Information & Computer Security

Users' activity logs: the good, the bad, the misconception and the disastrous

Eman Alashwali
Department of Information Systems, King Abdulaziz University, Jeddah, Saudi Arabia

Received 29 December 2025
Revised 1 March 2026
Accepted 20 April 2026

Abstract

Purpose – Most prior studies focused on the negative side of users' activity logs, such as users' lack of awareness about the logs' privacy controls and users' privacy concerns about their data. This paper aims to provide a balanced view of users' perceptions regarding activity logs by considering the positive, negative and extremely negative sides, as well as the misconceptions of activity logs.

Design/methodology/approach – The author conducted a secondary analysis of interview data from 30 Google personal account holders in Saudi Arabia. Using template analysis, the author analyzed the data from the lens of four key themes: the good, the bad, the misconception and the disastrous aspects of users' activity logs from the users' perspective.

Findings – Participants identified positive aspects of Google's *Activity controls*, such as saving browsing history and bookmarks, synchronization, security and safety and parental control. They also identified negative aspects, such as a lack of knowledge of Google's data practices and the presence of Google's *Activity controls*, privacy concerns and biased content. Some features, such as tailored ads, were controversial. The author identified misconceptions among participants, such as confusion between local browsing history and cloud-based activity logs and between security and privacy measures. Participants raised serious concerns about Google's *Activity controls*, such as unauthorized logins and data breaches.

Originality/value – The main contribution of this paper is offering a balanced view of users' perceptions of activity logs and providing a better understanding and a useful source for subsequent studies on related topics. The author offers a set of practical recommendations for service providers, security and privacy researchers and experts and users alike.

Keywords Privacy, Security, Policy, Settings, Data, Google, Web, Applications

Paper type Research paper

1. Introduction

Most Web and mobile service providers collect and analyze data generated by users while they use their services, such as users' search queries, visited locations and watched videos within a given service. In this paper, we refer to such data as "activity logs". Activity logs contain data that varies in sensitivity by application and data type. For example, intuitively, activity logs of orders in a food delivery application are unlikely to contain surprising or sensitive information to the user. However, with the rapid advancements in the Internet of Things (IoT), smart home devices, behavioral analytics and personalization, many service

Funding: This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, under grant no. (GPIP: 604-612-2024). The author, therefore, acknowledges with thanks the DSR for financial support.

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2025-0541

providers are now saving unconventional types of activity logs, e.g. saving every search query the user typed in a search engine, or every voice command given to a smart speaker, over a long period of time.

Many service providers offer users privacy controls (also known as privacy settings) that allow them to determine whether, how and for how long their activity logs are saved and used by the service provider. However, these controls are often hidden (Habib *et al.*, 2020; Chen *et al.*, 2019), confusing even for security and privacy experts (Germain, 2022; Green, 2018) and have relatively permissive defaults (Chen *et al.*, 2019; Haselton, 2017). Users who are unaware of default settings and how to adjust them may inadvertently share data (Green, 2018; Liu *et al.*, 2011; Madejski *et al.*, 2012; Shih *et al.*, 2015), leading to consequences such as embarrassment, bullying, stalking, identity theft and fraud (Gross and Acquisti, 2005). Some service providers have been accused of misleading users through privacy setting interfaces. For example, in the USA in 2022, Google agreed to a $392m settlement for misleading users about privacy controls that failed to clearly inform them of the status of the location-tracking setting (Kang, 2022).

Previous work has investigated users' perceptions and behaviors with respect to privacy controls in various contexts, such as social media (Liu *et al.*, 2011; Madejski *et al.*, 2012; Gross and Acquisti, 2005; Ellison *et al.*, 2007; Habib *et al.*, 2022), smart home devices (Malkin *et al.*, 2019; Zheng *et al.*, 2018; Lau *et al.*, 2018), mobile apps (Ramokapane *et al.*, 2019; Felt *et al.*, 2012) and Web service providers such as Google (Alashwali and Cranor, 2024; Farke *et al.*, 2021; Haque *et al.*, 2023). While most prior studies focused on the negative side of activity logs, such as users' lack of awareness about privacy controls and users' privacy concerns about their data, this work aims to provide a broader perspective of users' perceptions regarding activity logs.

Our research aims to answer the following:

Q1. What are the positive and negative aspects and misconceptions about activity logs from the users' perspective?

To answer this question, we conducted a case study on Google's *Activity controls*. We qualitatively analyzed interview data from 30 Google personal account holders in Saudi Arabia regarding their views on Google's *Activity controls*, which provide users with control over the activity logs that Google saves about them while using Google services.

Our work provides a secondary analysis of data obtained from a previous study by Alashwali and Cranor (2024). Nevertheless, the analysis we provide in this work was not covered in Alashwali and Cranor (2024), and is an original contribution for this paper. Namely, in Alashwali and Cranor (2024), the focus of the analysis was on identifying themes related to users' awareness, use, preferences, behaviors and concerns about Google's *Activity controls* and the data it collects about them, as well as the steps they take to control Google's collection or use of this data. This paper complements Alashwali and Cranor's (2024) work by analyzing data from a new perspective, focusing on the positive and negative aspects and misconceptions regarding Google's *Activity controls* as a case study of activity logs, from the users' perspective. See the related work in Section 2.2 for further details about how this work is different from Alashwali and Cranor (2024).

Our results show that participants identified some positive aspects of Google's *Activity controls*, such as saving browsing history and bookmarks, synchronization, security and safety and parental control. On the other hand, they also identified negative aspects, such as a lack of knowledge of Google's data practices and the presence of Google's *Activity controls*, privacy concerns and biased Web content. Some Google activity logs' features, such as tailored ads, were controversial, where some participants appreciated them while others did

not. We also identified misconceptions among participants, such as confusion between local browsing history and cloud-based activity logs and between security and privacy measures. Participants also raised serious concerns about Google's *Activity controls*, which can lead to serious consequences, such as unauthorized logins and data breaches.

