a technical and non-technical participant, respectively). In addition, a summary of the top five most frequently mentioned trust-enhancing/dampening factors by the participants is presented in Table 3, and 4 for an easier understanding of the results. The tables also show a relative difference between technical and non-technical participants in their factorization of trust towards Google's privacy protection (enhancing and dampening factors).

4.3.1 Factors affecting trust positively. Participants' comments revealed several reasons that go in Google's way and work towards building and maintaining a positive attitude towards Google, as we discuss here -

1. Rational Profit Motive vs. Top-notch Security. For technical participants, one of the top reasons for trusting Google was due to Google's business model, where users must be valued and protected for Google's own good. Specifically, participants discussed how Google's business model depends on protecting its reputation, following regulatory requirements, and keeping its user base, which they believe would motivate Google to protect its users (i.e., rational profit motive). In total, 14/65 (21.5%) technical participants, compared to only 6/144 (4.2%) non-technical participants, mentioned these reasons for trusting Google's privacy protection. Examples of such comments are given below.

"Google is a corporation. They have an interest in maintaining customers. While I don't necessarily trust Google, I do trust their profit motive. With that in mind, I trust that Google will, for the most part, do what they can to protect privacy to ensure that they are not losing too many customers or users in general. So, in that sense, I trust Google quite a bit, but not completely." (T)

"I feel they are not protecting my privacy but protecting their data. I feel like having my privacy protected is an unintended consequence to them keeping their data safe." (T)

These comments indicate that technical participants are more likely to trust based on their understanding that Google will protect its users in order to maintain its reputation and popularity. Such

Technical Participants	Non-technical Participants
#1. Rational profit motive calculations (21.5%)	#1. Top-notch security (24.3%)
#2. Having a good track record (21.5%)	#2. Quality services and convenience factors (17.4%)
#3. Positive attitude towards Google's perceived user protection (18.5%)	#3. Positive attitude towards Google's perceived user protection (15.3%)
#4. Top-notch security (16.9%)	#4. Having a good track record (12.5%)
#5. Availability of privacy options (15.4%)	#5. Availability of privacy options (7.6%)

Table 3: Top 5 trust enhancing factors across technical and non-technical groups

Technical Participants	Non-technical Participants
#1. Google's data collection and usage practices (40%)	#1. Google's data collection and usage practices (38.9%)
#2. Skepticism about Google's ulterior motive (33.8%)	#2. General distrust over Internet use (18.1%)
#3. Lack of transparency (18.5%)	#3. Skepticism about Google's ulterior motive (14.6%)
#4. Shortcomings of privacy options (12.3%)	#4. Lack of transparency (7.6%)
#5. General distrust over Internet use (7.7%)	#5. Shortcomings of privacy options (4.2%)

Table 4: Top 5 trust dampening factors across technical and non-technical groups

rational considerations are not among the top reasoning for non-technical users. This conjecture aligns with our quantitative finding of lower integrity and benevolence perceptions of Google among the technical participants, as their trust is mainly based on their rational understanding of Google's profit motives.

In comparison, non-technical participants' number one reason to trust Google was the availability of solid security in place to protect user data. 35/144 (24.3%) of the non-technical participants mentioned this as their primary reason for trusting Google. One such comment is listed below.

"Google is one of the topmost search-engine in the world. Google offers us high security to our data and protects our data. This is their main role, and this will eventually increase their consumers. They have highly trained technicians and well-structured code to protect our privacy." (NT)

While technical participants also mentioned Google's strong security as a reason for their trust in Google's privacy protection, only 11/65 (16.9%) of the technical participants mentioned this reason, ranking fourth compared to the most mentioned reason (ranked first) by the non-technical participants.

From quantitative analysis, we saw that both technical and non-technical participants had higher competence perceptions of Google. However, the qualitative comments add dimension to that. Even though both parties agree that Google is competent, non-technical participants seem more driven by it to put higher trust in Google's privacy protection. On the other hand, technical participants seem to give little weight to Google's competence in trusting Google's privacy protection.

2. Importance of Track Record. Having a good track record was mentioned by 14/65 (21.5%) technical participants compared to 18/144 (12.5%) non-technical participants as a reason behind their trust in Google. It was the second most common reason mentioned by the technical participants and the fourth most common reason by the non-technical participants. It is possible that this reason was mentioned more frequently by the technical participants as they are more likely to use Google services for an extended period due to their familiarity with technology compared to non-technical participants. For example, one technical participant mentioned the following.

"Google has a pretty good track record with security and I've used their services for over 10 years and trust them highly. I would trust them to protect my info on all my accounts evenly." (T)

While Google's dealing with personal data is a source of concern for most (exhibited in the trust-dampening factors), often having no negative experience subsided those concerns of data collection by Google, at least to some extent. Hence, while most participants felt concerned about Google's data-centric business model, having a good track record was still a positive factor that enhanced trust.

"I'm sure they are using user data in ways that the public is not aware of. I personally have not had any problems, so I cannot be too critical." (T)

3. Quality of Services and Convenience. In contrast to technical participants, the availability of e cient and convenient services was mentioned as one of the top reasons (ranked second) for trusting Google by the non-technical participants. Specifically, 25/144 (17.4%) non-technical participants mentioned this reason for trusting Google. For example, Google's search functionality was often perceived as an indication of its effective services and the core reason behind trust. Thus, for the non-technical participants, the quality and the convenience of the service that Google offers are likely to be essential in their consideration to trust Google. One such statement is listed below.

"I search many results in Google chrome. I trust this search engine for 90% percent." (NT)

For some non-technical participants, the utility of services seemed to suppress their suspicion of data collection, as noted in the comment below.

"I like the ease of using Google products. I do not like how Ads seem to tailor themselves to things I've said out loud. That makes me paranoid." (NT)

Compared to non-technical participants, 7/65 (10.8%) technical participants mentioned the services and conveniences as their

reason to trust Google (not in the top five). However, unlike non-technical participants, technical participants showed a more sophisticated understanding (often negative) of the tradeoffs while trusting Google, as expressed in the following comment.

"...It provides me with useful tools as long as in exchange it can take the data it wants, and then uses that data to its own advantage. I am under no delusion that Google does this in any way to help me - I am here to help it maximize its profit. This is the deal by which we operate. It is not perfect; it is just convenient." (T)

4. Positive attitude towards Google's perceived user protection. A common reason mentioned by participants that goes in favor of Google was a positive perception that Google is watching out for their users and not taking part in negative practices, which often led to trust in Google's privacy protection. 12/65 (18.5%) technical and 22/144 (15.3%) non-technical participants mentioned this as their reason for trusting Google (ranked third for both groups).

"Google has never let me down in many years and I've never seen them involved in negative privacy related events like Facebook. They seem like a great company always looks out for their customers." (T)

As suggested by the previous comment, having a good experience and track record can contribute to the overall positive attitude that Google is protecting its users and not participating in any privacy violation activities. In addition, participants who felt that Google is transparent about data collection also seemed to think positively about Google's benevolence.

Finally, a general positive attitude towards Google was also noticed among some participants.

"Google as being in the market for a long time, I genuinely think they offer a good service in regard to their customers, and they will remain being the top company in their field for a long time due to their policies." (NT)

5. Availability of Privacy Controls. Overall, 10/65 (15.4%) technical and (11/144) 7.6% non-technical participants mentioned the availability of privacy options as a reason for trusting Google (ranked fifth for both groups). This finding complements the prior work that shows the availability of control over data works as an antecedent of trust [74] and can reduce concern over privacy [18, 73].

One such comment is presented below.

"Google seems to give a lot of controls, especially around privacy and security, which, if you know how to use, can make things very secure and safe. Google seems open about how your information is used and shared if you know where to find it." (T)

Even when some participants had a negative attitude toward Google's data collection, they acknowledged the availability of privacy options as a positive thing.