The main contribution of this paper is offering a balanced view of users' perceptions of activity logs and providing a better understanding and a useful source for subsequent studies on related topics. We offer a set of practical recommendations for service providers, security and privacy researchers and experts and users alike.

2. Background and related work

In this section, we first describe Google's *Activity controls*. We then summarize related work on privacy perceptions and behaviors associated with privacy controls. Finally, we provide a background on the Saudi society and privacy.

Before we move to the related work, we need to shed light on the difference between two main types of privacy controls that have been described in the literature (Alashwali, 2025): between a user and other users ("user-to-user") and between a user and institution(s) ("user-to-institution"). Our study falls into the second category.

2.1 Google's Activity controls

Google's *Activity controls* [1] (Google, 2021), an area inside Google accounts that spans from the *Data and personalization* [2] *menu, was introduced in 2016 and then called My Activity* (*Farke et al.*, 2021; Olivarez-Giles, 2016). It provides Google account holders with control over multiple activity logs while using Google services, namely, the *Web & App Activity*, *Location History* [3] and *YouTube History*, with the following descriptions provided by Google (retrieved in 2021 (Google, 2021), see Figure 1 for illustration):

- *Web & App Activity*: "Saves your activity on Google sites and apps, including associated info like location […]".
- *Location History*: "Saves where you go with your devices, even when you aren't using a specific Google service […]".
- *YouTube History*: "Saves the YouTube videos you watch and the things you search for on YouTube […]".

As of 2021 (Alashwali and Cranor, 2024; Google, 2021), when a user creates a Google account, the *Web & App Activity* and the *YouTube History* are enabled by default. In contrast, the *Location History* is disabled by default. The default retention periods for the *Web & App Activity*, *Location History* and *YouTube History* are 18 months, 18 months and 36 months, respectively. Users can adjust the retention period by changing the *Auto-delete* setting, which can be set to decrease or increase up to "Don't auto-delete activity". Users can view and manually delete some or all of their activity logs. They can also customize which data to save in the logs. For example, in the *Web & App Activity*, users have two check boxes: "Include Chrome history and activity from sites, apps, and devices that use Google services", which is checked by default and "Include audio recordings", which is unchecked by default. Similarly, in the *YouTube History*, there are two choices: "Include the YouTube videos you watch" and "Include your searches on YouTube", which are both checked by default.

We chose to base our study on interview data from Google's *Activity controls* because Google is one of the largest service providers in the world. In 2024, Google had 1.8 billion active Gmail users (Kiran, 2024; Kumar, 2024).

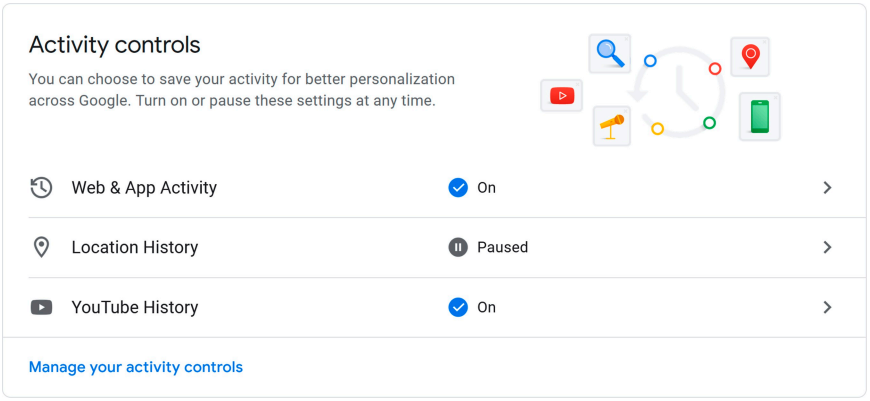

Figure 1. The Google's *Activity controls* lists three types of activity that Google saves: *Web & App Activity* (enabled by default), *Location History* (disabled by default) and *YouTube History* (enabled by default)
Source: (Google, 2021)

2.2 Perceptions and behaviors of privacy controls

Earlier work on the perceptions and behaviors of privacy controls has focused on user-to-user controls, such as profile and post visibility settings on social media platforms. While awareness and use of user-to-user privacy controls on social media platforms were low in the early years of social media use (Gross and Acquisti, 2005), subsequent studies on social media privacy have shown that awareness and use of user-to-user privacy controls have significantly improved over time (Stutzman *et al.*, 2013). However, several researchers have warned that overlooking user-to-institution privacy controls may lead to an illusory sense of control over privacy (Brandimarte *et al.*, 2013; Heyman *et al.*, 2014). That is, when users' perceived control is limited to a specific aspect of their data, ignoring what Stutzman *et al.*, 2013 called "silent listeners", such as service providers and third parties (Haque *et al.*, 2023; Brandimarte *et al.*, 2013; Stutzman *et al.*, 2013). This highlighted the need for further research to understand users' perceptions and behaviors for user-to-institution privacy controls, which our work tries to contribute to.

In recent years, several studies have looked at the user-to-institution privacy controls from the users' perspective, such as Alashwali and Cranor (2024), which we extend and reuse its data for the secondary analysis of this work. While we use the same data, this work differs from Alashwali and Cranor (2024) in the analysis template, and hence in the emerged themes presented in the results and discussion sections. In Alashwali and Cranor (2024), Alashwali and Cranor conducted interviews with 30 Google personal account holders in Saudi Arabia about perceptions and behaviors of Google's *Activity controls*. Their study was exploratory in nature, with an overarching goal to bridge the knowledge gap on privacy perceptions and behaviors in non-Western societies, such as the Saudi society, and to compare patterns with similar studies conducted in the USA. Their analysis was focused on the following main themes: awareness, use, preferences, behaviors and concerns about Google's *Activity controls*, where they reported the identified sub-themes at a fine-grained level. In the awareness theme, the authors reported the awareness level (how many participants reported they were aware of Google's *Activity controls*) and identified sub-themes for how they became aware of them. Similarly, in the use theme, they reported use level (how many participants reported they used Google's *Activity controls*) and identified

sub-themes for the reasons for using or not using them. In the attitudes part, the authors reported participants' feelings when they viewed some of their data in their accounts (e.g. *Web & App Activity*) in an interactive task during the interview, and why they felt that way. The authors also recorded participants' attitudes toward Google's default retention period and their preferences for the ideal retention period and their attitudes and preferences toward the acceptable use of their data by Google. Finally, the authors reported participants' privacy concerns. In addition, they discussed the observed trends on privacy awareness, attitudes, preferences, concerns and behaviors of Saudi participants compared to similar studies on US participants.

Our work extends Alashwali and Cranor's (2024) work by looking at the data from a new lens focused on identifying and reporting: what are the positive (good), negative (bad) and extremely negative (disastrous) aspects, and the misconceptions regarding activity logs from the user's perspective, using data on Google's *Activity controls* as a case study.

Most of the studies in user-to-institution privacy controls showed a lack of, or vague, awareness and use of these types of controls. For example, Farke *et al.*'s study on the then-called Google's *My Activity* found that only 12% of participants said they were "extremely aware" of Google's *My Activity*, while the majority were either "moderately aware" or "somewhat aware" of it (Farke *et al.*, 2021). They also found that only 36% of participants visited Google's *My Activity* page (Farke *et al.*, 2021). Nevertheless, the study showed that when participants were exposed to Google's *My Activity*, they were more likely to report feeling less concerned about data collection and to perceive it as more beneficial (Farke *et al.*, 2021). Malkin *et al.*'s study on Google and Amazon smart speakers found that less than half of smart speaker users knew that their audio recordings were permanently saved in their smart speakers, while 41.4% incorrectly believed that their recordings were saved temporarily (Malkin *et al.*, 2019). In addition, they found that only a minority used the smart speaker's privacy controls (Malkin *et al.*, 2019). For example, of those who knew about the logs' deletion feature, 67.9% never used it (Malkin *et al.*, 2019). Lau *et al.*'s study on smart speaker users found that most users did not use their devices' privacy controls (Lau *et al.*, 2018). In Ul Haque *et al.*'s study, which was based on Google's *Activity controls*, the majority of participants kept the default settings (Haque *et al.*, 2023).

Some of the documented reasons for the lack of awareness and use of user-to-institution privacy controls include: lack of knowledge about the controls, discoverability issues (hidden controls), overtrusting or undertrusting the service provider and resignation (Habib *et al.*, 2020; Chen *et al.*, 2019; Zheng *et al.*, 2018; Lau *et al.*, 2018; Ramokapane *et al.*, 2019).

Research showed that participants were surprised when they viewed their activity logs and saw the data saved about them. Farke *et al.* reported that more than a third of participants were surprised by the amount of data collected about them (Farke *et al.*, 2021). Malkin *et al.* reported that many participants were surprised that their voice interactions with the smart speaker were permanently saved (Malkin *et al.*, 2019). Similarly, multiple studies on mobile apps reported that most participants were surprised by the amount (Jung *et al.*, 2012) and frequency (Balebako *et al.*, 2013) of data collected by their mobile apps, as well as the destinations (Balebako *et al.*, 2013) to which it was sent. While most service providers' default settings are configured to retain activity logs for long periods, research shows that most users prefer shorter retention periods than the defaults (Malkin *et al.*, 2019).

Research showed that privacy concerns are highly contextual. Studies by Lau *et al.* (2018), Zheng *et al.* (2018) and Zeng *et al.* (2017) on smart home devices reported that participants had few privacy concerns. Reasons for low concern include not feeling targeted, trusting the manufacturer, an incomplete understanding of the privacy risks associated with the service and a trade-off between privacy and convenience or functionality (Zheng *et al.*,

2018; Lau *et al.*, 2018; Zeng *et al.*, 2017). Malkin *et al.* reported that only 28.3% of participants had privacy concerns about their smart speakers. Still, they also noted that users raised greater concerns in specific contexts, such as when audio recordings contain children's or guests' voices or if recordings are used for ads (Malkin *et al.*, 2019), offering contextual integrity as an explanation (Malkin *et al.*, 2019; Nissenbaum, 2004).

2.3 Saudi society and privacy

Saudi Arabia is a developing country in southwestern Asia, established in 1932 (Wikipedia, 2025). It has one of the youngest populations in the world. As of 2022, 39% of the population was below 30 years old (General Authority for Statistics GAS, 2022). It has around 17% of the world's proven oil reserves and is the second-largest member of the Organization of the Petroleum Exporting Countries (OPEC, 2025). This situation contributed to rapid development and technology adoption. The Internet penetration rate in Saudi Arabia reached 99% in 2023 (Communication, Space, and Technology Commission, 2023). As of 2022, it is reported that over 80% of the Saudi population are social media users (Kemp, 2022; GMI Blogger, 2022).

As of 2021, when Alashwali and Cranor's (2024) interview study was conducted (we reused its data for this study), internet users in Saudi Arabia have no legal protection for their personal data. However, the Personal Data Protection Law was enforced in Saudi Arabia in September 2024 (Malin, 2024; Yates and Abbas, 2024).

3. Method

In this section, we describe our methods. We first describe the interview data we used in our study. Then, we describe how we analyzed the data. Finally, we list some limitations.