"I think there are some things that are good about Google. They have a lot of different privacy options you can use. And you can see what data they have on you. But at the end of the day, they are a company and will always care about themselves first." (T)

It is important to note that while having privacy controls may increase trust when it comes to adopting privacy controls, trust has a more nuanced role, as we observed in our quantitative analysis. Specifically, we noticed that the adoption of "usage" controls is related to lower trust towards Google among the non-technical group. Hence, merely having privacy controls that enhance trust can be illusory, as suggested in this prior effort [16].

6. Availability of Alert Notifications. While not ranked as one of the top five reasons in either group, a small number of participants, especially in the non-technical group, mentioned the alert notification feature as a positive factor behind trusting Google. Specifically, 6/144 (4.2%) non-technical and 1/65 (1.5%) technical participants mentioned this as their reason for trust.

"Google notifies me of trusted websites. Google also alerts and prevents untrusted sources from trying to obtain my account information..." (NT)

One non-technical participant mentioned being notified by Google for non-Google accounts as a positive factor for trusting Google.

"...they even notify me when my non-Google accounts have possibly been compromised." (NT)

4.3.2 Factors affecting trust negatively. Participants in both groups noted several factors, such as limitations of privacy controls, malicious ulterior motives, and ethical concerns that influenced their trust negatively towards Google's privacy protection, as discussed below -

1. Google's Data Collection and Usage Practices. Google being a data-centric company, was noted as the top reason behind participants' distrust towards Google's privacy protection. In total, 26/65 (40%) technical and 58/144 (38.9%) non-technical participants mentioned this as the primary reason behind the lack of trust in Google. It implies that the data collection-based (i.e., Ad revenue) business model of Google is one of the most concerning factors for the participants and contributes to their decision not to trust Google. Most participants who mentioned this reason seemed to suspect that Google may be collecting a lot of personal data they are unaware of.

"I don't trust Google at all. I am sure it stores and shares data that I have given them either willingly or without knowing." (T)

"Tracks what websites I visit and targets ads to me. Sells or shares information with other companies and advertisers. " (NT)

Some participants indicated Google's profit motive to be a negative factor toward trusting Google. Specifically, these participants felt that Google would not care for end-user privacy (i.e., lower benevolence perception).

"I don't trust Google at all because it is a company interested in making money. I, and all users, are commodities to the company and are treated as such. It's not done out of malice, it's just business. I don't trust any company for the same reason." (T)

Getting targeted Ads caused some participants to get a feeling of "being followed," negatively affecting their trust.

"I think that using Google leads to me seeing targeted ads. It's uncomfortable to feel "followed" across platforms." (NT)

Even when users found Google to be a technically competent service provider, they seemed skeptical, considering Google's data-centric business model.

"Google is competent, but probably collects, shares, and/or sells certain data, so I don't trust it. It is concerned with profit, not people or users." (T)

2. Google's Malicious Ulterior Motive. In their comments, 22/65 (33.8%) technical participants and 21/144 (14.6%) non-technical participants indicated some suspicion toward Google's ulterior motives. While the distrust was commonly linked with Google's data collection and usage practices and profit motives, it often went beyond that, where participants viewed Google as a selfish actor who would not hesitate to sell/share user data with malicious or government entities to benefit itself.

"...Will invade my privacy itself or let others do it if it's in their more important interests." (T)

"Google collects and stores this information and could someday give it to the government if it doesn't already" (NT)

The company's sheer size and the amount of data collection were also seen as causes of concern by participants.

"...They have collected so much sensitive information on people, from their voice data to their location and even their pictures, that it would be extremely naive to assume that Google doesn't use this information to give to both advertisers and government for profit." (T)

Finally, some technical participants' comments reflected their suspicion that Google might be associated with controversial practices and policies.

"They keep profiles on their user's personal information like age, gender, sexuality, healthy, location, and many more personal attributes. There is no good reason to do this, only bad ones that I see like profiting off people, and possibly worse as the US government becomes more leftist and totalitarian as Google supports dangerous left-wing philosophy and ideology." (T)

3. Lack of Transparency. Lack of data collection and usage transparency was mentioned by 12/65 (18.5%) technical and 11/144 (7.6%) non-technical participants as a trust-dampening factor. In addition, many comments from both technical and non-technical groups indicate a suspicion that Google may be collecting much personal information without them knowing, which may also be attributed to the lack of proper data collection and usage transparency on Google's end. Note that Google does offer a transparency report[1]. However, many users may be unaware of the report, or the report might not be informative enough or well-understood. Future work can investigate which one is true in Google's case. Nonetheless, lacking clarity and transparency seemed to be a deal breaker for some participants, contributing to suspicion and a lack of trust.

"...I'm fairly uneducated about how Google actually uses my information or how it's exchanged across these platforms. I really have no idea about how Google exchanges or sells information to third parties." (NT)

Some participants complained about how Google's data collection and usage policies can be difficult to find and how Google never asks for consent (or assumes consent by default) before collecting and storing data.

"...You may not always realize you've given permission because it's not clear." (T)

"...I know my search history is saved across multiple devices which is something I never agreed to but it's just there and it happens so I can't put all my faith into how Google handles my data." (T)

Finally, some participants pointed out distrust concerning Google's policy while trust in their quality of service, underlying the nuanced nature of the relationship between Google and its users.

"I'm sure Google is collecting some data "for my own good" - like to help me find items to buy based on my recent interest, but who else is seeing my personal data? Highest bidder? That Google will never share... But, yeah, it works good, and I'm satisfied with its service." (NT)

4. Limitations of the Privacy Controls. Overall, 8/65 (12.3%) technical and 6/144 (4.2%) non-technical participants mentioned limitations of existing privacy controls behind their lack of trust. Some participants pointed out that current controls require users to "opt out" to prevent data collection rather than "opting in," which allows Google to track users by default.

"... I do know there are privacy settings, but by default, it is set for Google to collect info from you while you browse and to provide you with 'targeted marketing' (a rather creepy experience) and some don't know you can actually set your account not to collect, therefore the fact that it's set by default to collect your browsing information is rather unfair..." (T)

Some participants indicated the need for educating users about the privacy options that Google offers, especially given that users need to opt out rather than opting in (e.g., *"Google does have privacy settings but doesn't make a point of educating users. You have to opt out not in..."(NT)*).

Notably, some questioned the efficacy of the controls in protecting privacy, considering Google's data-centric business model. These participants rationalized that Google must collect data to continue its revenue structure. However, privacy controls are given to restrict data collection, directly contradicting the Ad revenue-based business model.

".... I'm not certain that they protect my privacy, at all, and I don't believe that my settings have any effect on what their servers collect and I don't know the who story behind what they do with that information. I know they are an advertising company and it is used for that purpose..." (T)

Importantly, though the availability of privacy controls is seen as a trust-enhancing factor, knowing that the controls have limitations and may not be effective as they counteract Google's data-centric model may contribute to the lower adoption of these controls that we observed in our quantitative analysis. It implies that the mere offering of the controls may enhance trust, but ensuring adoption requires much more effort than that.

5. Distrust towards the Internet, Negative Media Coverage, and Bad Personal Experience. Among the comments, 5/65 (7.7%) technical and 26/144 (18.1%) non-technical participants expressed distrust towards the Internet in general as a justification for not trusting Google (e.g., *"I do not trust any entity that has access through the Internet..." (NT)*). Finally, media portrayal of negative information sometimes led a small number of participants to distrust Google's privacy protection. Specifically, 3/65 (4.6%) technical and 5/144 (3.5%) of non-technical participants mentioned hearing negative stories, which made them concerned.

[1]https://transparencyreport.google.com/

"Recently Google was in the news about how their private browsing was not as private as people thought, which makes me distrust Google even more." (T)

Finally, Some participants mentioned having negative personal experiences with Google services which affected their trust perception.

"I have heard far too many stories about privacy issues related to Google, and have even had some of my login information to one of my accounts end up in someone else's hands after never giving it out to anyone..." (T)

5 DISCUSSION AND DESIGN RECOMMENDATION

5.1 Trust and Power Dynamics between Service Providers and End-users

Prior efforts (including ours) confirmed that trust is vital in building a positive relationship between a service provider and end-users. However, it is important to acknowledge that service providers (i.e., Google) can indeed be perceived as trustworthy and caring while using that perception for their gain. Understanding this requires looking at the notion of privacy from both parties' perspectives while considering the power dynamics between them.