3.1 Interviews

We obtained 30-participant interview data from Alashwali and Cranor's study on privacy perceptions and behaviors of Google personal account holders in Saudi Arabia (Alashwali and Cranor, 2024). Participants were recruited through the first author of Alashwali and Cranor (2024) via her university's mailing list, social and professional WhatsApp groups and social media accounts, including Twitter and LinkedIn. Full details of the recruitment process are provided in Alashwali and Cranor (2024). The interviews were conducted online in August 2021 in Arabic (the native language of the participants and the interviewer) in a semi-structured format. Each interview lasted 33 min on average and included open-ended, multiple-choice and interactive task-based questions. In the latter, the interviewer asked participants to log in to their Google accounts on their computers and to answer questions about their settings, awareness of Google's *Activity controls* and their sentiments after viewing their activity logs. The interview questions are provided in Appendix 2 [4],[5],[6].

3.2 Participants

All participants were living in Saudi Arabia. Participants included 19 (63%) females and 11 (37%) males, with ages ranging from 18 to 54 years. Eight participants (27%) reported having technical backgrounds, i.e. a university degree or work in computer science (CS), information systems (IS), information technology (IT) or computer engineering (CE). None of them reported a degree or work in the cybersecurity field (confirmed via a question at the end of the interview). See Table A1 in Appendix 1 for further demographic details.

3.3 Ethical considerations

The secondary use of Alashwali and Cranor's interview data (Alashwali and Cranor, 2024) was approved by the Institutional Review Board committee of the main author of Alashwali and Cranor (2024), King Abdulaziz University. The data was obtained directly from the authors of Alashwali and Cranor (2024). All participants were adults who aged 18 years or older and provided consent before taking part in the study. Participants were informed about the purpose of collecting the data and that the results will be published in anonymized format.

3.4 Analysis

We qualitatively analyzed the transcribed interview data using template analysis, a style of thematic analysis that combines inductive and deductive approaches, with an emphasis on hierarchical coding but without a specific prescription for the number of levels required or what the levels represent (King, 2025; Brooks and King, 2014). It involves creating a codebook (the template), which defines the themes identified by the researcher in the data set, and can be updated during the analysis where codes can be added, updated and deleted. The researcher normally starts the analysis with a "*a priori* themes", which represent themes anticipated by the researcher.

We started the analysis with the following *a priori* themes: the good, the bad, the misconception and the disastrous aspects of Google's activity logs, which were inspired by previous work (Alashwali and Cranor, 2024). Then, for each interview transcript, the researcher first read the entire transcript and identified the emergent sub-themes of the *a priori* themes and documented the frequency and supporting narrative(s) of each sub-theme. In this paper, we translated the interview questions and participants' direct quotes from Arabic into English, using the Google Translate (Google, 2026) followed by a manual review by the researcher, who is a native Arabic speaker and fluent in English.

While multiple coders can confirm consistent interpretations, analyzing the data by a single experienced researcher is deemed acceptable in both the template analysis method (King, 2025) and Human-Computer Interaction (HCI) research (McDonald *et al.*, 2019).

4. Results

In this section, we first summarize the participants' demographics. We then summarize the four overarching themes and subthemes that categorize users' perceptions of Google's *Activity controls*, including *Web & App Activity*, *YouTube History* and *Location History*. Namely, we summarize the positive (good), negative (bad) and extremely negative (disastrous) aspects, as well as misconceptions, of Google's activity logs. Figure 2 summarized the subthemes we identified under the main themes.

We denote participants as (P_#). Since our study is qualitative in nature and aims to identify themes rather than quantify them, we do not report the number of participants reporting each theme. Instead, we adopt the following terminology from Emami-Naeini *et al.* (2019): (few: 0%–25%; some: 25%–45%; about half: 45%–55%; most: 55%–75%; almost all: 75%–100%).

4.1 Positive aspects of Google's Activity controls (the good)

In this section, we summarize the subthemes we identified as positive aspects of Google's *Activity controls* (the good).

4.1.1 History and bookmark. Some participants found the *Web & App Activity* useful for retrieving previously visited websites or mistakenly closed websites, as described by P_04: "For example, there is something I want to remember, so I can see it again and review it". To some participants, the *YouTube History* was especially useful as P_11 noted: "On YouTube, if it is up to me, I would never turn on the auto-delete". A few participants appreciated the

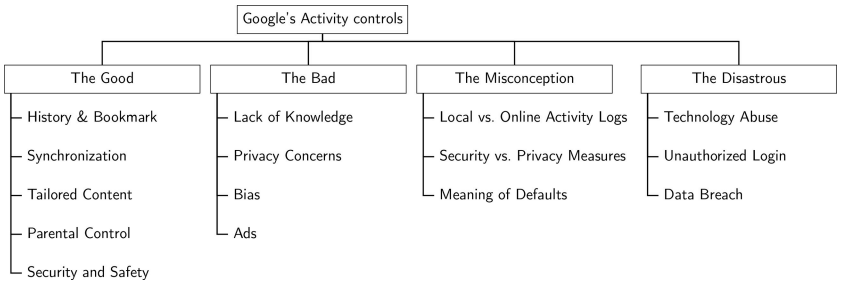

Figure 2. A diagram summarizing our qualitative analysis themes for the positive (good), negative (bad) and extremely negative (disastrous) aspects and misconceptions of Google's *Activity controls* from the users' perspective

Location History feature for saving location maps of infrequently visited locations that they might otherwise forget.

4.1.2 Synchronization. One participant mentioned that she finds the *Web & App Activity* useful to synchronize the Web history between multiple devices: "Because I use them from several devices, for example, sometimes I search on Google Chrome from my mobile phone, sometimes from the desktop computer, sometimes from the laptop, so here it is like a unified place for all activities from all devices" (P_08).