For instance, from the service provider's point of view, one of the goals would be to increase trust to maintain and grow its user base. As we observed, offering privacy controls could be a viable option for Google to increase trust. However, the availability of privacy controls does not automatically mean adoption. In fact, our findings imply that increasing users' trust would benefit Google in two ways. First, increasing trust would motivate users (primarily non-technical users) to adopt the "sharing" controls that do not restrict the usage of shared data. Second, increasing trust would lead users to keep the defaults of "usage" controls, allowing Google to leverage shared data across Google services, which is crucial for its Ad-revenue based business model. As such, making privacy controls available for users can help Google sit on top of the power dynamics while increasing trust, thereby giving more control over its user base regarding data collection and service personalization. However, this could threaten users' privacy due to overtrusting Google.

On the other hand, our qualitative findings underscore users' concerns over data submitted to Google and their lack of trust in Google's data privacy protection. Our participants expressed concerns over Google's data collection strategies, indicating a plausible "undertrust" scenario. Unfortunately, suspicion about Google's ulterior motives, which can lead to undertrusting Google, can cause users to avoid the available privacy controls as well (even if Google offers "usage" controls). As per our findings, undertrusting Google can induce privacy avoidance behavior, as suggested by the lower adoption rate of the privacy controls and participants questioning the privacy controls' e cacy.

Ideally, from a privacy perspective, we do not want users to overtrust or undertrust the service providers. Instead, a notion of appropriate trust is crucial for the mindful adoption of privacy. We argue that ensuring user data privacy will require a combined effort, which cannot be achieved by the service providers or end-users alone. Towards that, privacy researchers need to develop privacy risk communication and mitigation strategies ensuring that users' trust is calibrated at an appropriate level, thereby promoting informed privacy decision-making. Users' individual differences need to be considered while designing and testing these strategies, as differences such as technical vs. non-technical and adopters vs. non-adopters can lead to differences in trust. Further, government policymakers must investigate ways to address the differential power dynamics between service providers and end-users. For instance, legislatures need to look at policies that can prevent service providers from offering "sharing" controls merely as a trust-building strategy. Instead, regulations should push service providers to offer more "usage" controls to their users to give more control over data shared with them.

Additionally, we noticed a subtle but significant association between the controls' purpose of "sharing" vs. "usage" and users' trust perception, where non-technical adopters of the "sharing" controls indicate more trust towards Google than non-technical non-adopters of "sharing" controls. However, non-technical adopters of the "usage" controls indicate less trust than their non-adopter counterparts. Brandimarte et al. argued that the nuanced distinction between "sharing" and "usage" is likely hard to be perceived by general consumers, as suggested by the research on bounded rationality [59] and level-k thinking [23, 35]. Failure to engage in conditional thinking to understand such differences between "sharing" vs. "usage" opens the door for the service providers to offer "sharing" controls as a means to mislead users while continuing unrestricted data collection and usage [16]. Thus, end-users need to be educated about these nuanced differences in the privacy controls' underlying purpose of "sharing" vs. "usage" to engage in a more informed privacy control adoption decision-making.

Although our work investigated privacy-trust interrelation in Google's context, we expect the implications of our findings to apply to other service providers (especially with brand trust), as offering privacy controls has become a common practice adopted by the industry. Our findings align with prior efforts that investigated privacy controls in different contexts and noted that the availability of privacy controls can enhance users' trust [61, 74] while manipulating users towards practices that benefit service providers in terms of data collection [2, 28]. Furthermore, prior works that looked at disclosure settings observed a similar effect of overtrusting the SNS provider, despite the provided controls (i.e., "sharing" controls) not restricting data usage by the provider in any way [16]. Hence, the overtrust and understrust effects we observed in Google's context are very likely to be present for other service providers. As such, the skewness in the power dynamics between the service providers and the consumers and the service providers' control over user data should be considered a threat to user data privacy and call for close attention.

5.2 Nuanced e ect of Technical Literacy and Trust on Privacy Control Adoption

Our findings suggest that non-technical participants are more likely to use non-default settings and stricter privacy options than technical participants. While counterintuitive, this is in line with prior

work showing that a more articulated mental model enables technical users to rely on rational cost-benefit analysis-oriented decision-making strategies [27, 37]. Our qualitative findings support this argument where technical participants more frequently justified trusting Google based on rational profit motive calculations. Comments showed that technical participants often questioned the effectiveness of the controls as Google's data-centric business model directly conflicts with the controls' purposes. These findings suggest a possibility that technical participants' privacy control adoption decision-making is more likely to be influenced by the privacy-calculus-based rational risk-benefit trade-off calculation. From quantitative analysis, technical participants were found to trust Google's integrity and benevolence significantly less than their non-technical counterparts. As such, lower trust perception is likely to contribute to the observed negative attitude towards Google that led them to question the controls' e cacy. The perception that the controls may not be doing what they are supposed to do can subsequently lower the perceived benefit of using these controls among the technical participants. From a privacy-calculus perspective, it implies that, even after seeing the risk of data collection, technical participants may not be willing to adopt the privacy controls, similar to what we observed in this study. Prior works also support this conjecture showing that trust affects the perception of the usefulness of the protective measures offered by service providers [7]. In addition, prior efforts suggest that lower trusting belief will likely decrease users' confidence towards the service provider and subsequently lead to prevention-focused behavior (e.g., asking for data retrieval, not providing data for personalized services) [46]. Thus, due to higher risk perception and lower confidence in Google's data practices, technical participants are more likely to rely on downstream privacy behavior and restrict themselves from providing personal data to Google rather than relying on the privacy controls and choices offered by Google. Protection Motivation Theory (PMT) suggests that users constantly try to protect themselves from threats by adopting protective measures to minimize the (privacy) risks [54]. In line with PMT, prior research confirms that consumers respond to privacy threats by adopting protective measures such as fabricating or falsifying data submitted online or withholding data altogether [45]. Thus, privacy-calculus-based approaches focusing on communicating the e cacy of the privacy controls while addressing the shortcomings can help reduce technical participants' negative attitudes towards the service provider and subsequently lead to a higher perceived benefit of the privacy controls in order for them to adopt the controls proactively.

Compared to technical participants, non-technical participants perceived Google's higher integrity and benevolence, which seemed to play an important role in adopting Google's privacy controls at a higher rate in this user group. Thus, from Google's point of view, maintaining trust can be beneficial to make this user group adopt the offered privacy features. Towards that, identifying and addressing the trust-dampening factors should help to develop and maintain trust. However, caution should be taken so that trust-building strategies do not lead to inappropriate trust (i.e., overtrust), potentially leading to privacy violations. The proposition of inappropriate trust in the context of Google has recently been investigated by Balash et al., showing that trust in Google was inappropriately transferred towards the third-party services that were authorized with Google's Single Sign-on (SSO) services, making users vulnerable to security and privacy risks [9]. Prior research also suggests that overtrust may make users feel that the service provider is only responsible for protecting them, pushing them towards negligence or retirement from privacy protection activities [24]. Non-technical participants, due to their higher trust perception, may fall into this risky territory, which should be carefully considered in the organizations' trust-related promotional activities.

It is worth noting that users do not view the privacy risks of different data equally, which is evident from the difference in adoption rate for different controls. In particular, we noticed that the adoption of *Location history* control does not match the adoption of *Ad personalization* control and vice versa. This observation underscores the need for context-specific communication while promoting trust and privacy controls. Specifically, instead of designing promotions following a "one-size-fits-all" strategy, service providers need to promote individual privacy settings considering the utility of each specific setting and users' context.