4.1.3 Tailored content. Some participants perceived the tailored content that Google's *Activity controls* may provide positively. This was mentioned in relation to ads, YouTube videos, or Web browsing content. The main perceived benefits were the convenience, relevance to their interests and ease and speed of finding Web and ad content. P_03 can summarize this: "It might make it easier for me and save time for them to find me important things that suit me" and P_11: "they help me by giving me things I've searched for before, things that suit me personally".

Some participants provided more specific examples of how tailored content helps them, such as P_08, a postgraduate student who said: "I am studying for a doctorate […] so I search a lot, so the results come out to me faster and better, and it understands more, so I reach the things I actually want". Similarly, P_19, a university instructor, said: "as a teacher, I prepare [for classes] […] I write the thing, right away it remembers things that I have done before and things come up for me". P_05 mentioned that tailored ads helped her "find the products on a cheaper site". A few participants noted that tailored ads are more convenient, such as P_08: "because if I leave it not personalized for me, it shows me a lot of annoying or inappropriate advertisements". This is especially true for conservative societies, such as Saudi society, which may have reservations about the content they view online.

4.1.4 Parental control. A few participants mentioned the use of Google's *Activity controls* for parental control, as P_09 mentioned using *YouTube History* for this purpose: "I put the tablet on the same account, the mobile phone on the same account, and the laptop on the same account, to see the videos my children watch". P_30 found the *Web & App Activity* useful for a similar purpose: "I can go back to the history so that I can see what, for example, my children watched".

4.1.5 Security and safety. One participant (P_08), with a technical background, mentioned that she reviews logs from time to time for security purposes and described: "to make sure that no one else or another device is open with my account". P_19 found a safety benefit related to the *Location History*, namely, in location tracking: "to the contrary, so that you don't get lost, even let someone know where you are".

4.2 Negative aspects of Google's Activity controls (the bad)

In this section, we summarize the subthemes we identified as negative aspects of Google's *Activity controls* (the bad).

4.2.1 Lack of knowledge. Most participants showed a lack of, or incomplete, knowledge about Google's data practices, including the consent they gave to Google and the existence of Google's *Activity controls* and their features, such as reviewing, deleting and auto-deleting activity logs. This is exemplified in P_06's response when he was asked whether he was aware of Google's *Activity controls*: "I expected something like this to exist, but I don't know it". He was asked about his feelings when he saw his *Web & App Activity* data: "I was surprised that it was stored. I mean, I didn't expect […] that it would record like this". P_09 commented on the consent: "Agree and click click […] but you don't know what the mechanism is, because they give you the terms and conditions on 30 pages".

4.2.2 Privacy concerns. Some participants expressed privacy concerns after they learned about Google's *Activity controls* or after they viewed their activity logs, such as the *Web & App Activity* and the *YouTube History*, mainly because they felt being watched or tracked, as P_03 described: "The feeling of being monitored is honestly unpleasant. That it might record what I do, what I search for, where I am, even YouTube, even if it's not important, I don't like things to be recorded". P_03 also mentioned that she might be self-aware of what she does on the Web: "I feel like I might be more careful about what I search for because it's all recorded, I mean it's all saved and recorded in the history, so it's a bit scary". P_10 explained concerns about personalized Web content in remote work settings: "in our remote work, we share the screen now […] If you are searching for something, it becomes visible, it immediately shows up to the users, meaning that it shows up to the employees with you. Sometimes it is something personal, meaning that it is not something that you share with people".

Regarding retention periods, when asked about Google's defaults, most participants did not prefer Google's default retention periods, which are: 18 months for the *Web & App Activity*, 18 months for the *Location History* and 36 months for the *YouTube History.*

Moreover, a few participants mentioned concerns about data sales and data abuse. When participants were asked about the acceptable use of their *Web & App Activity* data in three scenarios, most found that using their data to display ads, whether by Google or by third parties with Google partnerships, is unacceptable.

4.2.3 Bias. One participant (P_10) mentioned that tailored content provides her with a non-neutral (biased) view of the Web, such as showing her content based on her search interests, as she described: "sometimes there is information hiding. It may not be related to what I searched for, but may be useful to me […] meaning that I did not see the subject in its complete form". Another participant (P_15) explained how repeated tailored ads can drive people into buying something they do not need: "you are curious about a particular product, and you don't need it. Then this [Google] comes and makes you an ad, and you feel like you want to buy it because you see it so much".

4.2.4 Ads. Some participants viewed ads in a generally negative tone, describing them as "annoying". P_14 added: "if I want something, I will go and search for it myself." While tailored ads were perceived as a positive feature by some participants (see Section 4.1.3), others perceived tailored ads negatively, especially when they were repeated as P_10 said: "I searched for a specific topic, everything starts showing up related to [it]" or when ads are from third-party websites as P_14 described: "you [Google] are taking information from me everywhere, you [Google] are not leaving me alone". P_07 criticized the quality of ads and found them useless: "In 10 years, I haven't gotten an ad that really deserves me to go in and see it". P_14 viewed ads as a plan to push users toward premium subscriptions: "flood YouTube with ads and sell a premium subscription. I mean the plan is simple, but effective".

4.3 Misconceptions about Google's Activity controls (the misconception)

In this section, we summarize the subthemes we identified for misconceptions about Google's *Activity controls* (the misconception).

4.3.1 Local versus online activity logs. Multiple participants reported confusion between activity logs saved on a local device (e.g. the local browser's *History*) and those saved in the cloud (e.g. Google's *Web & App Activity*). For example, when asked about the steps they took to protect their privacy on the Internet while using Google services, if any, participants mentioned: deleting the browser's cookies and local history, using private browsing (a feature in most mainstream browsers that deletes local browsing data at the end of the session, e.g. Mozilla's Firefox private browsing (Mozilla, 2025) and Google's Chrome Incognito mode (Google, 2025)) and using a virtual private network (VPN). However, while they partially protect privacy, these techniques cannot protect the user's privacy if the service provider saves and uses the user activity logs on the cloud, such as Google's *Web & App Activity*, *YouTube History* and *Location History*.

4.3.2 Security versus privacy measures. While security and privacy measures are interrelated and often conflated, they are technically distinct (Bambauer, 2013). Generally speaking, privacy concerns the control of who can access and use users' data, whereas security concerns the implementation of technical mechanisms that mediate access or use requests to the data (Bambauer, 2013). That is, "security implements privacy" (Bambauer, 2013). A few participants showed confusion between security and privacy. For example, when asked about the steps they took to protect their privacy on the Internet while using Google services, if any, participants reported security-related measures, such as not using public Wi-Fi (P_08), changing their password (P_17) and using two-factor authentication (P_25).

4.3.3 Meaning of defaults. Most participants in this study did not change default settings, which are often permissive by default. For example, Google's *Web & App Activity* and *YouTube History* were enabled by default. When asked about the reasons for keeping the defaults, some participants indicated misconceptions. For example, not changing defaults unless something went wrong, as P_13 noted "I don't go to the account and its choices except when I face a problem, and I search for the problem I want and that's it". P_06 said he did not change the defaults because "It won't have an impact or make a difference in use", while P_17 indicated fear of messing things up: "I don't want to change anything, leave it as it is as long as the email is working. I don't want to change anything and mess with the email. I'm afraid that [I] do something and then something happens to [my] email". These responses indicate misconceptions about what the default settings are and the effect of changing them.

4.4 Extremely negative aspects of Google's Activity controls (the disastrous)

In this section, we summarize the subthemes we identified for extremely negative aspects of Google's *Activity controls* (the disastrous).

4.4.1 Technology abuse. While none of the participants reported using Google's *Activity controls* for stalking, we inferred potential abuse from two use cases mentioned by the participants. The first was parental control, where two participants found the *Web & App Activity* useful for monitoring what their children viewed online. The second was related to location tracking for security and safety, where one participant found the *Location History* useful if someone knew her location in case she got lost. These sound like good uses of Google's *Activity controls* if they are used by a legitimate party who has been authorized by the account owner or who has the authority to access the account, such as parents of minors. However, these features can be abused if the account falls into the wrong hands, e.g. for stalking a close person. For example, technology abuse by intimate partners has been

documented and studied (Freed *et al.*, 2018). Google's *Activity controls*, which allow the account holder's online and location activity logs to be saved, is a feature that can be abused.

4.4.2 Unauthorized login. Participants recognized that Google's *Activity controls* include highly personal data, including *Web & App Activity*, *YouTube History* and *Location History*. A few participants mentioned that unauthorized access to their Google account (account hijacking) represents a major privacy concern, as P_19 expressed: "I'm afraid that someone might be able to access my account and see what I'm searching for". P_19 added that she is more concerned about "Someone I know more than Google". A hijacked account can endanger not only their privacy, but even their physical security, e.g. through the *Location History* as P_23 expressed concerns "if […] my email was hacked, for example, and the person who accessed my email and activity control would be able to see all the locations that I was there, right?"

4.4.3 Data breach. A data breach is a security incident at the service provider's end that can result in the disclosure of users' credentials and activity data. This was one of the main concerns for several participants, such as P_18: "Because we heard that Google and even Apple were hacked, and thousands, even hundreds of thousands, of millions of personal information of those involved were leaked".

5. Discussion

In this section, we summarize our results and discuss implications and recommendations stemming from our findings, summarized as follows:

5.1 Summary of findings

Our findings reveal themes and use cases in which activity logs were perceived and used positively. Participants perceived some benefits in Google's *Activity controls* such as, history and bookmarking, synchronization, parental control and security and safety. On the other hand, lack of knowledge about Google's *Activity controls*, privacy concerns, biased content and ads were on the negative side of the activity logs. Tailored content was a double-edged sword, with participants perceiving it both positively and negatively. Some of our themes for the positive aspects (history and tailored content such as personalized ads and improved suggestions) and the negative aspect (privacy concerns) align with Farke *et al.*'s findings (Farke *et al.*, 2021). Our analysis also revealed that participants had misconceptions, including confusion between local and online activity logs. At the extreme negative end (the disastrous), unauthorized access to activity data, data breaches at companies and technology abuse were outstanding concerns. Such a balanced view of the activity logs and the themes we uncovered represents a valuable source for subsequent studies in this area. Moreover, our results allowed us to provide practical recommendations for policy makers and technology designers.

In what follows, we present insights and recommendations to mitigate the risks associated with the negative aspects and maximize the benefits of users' activity logs. We close the section with a summary of the study implications and limitations.

5.2 Implement additional layers of security

Our participants expressed significant concerns regarding data breach and unauthorized access to their accounts. This is in line with previous work where participants had similar concerns regarding Google data collection (Farke *et al.*, 2021). We also inferred the potential risk of abusing the *Activity controls* feature, for example, by a violent intimate partner, for stalking or exposing data about their victims. Clearly, accounts that save activity logs, such as Google's *Activity controls*, that contain very personal details, such as *Web & App Activity*, *YouTube History* or *Location History*, pose additional serious concerns.

Thus, we recommend service providers add a mandatory additional layer of security to protect users' activity logs from serious potential risks. This includes requiring an extra verification step to access activity logs in users' accounts. For example, similar to changing a password in most service providers, requiring additional verification for the password or second-factor authentication. Moreover, we recommend service providers use a form of feedback nudges (Acquisti *et al.*, 2017), to keep the user informed about any changes made to their activity logs settings, such as enabling or disabling them, to reduce risks.