5.3 E ect of the Purpose of Controls ("Sharing" vs. "Usage") on Privacy

While several prior efforts looked into the adoption behavior of privacy control in the context of social networking sites (SNS), the choices investigated in SNS settings often fall under the category of "sharing" controls. Prior literature pointed out that "sharing" controls may be "illusory" as they do not give users control over how the shared data can be accessed or used even though the offerings evoke a perception of control and help build trust [16]. In our case, while technical adopters and non-adopters did not differ much in their perception of trust, we observed a crucial interaction of trust and control adoption among the non-technical group. Among the non-technical participants, adopters of the "sharing" controls perceived Google's integrity and benevolence significantly more than the non-adopters of these controls. However, this interaction was reversed for the "usage" controls, where non-technical adopters indicated a lower perception of Google's integrity and benevolence than non-adopters. This reversed interaction indicates that less trusting belief is likely to influence non-technical users, who are concerned about Google's data collection and sharing strategies, to adopt the "usage" controls that restrict shared data from being used by Google for providing targeted advertisements and personalized services (e.g., personalized Maps). Our findings complement prior efforts that suggest that trust is crucial in determining willingness to share personal data and use personalized services in return [45].

It is worth noting that the difference is observed in the adoption behavior of non-technical participants but not among the technical participants. Due to the low overall trust towards Google, technical participants' adoption decision is more likely to be influenced by their rational risk-benefit analysis suggested by PMT [54], and their perceptions of the e cacy of the controls. Nonetheless, the distinctive reverse interplay of trust-privacy adoption contributes to the literature. It confirms the trust-literacy requirements for promoting privacy adoption based on the underlying purpose of the controls. Further, the observed interactions can guide privacy researchers to develop effective trust-building, trust-repairing, and trust-calibrating mechanisms that consider the privacy control's

underlying purposes. For example, communicating that a "sharing" control can be limited in terms of how the service providers may use collected data can help address the issue of overtrusting the service provider that we observed among the non-technical participants. Subsequently, informing users about how adopting "usage" controls can increase control over how the service providers can use the shared data can help reduce data concerns and work as a trust-building mechanism.

5.4 Design Recommendations Promoting Trust and Privacy Control Adoption

Our findings suggest several antecedents, including the business strategies (e.g., data collection for monetization) and shortcomings of the current implementations, that made participants question their perceptions of trust towards Google. Based on the results, we recommend the following changes to the current practices that can help build a better trusting provider-consumer relationship while promoting the usage of privacy controls.

First, looking closely at the trust-dampening factors showed that users are often concerned about obscure data collection practices and unclear regarding the type of data being collected and how the collected data is potentially being used. Profit motives further exacerbate the psychological discomfort and distrust around these issues. As such, service providers need to make the data collection and usage policies easier to locate and comprehend. In doing so, the traditional long-text privacy policy approach should be avoided as literature shows that these policy documents are mostly ignored due to their long length and hard-to-understand language [49]. As alternatives to the long-text policy documents, researchers suggest approaches such as privacy "nutrition" labels and privacy dashboards which were shown to be easier to read and understand [34, 39]. Literature on trust suggests that transparency and clarity regarding data collection and usage practices impact positive attitudes towards the entity, heighten the entity's behavioral integrity perceptions, and help build trust [45, 46]. Hence, to build and maintain trusting relationships, service providers can leverage transparent communication with the collection of user data and subsequent usage and disclosures of such data. This can further be an effective means of repairing user trust when trust is decreased due to a violation of privacy by security breach incidents [7, 8, 11, 45]. In the post-data breach scenarios, communication regarding protective actions taken to prevent future data violations has been shown effective in maintaining and repairing users' trust perception [7, 8]. However, companies should be careful in preventing any inconsistency between their words and subsequent actions they take, as words without noticeable actions can be considered "cheap talk" and lead to lower trust perceptions [7].

Second, participants often mentioned that they had to opt out to stop data collection and tracking, which negatively affected their trust in Google. Further, some participants complained about privacy settings being overridden without notification. As the decision-making process is susceptible to "default effect" (decision being influenced by default settings) [5, 55], to promote proactive privacy behavior, it might be a good idea for service providers to set the default settings to more privacy conservative options, and give users the control to make the decisions whether they want data to be collected for better personalization. Such a strategy can go a long way in demonstrating "goodwill" on the company's part.

Third, many participants were skeptical about the e cacy of the privacy controls. Interestingly, even after being aware of the availability of privacy controls, many technical participants expressed doubt about whether the tools effectively restrict Google from collecting data, given that Google's business model largely depends on users' data. Notably, multiple participants expressed confusion regarding whether enabling a setting will stop data collection or not. To instill trust, service providers must address such skepticism and clearly communicate the e cacy and limitations of the privacy controls in different contexts to give users confidence in using them for privacy protection. Communication of the limitations of the privacy controls can help reduce overtrust, especially among non-technical participants.

Fourth, participants were often suspicious about Google possibly collaborating with Government and sharing users' personal data, and selling collected data to third parties for profit. It is di cult to say whether these allegations are, in fact, true or not. Nonetheless, service providers should be upfront about such possibilities and have a moral obligation to their users to disclose under what circumstances such sharing of collected data with third parties (either Government or private entities) may occur. Service providers cannot expect users to trust them and follow their recommended practices while perceived as malicious. To avoid such concerns, service providers may provide transparency reports to end-users along with policy documents. These documents should include whether and how user data may be shared with law enforcement and other legal obligations that a service provider must follow by law. For example, in Google's case, a transparency report is available online for the end-users. Nonetheless, it is necessary to communicate the presence of such documents with end-users and address their most raised concerns by keeping these documents up-to-date.

5.5 Addressing Trust Resulting from Misconception about Technology

Multiple non-technical participants expressed a certain degree of misconceptions about privacy protection and technology in general, which contributed as a positive factor to their trust ratings. For instance, one non-technical participant erroneously argued about the lack of sensitivity of the collected data (*"I don't mind as long as what they record and track isn't personal such as social security numbers, credit card info, etc." (NT)*). Another participant indicated a lack of understanding regarding how location data is tracked and used by Google in the following comment.

"I feel that when using Google maps I am tracked because they ask for my destination. However, I don't think that is too harmful when I am always on the move." (NT)

While misconceptions can lead to trust, they can also create a false sense of security and make users vulnerable to compromise. In the long run, negative consequences due to erroneous understanding regarding technology can backfire and make users even more suspicious of technology and service providers. Therefore, such misconceptions should be carefully identified and addressed by the service providers proactively.

5.6 Limitations of the Study

While we took several steps to ensure the study's internal validity (e.g., using prescreening questionnaire and attention check questions), our findings should be interpreted with the following limitations in mind.

First, we restricted our participants to the adult population who currently live in the United States and have the technical ability to use MTurk, which may not be a representative population of the United States.

Second, to account for the possible effects of control types on privacy control adoption, we looked at four privacy settings offered by Google to keep the study tractable. However, other controls offered by Google can be perceived differently than the ones we picked. As such, the adoption of those controls may not align with the adoption behavior we noticed for the four controls we considered. Further, privacy controls across other tools and platforms (e.g., Facebook) may be perceived and adopted differently. Therefore, while we expect the trend in our findings to hold in general, our findings need to be interpreted accordingly.

Third, in this study, We asked participants to report their current settings (i.e., behavioral measurement) instead of taking self-reports of whether they use a particular privacy control and defined adopting a privacy control as changing the current setting of a privacy control from the default setting, which is usually the least restrictive option. This definition labels participants who kept the default options as non-adopters of the controls.

However, behavioral measurement alone does not report the underlying reasons behind the observed behavior; in our case, the reason behind keeping the defaults. Hence, keeping the default value may indicate one of several possibilities. For instance, it is possible that the participant is unfamiliar with the control or knows about it but decided not to change the default value. Suppose, a participant kept the default because they were unaware of the privacy controls. In that case, it is likely to be an outcome of a lack of concern over data privacy facilitated by a low perceived data value or higher trust perception towards the service provider. Our findings indicate a higher trust perception towards Google among the non-adopters, while prior efforts indicate that higher trust can indeed lower users' concern over privacy [18, 73]. Hence, the implications of our findings apply to this user group, where we noticed a notion of overtrust among the non-technical participants.

On the other hand, if a participant knew about the controls but chose not to change the defaults, there might be different reasons for that. Our qualitative findings hint at some of these reasons where participants (especially the technical participants) question the controls' e cacy or think that the controls contradict Google's data-centric business model, indicating a likelihood that these participants would not interact with the options even after knowing their existence. Similarly, our quantitative analysis shows that technical participants more frequently kept the defaults than non-technical participants, which can result from such concerns. Hence, not proactively adopting the controls by changing the defaults may not indicate a lower privacy risk perception, especially among the technical participants, as discussed in the paper. Either way, we argue that participants who retain the default values are likely to be different in their privacy decision-making compared to participants who take the initiative to change the default values, indicating a higher degree of initiative and motivation in taking control of their privacy. Due to this, irrespective of the underlying reasons behind not changing the default value, we considered default users as non-adopters of the privacy controls. Nonetheless, we realize that there can be some differences in perception of privacy and trust among these fine-grained groups of non-adopters based on the reasons behind keeping default values that we did not consider separately to keep the study tractable at this stage, which can be examined in future efforts.

Fourth, drawing on prior works, in this work, we used "other" as an option for the participants to report their gender. However, using "other" as an option can be exclusionary to anyone who is gender-queer or whose birth sex does not fall within the binary [62]. While this does not affect our findings, our demographic may not accurately reflect the complete gender distribution of the participants.

6 CONCLUSION

In this work, we explored how the adoption of privacy controls varies between technical and non-technical participants based on the purpose of the controls and trust perceptions towards the service providers. Our findings confirm that trust perceptions are indeed related to adoption behavior and vary based on technical literacy. Furthermore, from the qualitative data analysis, we identified factors that enhance or dampen trust in Google's data privacy protection and their divergence based on technical literacy. Finally, based on our findings, we outlined possible strategies to develop trust relationships with end-users and help promote the mindful adoption of privacy controls.

ACKNOWLEDGMENTS

This research was supported by a NSF CAREER award to the second author, 1750908.

REFERENCES

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. 2019. More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 451–466.
[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.
[3] Idris Adjerid, Alessandro Acquisti, and George Loewenstein. 2019. Choice architecture, framing, and cascaded privacy choices. *Management science* 65, 5 (2019), 2267–2290.
[4] Gabe Turner Aliza Vigderman. 2022. The Data Big Tech Companies Have On You. (2022). https://www.security.org/resources/data-tech-companies-have/
[5] Reza Ghaiumy Anaraky, Tahereh Nabizadeh, Bart P Knijnenburg, and Marten Risius. 2018. Reducing default and framing effects in privacy decision-making. *SIGHCI 2018 Proc. Assoc. for Info. Sys.(AIS), Atlanta, GA, USA* 7 (2018).
[6] Angelo Antoci, Laura Bonelli, Fabio Paglieri, Tommaso Reggiani, and Fabio Sabatini. 2019. Civility and trust in social media. *Journal of Economic Behavior & Organization* 160 (2019), 83–99.
[7] Emmanuel Ayaburi, Francis Andoh-Baidoo, and Jae Ung Lee. 2020. Post Data Breach Use of Protective Technologies: An Examination of Users' Dilemma. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.
[8] Emmanuel W Ayaburi and Daniel N Treku. 2020. Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management* 50 (2020), 171–181.
[9] David G Balash, Xiaoyuan Wu, Miles Grant, Irwin Reyes, and Adam J Aviv. 2021. Security and Privacy Perceptions of Third-Party Application Access for Google Accounts (Extended Version). *arXiv preprint arXiv:2111.03573* (2021).
[10] Ruwan Bandara, Mario Fernando, and Shahriar Akter. 2020. Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. *Journal of Retailing and Consumer Services* 52 (2020), 101947.

[11] Gaurav Bansal and Noah Redfearn. 2019. Trust Violation and Rebuilding After a Data Breach: Role of Environmental Stewardship and Underlying Motives. *Journal of the Midwest Association for Information Systems| Vol* 2019, 2 (2019), 45.

[12] Miriam Bartsch and Tobias Dienlin. 2016. Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior* 56 (2016), 147–154.

[13] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. 2017. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication* 67, 1 (2017), 26–53.

[14] Zinaida Benenson, Freya Gassmann, and Lena Reinfelder. 2013. Android and iOS users' differences concerning security and privacy. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. 817–822.

[15] Adam J Berinsky, Gregory A Huber, and Gabriel S Lenz. 2012. Evaluating online labor markets for experimental research: Amazon. com's Mechanical Turk. *Political analysis* 20, 3 (2012), 351–368.

[16] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* 4, 3 (2013), 340–347.

[17] Visualcapitalist.com Carmen Ang. 2022. How Do Big Tech Giants Make Their Billions? (2022). https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/

[18] Eve M Caudill and Patrick E Murphy. 2000. Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing* 19, 1 (2000), 7–19.

[19] Kuanchin Chen and Alan I Rea Jr. 2004. Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems* 44, 4 (2004), 85–92.

[20] European Commission. 2018. EU Data Protection Rules. (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[21] Federal Trade Commission. 2009. CAN-SPAM Act: A Compliance Guide for Business. (2009). https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

[22] Federal Trade Commission. 2017. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. (2017). https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

[23] Vincent P Crawford. 2003. Lying for strategic advantage: Rational and boundedly rational misrepresentation of intentions. *American Economic Review* 93, 1 (2003), 133–149.

[24] Shelby R Curtis, Jessica Rose Carre, and Daniel Nelson Jones. 2018. Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal* (2018).

[25] Ralf De Wolf, Koen Willaert, and Jo Pierson. 2014. Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook. *Computers in Human Behavior* 35 (2014), 444–454.

[26] Kenan Degirmenci. 2016. Trust-promoting seals in green information systems: the case of smart meters and privacy. (2016).

[27] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*. 59–75.

[28] Florian M Farke, David G Balash, Maximilian Golla, Markus Dürmuth, and Adam J Aviv. 2021. Are Privacy Dashboards Good for End Users? Evaluating User Perceptions and Reactions to Google's My Activity. In *30th USENIX Security Symposium (USENIX Security 21)*. 483–500.

[29] Yang Feng and Quan Xie. 2019. Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps. *Journal of Interactive Advertising* 19, 1 (2019), 43–57.

[30] Andy Field. 2013. *Discovering statistics using IBM SPSS statistics*. sage.

[31] C Bryan Foltz and Laura Foltz. 2021. MUIPC and intent to change IoT privacy settings. *Journal of Computing Sciences in Colleges* 36, 7 (2021), 27–38.

[32] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To disclose or not to disclose: examining the privacy decision-making processes of older vs. younger adults. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[33] Cathy Goodwin. 1991. Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing* 10, 1 (1991), 149–166.

[34] Eelco Herder and Olaf van Maaren. 2020. Privacy dashboards: the impact of the type of personal data and user control on trust and perceived risk. In *Adjunct publication of the 28th ACM conference on user modeling, adaptation and personalization*. 169–174.

[35] Teck-Hua Ho, Colin Camerer, and Keith Weigelt. 1998. Iterated dominance and iterated best response in experimental" p-beauty contests". *The American Economic Review* 88, 4 (1998), 947–969.

[36] Donna L Hoffman, Thomas P Novak, and Marcos Peralta. 1999. Building consumer trust online. *Commun. ACM* 42, 4 (1999), 80–85.

[37] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. 327–346.

[38] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 39–52.

[39] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

[40] Paul E Ketelaar and Mark Van Balen. 2018. The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior* 78 (2018), 174–182.

[41] Hanna Krasnova, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. 2010. Online social networks: Why we disclose. *Journal of information technology* 25, 2 (2010), 109–125.

[42] Hanna Krasnova and Natasha F Veltri. 2010. Privacy calculus on social networking sites: Explorative evidence from Germany and USA. In *2010 43rd Hawaii international conference on system sciences*. IEEE, 1–10.

[43] Lydia Kraus, Ina Wechsung, and Sebastian Möller. 2017. Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications* 34 (2017), 34–45.