As of this writing, Google provides a feature for extra verification to manage (e.g. view and delete) the activity logs (see Figure A1 in Appendix 1). However, it is not enabled by default, buried inside each activity page, meaning that it requires user's prior knowledge about the *Activity controls*, leaving unaware users vulnerable to risks, which may present serious concerns for them. This leads us to discuss privacy by default in the next section.

5.3 Implement privacy by default

Research showed that default settings influence users' choices (Alashwali, 2025; Baek *et al.*, 2014; Bellman *et al.*, 2001). However, service providers often adopt permissive defaults and long retention periods for users' activity logs. This was the case in Google's *Activity controls* at the time of the study, where the *Web & App Activity* and the *YouTube History* were enabled by default. Most of our participants kept the default settings (Alashwali and Cranor, 2024). This is also evident in related work, such as Lau *et al.* (2018), Farke *et al.* (2021) and Haque *et al.* (2023). At the same time, most participants in our data set found that Google's default retention periods for all three types of activity that Google logs are longer than needed and preferred shorter retention periods (Alashwali and Cranor, 2024). This is inline with what is reported in Malkin *et al.* (2019) regarding smart speaker users' preferences toward voice command logs. Moreover, recent work showed that participants who used privacy interfaces with preloaded default settings (presets) had less comprehension of the choices they made (Alashwali *et al.*, 2025). It also showed that participants preferred a privacy interface that requires them to select each setting individually over interfaces with default settings, citing the ability to customize settings as they wish and to make informed decisions about each setting as the main reasons for their preference (Alashwali *et al.*, 2025). Research suggests that an opt-in approach (where users need to approve using their data) is more advantageous to protecting users' information privacy than an opt-out approach (where users need to disapprove using their data) (Baek *et al.*, 2014; Bellman *et al.*, 2001; Alashwali *et al.*, 2025).

Thus, we recommend adopting privacy by default for settings, including shorter retention periods to maintain users' activity logs. Further research is needed to identify what constitutes good defaults, and the role data protection laws and regulations can play in developing guidelines for default settings that prioritize users' privacy, especially when the data is very personal, such as the *Web & App Activity* and *YouTube History*, which are, as of this writing, turned on by default in Google's *Activity controls*.

5.4 Raise awareness about potential technology abuse

Participants viewed some uses of Google's *Activity controls* positively, such as parental control to review the content their children viewed and location tracking by an authorized individual for security and safety. However, it should be noted that such features are prone to abuse, such as, stalking, tracking or unauthorized exposure of log data, had they fallen into the wrong hands, for example, by a violent intimate partner. Slupska and Tanczer stressed the importance of threat modeling technology abuse in intimate partner violence, and the need for a combination of technical and social measures to address it (Slupska and Tanczer, 2021). Our identification of the activity logs abuse theme is a step in this direction.

Identifying the potential abuse of the activity logs supports our aforementioned recommendations regarding the need for a second layer of security for the activity logs feature (Section 5.2) to protect users' privacy by default (Section 5.3), at least for sensitive data such as location and Web activity logs, which have been reported as more sensitive than other types of logs, such as the *YouTube History* (Alashwali and Cranor, 2024). In addition, from an awareness perspective, service providers need to educate users through informational messages about the potential for abuse of these double-edged features, so that users are aware that sharing an account's password entails not only mailbox access but also access to much more personal data. Privacy experts also need to raise awareness about technology abuse, including the abuse of subtle features such as the activity logs.

5.5 Address misconceptions

We identified misconceptions among participants regarding intrinsic issues related to activity logs, including local versus online logs, private browsing and VPNs. Google Chrome added information below the "Delete browsing history data" option, clarifying which data is being deleted. For example, when a Google Chrome user deletes the browsing history data while signed out, the following statement appears: "To delete browsing data from all of your synced devices and your Google Account, sign in". However, Google account users who use browsers other than Google's Chrome, such as Mozilla's Firefox, may not be aware that deleting browsing local history does not delete online activity logs saved in the cloud, such as Google's *Web & App Activity*.

We recommend that service providers, such as browser and VPN vendors, address these misconceptions regarding activity logs and privacy protection, for example, by providing users with more information. In addition, raising public awareness of the nuanced issues surrounding Web privacy can help protect users' privacy by reducing unintentional data sharing.

5.6 Cultural influence

Our participants are from Saudi Arabia, which may be culturally, religiously, politically and economically different than most of the Western, Educated, Industrialized, Rich and Democratic countries (Hasegawa *et al.*, 2024). This may limit the generalizability of our results. One might ask whether and how the themes we identified are linked to the participants' cultural background. While this paper provides an original perspective, when reasoning about the identified themes (summarized in Figure 2), we do not find any that may not be applicable to other cultures. At first glance, we suspected that the reported use cases of using Google's *Web & App Activity* and *YouTube History* for parental control are uniquely related to the collective nature of Saudi society and the controlling parenting style that is arguably prevalent in Saudi Arabia (Dwairy *et al.*, 2006). However, a study in the UK identified technology repurposing (using technology for purposes beyond its original purpose) in IoT device context, e.g. using smart cameras, smart lights and smart speakers for parental control and entertainment (Chalhoub *et al.*, 2021).

Alashwali and Cranor's observation in Alashwali and Cranor (2024), which produced the data we used in our analysis, whose analysis focused on participants' awareness, attitudes, preferences, concerns and behaviors, noted that their identified themes are similar to those found in studies in the USA. In this perspective, we reiterate their observation and note that we do not observe themes unique to the Saudi Arabian culture in our analysis of the positive and negative aspects and misconceptions regarding Google's *Activity controls*. However, both of our studies are qualitative, thus we are limited to reasoning about the emerged themes. Further quantitative studies may reveal cultural differences at other levels, such as prevalence and scale. Moreover, it is important to consider the type of privacy control in our study, which is user-to-institution,

with the institution being a company, where the cultural aspects may have less influence than in user-to-user (between a user and other users) privacy control (Alashwali, 2025).