[44] J Richard Landis and Gary G Koch. 1977. The measurement of observer agreement for categorical data. *biometrics* (1977), 159–174.

[45] Emmanuel Elioth Lulandala. 2020. Facebook Data Breach: A Systematic Review of Its Consequences on Consumers' Behaviour Towards Advertising. *Strategic System Assurance and Business Analytics* (2020), 45–68.

[46] May O Lwin, Jochen Wirtz, and Andrea JS Stanaland. 2016. The privacy dyad: antecedents of promotion-and prevention-focused online privacy behaviors and the mediating role of trust and privacy concern. *Internet Research* (2016).

[47] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[48] Kristin Masuch, Maike Greve, and Simon Trang. 2021. What to do after a data breach? Examining apology and compensation as response strategies for health service providers. *Electronic Markets* 31, 4 (2021), 829–848.

[49] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[50] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. 2002. Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research* 13, 3 (2002), 334–359.

[51] Miriam J Metzger. 2006. Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research* 33, 3 (2006), 155–179.

[52] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. sage.

[53] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. 2020. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*. 89–108.

[54] Ronald W Rogers and Steven Prentice-Dunn. 1997. Protection motivation theory. *Handbook of health behavior research 1: Personal and social determinants* (1997), 113–132.

[55] William Samuelson and Richard Zeckhauser. 1988. Status quo bias in decision making. *Journal of risk and uncertainty* 1, 1 (1988), 7–59.

[56] Stuart Schechter. 2013. Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them. *Microsoft, January* (2013).

[57] Hadas Schwartz-Chassidim, Oshrat Ayalon, Tamir Mendel, Ron Hirschprung, and Eran Toch. 2020. Selectivity in posting on social networks: the role of privacy concerns, social capital, and technical literacy. *Heliyon* 6, 2 (2020), e03298.

[58] Semrush.com Shelley Walsh. 2021. 50 Google Search Statistics & Facts. (2021). https://www.semrush.com/blog/google-search-statistics/

[59] Herbert A Simon. 1990. Bounded rationality. In *Utility and probability*. Springer, 15–18.

[60] Datareportal.com Simon Kemp. 2021. Digital 2021: Global Overview Report. (2021). https://datareportal.com/reports/digital-2021-global-overview-report

[61] H Jeff Smith, Tamara Dinev, and Heng Xu. 2011. Information privacy research: an interdisciplinary review. *MIS quarterly* (2011), 989–1015.

[62] Katta Spiel, Oliver L Haimson, and Danielle Lottridge. 2019. How to do better with gender on surveys: a guide for HCI researchers. *Interactions* 26, 4 (2019), 62–65.

[63] Deepesh Kumar Srivastava and Basav Roychoudhury. 2021. Understanding the Factors that Influence Adoption of Privacy Protection Features in Online Social Networks. *Journal of Global Information Technology Management* 24, 3 (2021), 164–182.

[64] Statcounter.com. 2022. Search Engine Market Share Worldwide - August 2022. (2022). https://gs.statcounter.com/search-engine-market-share

[65] Artur Strzelecki and Mariia Rizun. 2022. Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability* 14, 10 (2022), 5866.

[66] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. *arXiv preprint arXiv:2202.14036* (2022).
[67] Jennifer Fries Taylor, Jodie Ferguson, and Pamela Scholder Ellen. 2015. From trait to state: Understanding privacy concerns. *Journal of Consumer Marketing* (2015).
[68] Eric Tutu Tchao, Kwasi Diawuo, Christiana Selorm Aggor, and Seth Djane Kotey. 2017. Ghanaian Consumers Online Privacy Concerns: Causes and its Effects on E-Commerce Adoption. *arXiv preprint arXiv:1801.01086* (2017).
[69] Richard H Thaler, Cass R Sunstein, and John P Balz. 2013. *Choice architecture.* Vol. 2013. Princeton University Press Princeton, NJ.
[70] Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J Rifon, and Shelia R Cotten. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 59 (2016), 138–150.
[71] California State Legislature Website. 2018. SB-1121 California Consumer Privacy Act of 2018. (2018). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
[72] Wenjing Xie and Kavita Karan. 2019. Consumers' privacy concern and privacy protection on social network sites in the era of big data: Empirical evidence from college students. *Journal of Interactive Advertising* 19, 3 (2019), 187–201.
[73] Heng Xu and Hock-Hai Teo. 2004. Alleviating consumers' privacy concerns in location-based services: a psychological control perspective. *ICIS 2004 proceedings* (2004), 64.
[74] Heng Xu, Hock-Hai Teo, and Bernard Tan. 2005. Predicting the adoption of location-based services: the role of trust and perceived privacy risk. (2005).
[75] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information systems research* 23, 4 (2012), 1342–1363.
[76] Susumu Yamaguchi. 2001. Culture and control orientations. *The handbook of culture and psychology* (2001), 223–243.
[77] Tao Zhou. 2011. The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems* (2011).
[78] Moshe Zviran. 2008. User's perspectives on privacy in web-based applications. *Journal of Computer Information Systems* 48, 4 (2008), 97–105.

A APPENDIX

A.1 Supporting Data

A.1.1 Demographic distribution. Table 5 show participants' demographic information and distribution across our two different groups. Statistical analysis showed that the groups were demographically similar, as presented in the section 4.

A.1.2 Trust and adoption of the controls. We observed a differential effect of technical literacy on the association between trust measures and adoption of the controls. Compared to technical participants, non-technical users were found to vary in terms of posing trust towards Google, as reported in section 4.2.2. All of the observed significant statistics of these effects are summarized and presented in Table 2. Also, the descriptive statistics between the groups for all of the significant effects are presented in Table 6 to show the compete picture of the effects and the direction of association.

A.2 Survey Instruments and Scales

We measured participants' technical literacy using the Technical Knowledge of Privacy Tools Scale used in Kang et al's work [38]. The scale consists of 6 statements that is either true or false. The scale is presented in Table 7, the correct answers are marked for readability.

We measured trust towards Google using McKnight et al.'s technology Trusting Belief scale (using 7-point Likert items (Strongly disagree to Strongly Agree)), which consist of three dimensions: *integrity*, *competence*, and *benevolence* [50]. Items were presented in random orders to the participants.

In addition, To understand what factors affect this trust perception, we asked participants to mention their reasoning behind trusting Google's privacy protection, which were used for Qualitative analysis. The items for measuring trust is presented in Table 8.

A.3 Survey Questionnaire

A.3.1 Prescreening Questionnaire. Prescreening questions to check eligibility. The selection criteria is highlighted in bold. Two additional questions were asked to prevent participants from guessing the eligibility criteria. Participants answer to these two questions did not matter for eligibility.

(1) Are you proficient in English? Options: **Definitely yes**, Probably yes, Might or might not, Probably not, Definitely not
(2) Do you have a degree in Computer Science, including a "minor," or any professional computer science certifications? Options: Yes, **No**
(3) Do you own a personal computer that is not used for official/business related work and only used for personal purposes (e.g., web browsing, entertainment, education, self-employment, personal banking, online bill payment, other online services etc.)? Options: **Yes**, No
(4) What kind of personal computer do you have that you use for only personal purposes (e.g., web browsing, entertainment, education, self-employment, personal banking, online bill payment, other online services etc.)? Options: **Windows**, Mac, Linux, Other (Please specify), I do not own a personal computer
(5) What kind of personal smartphone do you use? Options: iPhone, **Android**, Other (Please specify), I do not use a personal smartphone
(6) Approximately how many hours a day do you typically browse Internet on your personal devices (e.g., personal computer, smartphone etc.)? Options: Less than 1 hour, 1-3 hours, 4-10 hours, 11-16 hour, More than 16 hours (*This question did not contribute to eligibility*)
(7) Which of the following browsers do you use? You can select more than one if you use multiple different browsers. Options: Edge, Firefox, **Chrome**, Safari, Other (Please specify), I do not have any favorite browser of choice
(8) Do you have a personal Google account that you use to login to different Google services (e.g., Gmail, Google maps, Google drive, Google photos, etc.)? Options: **Yes**, No, I am not sure
(9) Do you use two-step verification (2-FA) for your personal Google account? Options: Yes, No, I am not sure (*This question did not contribute to eligibility*)

A.3.2 Main Survey. Eligible participants from the prescreening survey took the main survey. Participants were randomly assigned to one of our two groups: "sharing": Participants reported setting for "sharing" controls; "usage": Participants reported setting for "usage" controls. Main survey questionnaire:

Measurement of Technical Literacy (Same for "sharing" and "usage"): Participants technical literacy is measured using the Technical Knowledge of Privacy Tools Scale shown in Table 7.

Group	Technical Literacy Level	Age	Gender Breakdown
"sharing" group	Technical	M = 37.2, Mdn = 35.5, SD = 10.1	21 Male, 13 Female
	Non-Technical	M = 40.6, Mdn = 38, SD = 11	31 Male, 39 Female, 1 Prefer not to answer
		N = 105	
"usage" group	Technical	M = 38.5, Mdn = 36, SD = 9.5	22 Male, 8 Female, 1 Other
	Non-Technical	M = 37.1, Mdn = 33, SD = 10.3	38 Male, 35 Female
		N = 104	
	Total	N = 209	

Table 5: Participant demographics

Non-technical Participants				
Control Purpose	**Privacy Control**	**Trust Integrity**	**Trust Competence**	**Trust Benevolence**
Sharing	Browser history (post-hoc: within a week vs. within three months)	**F**: $M = 4.8, Mdn = 5.33, SD = 1.2$ **L**: $M = 4, Mdn = 4, SD = 1.2$	*NS*	**F**: $M = 4.6, Mdn = 4.67, SD = 1.3$ **L**: $M = 3.7, Mdn = 4, SD = 1.1$
Sharing	Browser history (post-hoc: within a month vs. within three months)	*NS*	*NS*	**F**: $M = 4.6, Mdn = 4.67, SD = 1.1$ **L**: $M = 3.7, Mdn = 4, SD = 1.1$
Usage	Location history	*NS*	*NS*	**N**: $M = 5.3, Mdn = 5.33, SD = 1.4$ **U**: $M = 4.6, Mdn = 5, SD = 1.3$
Usage	Ad personalization	**N**: $M = 5.1, Mdn = 5.33, SD = 1.2$ **U**: $M = 4.3, Mdn = 4.67, SD = 1.5$	*NS*	**N**: $M = 5.1, Mdn = 5.33, SD = 1.3$ **U**: $M = 4.14, Mdn = 4, SD = 1.3$

Table 6: Descriptive statistics of the signi□cant trust-adoption associations. (N: non-adopters; U: proactive adopters, F: frequent adopters - uses weekly/monthly, L: less frequent adopters - uses in three months). The symbol *NS* indicates non-signi□cant results

Measurement of Trust (Same for "sharing" and "usage"): Participants trust perceptions towards Google is measured using the questionnaire shown in Table 8.

Measurement of Privacy Control Adoption: "sharing" group

1. Privacy Control: Browser history:

(1) Are you familiar with the control "Clear Browsing history" present in the chrome browser? Options: Yes, No, I am not sure
(2) Have you ever used "Clear Browsing history" control in the chrome browser? Options: Yes, No (If "Yes" to the previous questions)
(3) When was the last time you used "Clear Browsing history" in your chrome browser? Options: In a day, In a week, In two weeks, In a month, In three months, Other (Please specify) (If "Yes" to the previous questions)

2. Privacy Control: Cookies:

(1) Are you familiar with the control that lets you block cookies in the chrome browser? Options: Yes, No, I am not sure
(2) What is the current setting for blocking cookies in your chrome browser? **Here is how you can check it (Image with steps). Please submit your answer below.** Options: Allow all cookies, Block third-party cookies in Incognito, Block third-party cookies, Block all cookies, I am not able to check

Measurement of Privacy Control Adoption: "usage" group

1. Privacy Control: Location history:

(1) Are you familiar with the feature called "Activity Controls" present in your personal Google account? Options: Yes, No, I am not sure
(2) What is the current setting for "Location History" in "Activity Controls" in your personal Google Account? **Here is how you can check it(Image with steps). Please submit your answer below.** Options: Allowed with auto deletion on, Allowed with auto deletion off, Paused with auto deletion on, Paused with auto deletion off, I am not able to check

2. Privacy Control: Ad personalization:

(1) Are you familiar with the control called "Ad Personalization" present in your personal Google account? Options: Yes, No, I am not sure
(2) What is the current setting for "Ad Personalization" control in your personal Google Account? **Here is how you can check it(Image with steps). Please submit your answer below.** Options: Ad personalization turned on, Ad personalization turned off, I am not able to check

A.3.3 Demographic and End of Survey □ estionnaire.

(1) What is your age (in years)?
(2) What is your gender? Options: Male, Female, Other, I prefer not to answer

Please indicate whether you think each statement is true or false. Please select "I am not sure" if you do not know the answer.

	True	False	I am not sure
Incognito mode / private browsing mode in browsers prevents websites from collecting information about you.		✓	
Tor can be used to hide the source of a network request from the destination.	✓		
A VPN is the same as a Proxy server.		✓	
IP addresses can always uniquely identify your computer.		✓	
HTTPS is standard HTTP with SSL to preserve the confidentiality of network tra c.	✓		
A request coming from a proxy server cannot be tracked to the original source.		✓	

Table 7: Technical Knowledge of Privacy Tools Scale (reproduced from [38])

Trust Construct	Scale Item	Statement
Trust Integrity	TI1	Google is truthful in its dealings with me
	TI2	Google is honest
	TI3	Google keeps its commitments
Trust Competence	TC1	Google is competent and effective in providing the services I need
	TC2	Google performs its role of providing the services I need very well
	TC3	Google is a capable and proficient service provider that provides the services I need
Trust Benevolence	TB1	Google acts in my best interest
	TB2	Google does its best to help me if I need help
	TB3	Google is interested in my well-being, not just its own
Privacy Protection Trust (Qualitative)		Please briefly describe your reasoning behind trusting Google in protecting your privacy across different Google services (e.g., chrome, maps, gmail, photos, drive etc.). Please point down the factors (both positive and negative) that contribute to your rating

Table 8: Scale items used to measure di erent construct of Trust towards Google (items are borrowed and adapted from [50])

(3) What is the highest level of education you have received? Options: Less than high school, High School graduate or GED, Some college, 2 year degree, 4 year degree, Master's degree, Doctoral degree, Professional degree
(4) Do you have any other comments or feedback about the study?

A.4 Images with Steps to Report Privacy Control Settings

A.4.1 Steps to Report sharing Control se ings. The step by step guide to report "Cookies" setting is presented in Figure 8

A.4.2 Steps to Report usage Control se ings. The step by step guide to log in to Google account is shown in Figure 5. Guide to report "usage" control settings is presented in Figures 6 and 7

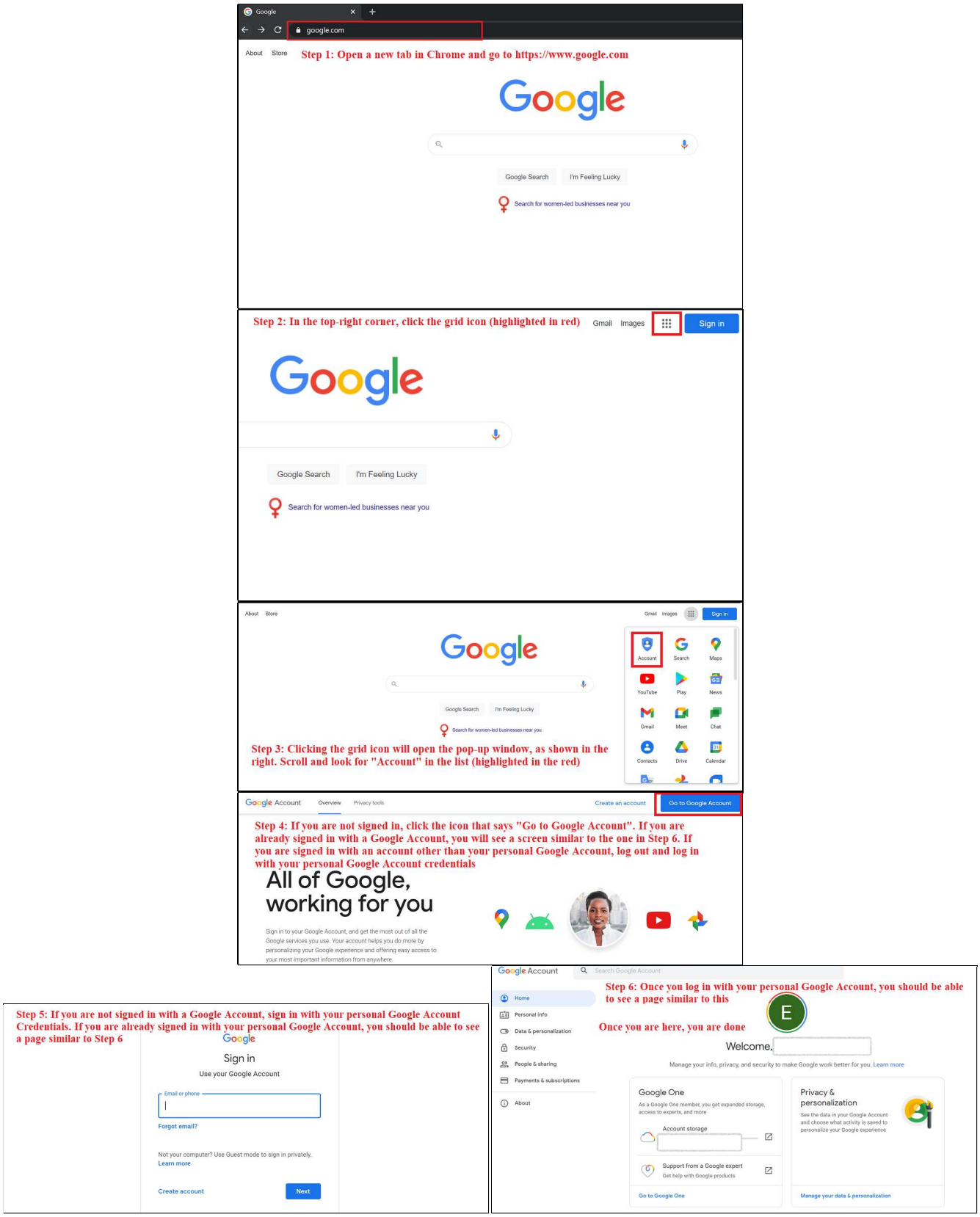

Figure 5: Steps to open Google Account

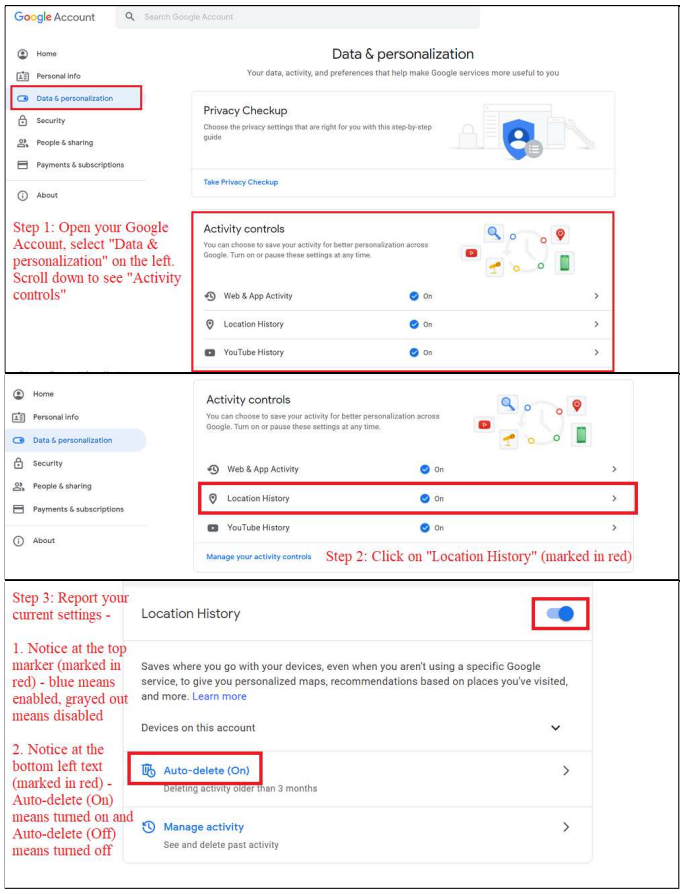

Figure 6: Steps to report "Location history" control settings

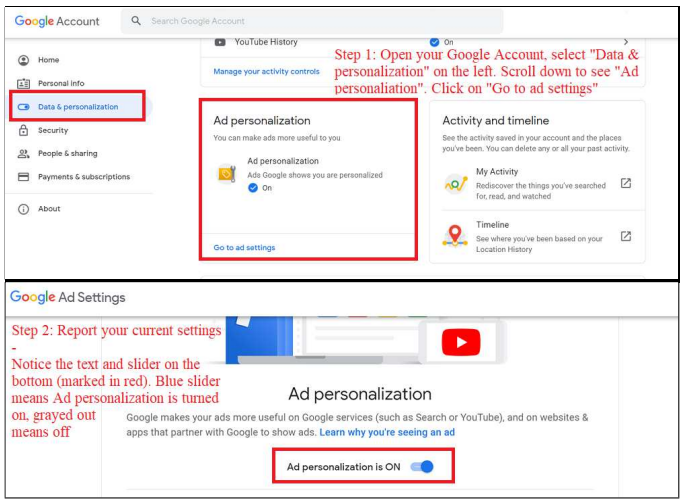

Figure 7: Steps to report "Ad personalization" control settings

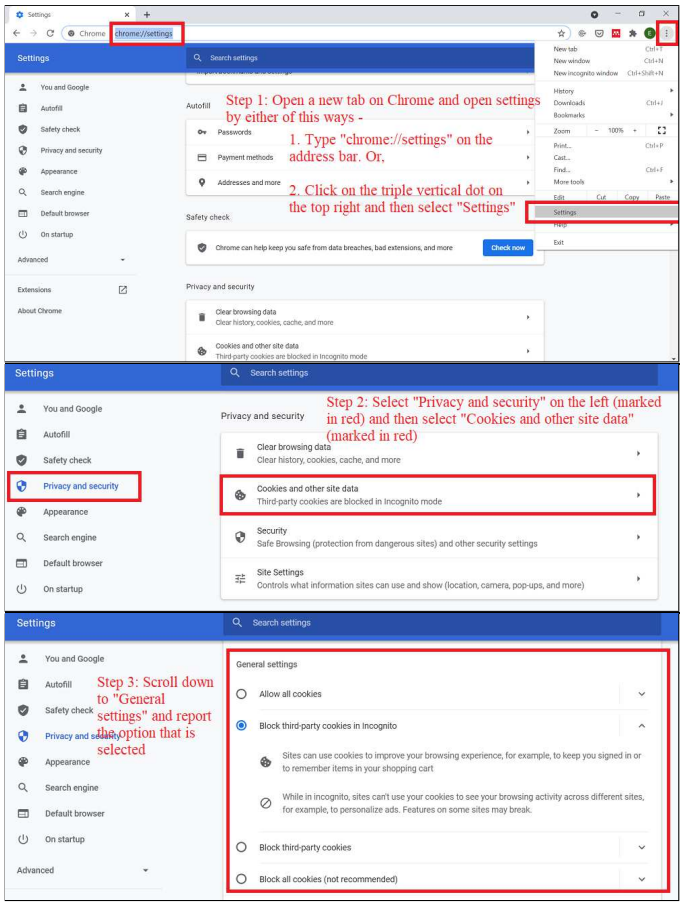

Figure 8: Steps to report "Cookies" control settings