5.7 Implications

From a theoretical perspective, our results provide a balanced view regarding users' activity logs from users' perspective, represented by the Google *Activity controls* as a case study. Namely, we distilled sub-themes that fall into the following four themes: the good, the bad, the misconception and the disastrous (depicted in Figure 2). Our analysis highlighted overlooked themes, such as the positive perception of Google's *Web & App Activity* for parental control and account security monitoring and the *Location History* for physical safety. In addition, we also inferred the potential abuse of the activity logs, such as in intimate partner violence.

In terms of practical implications, our results provide practical recommendations for service providers, security and privacy researchers and experts and users alike. This includes emphasizing the need for an additional layer of security to activity logs, and for security and privacy by default, especially for data that is often perceived as sensitive, including *Web & App Activity*. We also recommend feedback nudges that notify the account holder of changes to the activity log settings, such as when they are turned on or off. Moreover, we recommend that products, such as Web browsers, include more information by design to address misconceptions about activity logs, including information about where the logs' data will be stored (locally vs in the cloud). Finally, we recommend public awareness programs that educate users about the potential for abuse of technology features, such as activity logs and strategies for protection and support.

5.8 Limitations

Our study has the following limitations. First, a common limitation in secondary analysis is that the data were not collected for the research question we address in this paper (Doolan and Froelicher, 2009). Nevertheless, the data are closely related to our research question and have been carefully assessed for their suitability. Second, the interview data we used were collected in 2021. We balanced the cost of gathering new data versus the benefits of reusing existing data. Accordingly, we decided to reuse existing data as we do not anticipate that users' privacy perceptions change rapidly. Third, the interview data are for 30 participants living in Saudi Arabia, which may affect the generalizability of our results. However, the results of Alashwali and Cranor suggest that, Saudi participants exhibited patterns in perceptions and behaviors similar to those of US participants in similar studies with respect to user-to-institution privacy (Alashwali and Cranor, 2024). Moreover, a sample size of 30 is deemed acceptable for qualitative interview studies that focus on surfacing themes rather than drawing quantitative conclusions (Distler *et al.*, 2021). Fourth, participants' demographics are biased toward those located in the western region of Saudi Arabia (93%) and slightly toward females (63%). However, as noted in Alashwali and Cranor (2024), the western region of Saudi Arabia (a.k.a. the Makkah Region) is very large and diverse, containing several cities and towns with a population of 8,021,463 according to the latest population estimates of the Makkah region as of 2022 (General Authority for Statistics (GAS), 2022) . Fifth, participants' answers are prone to recall bias and social desirability. However, this is a common limitation in interviews and self-reporting studies. Both of these limitations were addressed in Alashwali and Cranor (2024). To address recall bias, the interviews used interactive task-based questions in which participants were instructed to open their Google account's *Activity controls* and answer accordingly. To address social desirability bias, participants were reminded at the beginning and during the interview that there is no right or wrong answer and that the research team has no relationship with Google. Moreover, the interviewer did not use the "security" and "privacy" words until the very last

sections of the interview, to avoid privacy and security priming. Sixth, the direct quotes from participants in this paper are the most accurate translations from Arabic into English. We tried to translate participants' responses as-is, including imperfections, accurately. Nevertheless, "lost in translation" expressions may have occurred. Finally, some of the terms used by Google during the interviews have been updated (some terms were updated during interviews with four participants (Alashwali and Cranor, 2024)). However, as noted in Alashwali and Cranor (2024), interface and terminology changes by service providers during and after field studies are common and reported in privacy studies (Malkin *et al.*, 2019; Wang *et al.*, 2014; Almuhimedi *et al.*, 2015).

6. Conclusion

In this paper, we present a secondary analysis of interview data from 30 participants in Saudi Arabia who hold Google personal accounts regarding their perceptions of Google's *Activity controls*. Using template analysis, we qualitatively analyzed the data from the lens of four main themes: the good, the bad, the misconception and the disastrous aspects of users' activity logs from the users' perspective. Unlike previous work that emphasizes the negative side of activity logs, our work provides a balanced view of users' perceptions regarding activity logs and covers the positive, negative and extremely negative aspects, as well as the misconceptions about users' activity logs, providing a better understanding of users' perceptions of users' activity logs and a useful source for subsequent studies in related topics.

Acknowledgement

The author acknowledges using an AI-assisted tool (Grammarly, 2026) to proofread the paper to improve the English language write-up. The text is entirely generated by the author. The language corrections made by the tool were thoroughly reviewed by the author.

Notes

[1.] Now called Personalisation and activity.

[2.] Now called Data and privacy.

[3.] Now called Timeline.

[4.] A fictitious answer was added as an answer validity check.

[5]. The participant was asked about either the Web & App Activity, YouTube History or Location History, depending on the participants' answer on the basic settings (Q. 1). Full details of the task description can be found in Alashwali and Cranor (2024).

[6.] Asked as three separate questions, one question per data type.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. and Wilson, S. (2017), "Nudges for privacy and security: understanding and assisting users' choices online", *ACM Computing Surveys*, Vol. 50 No. 3, pp. 1-41.

Alashwali, E. and Cranor, L. (2024), "Privacy perceptions and behaviors of google personal account holders in Saudi Arabia", In: Moallem, A. (Ed.), *HCI for Cybersecurity, Privacy and Trust*, Springer, pp. 3-29.

Alashwali, E., Miller, A., Nisenoff, A., Norton, K., Young, E., Bothra, P., Lanyon, M. and Cranor, L.F. (2025), "Interface design to support informed choices when users face numerous privacy decisions", *IEEE Transactions on Privacy*, Vol. 2.

Alashwali, E. (2025), "Two types of data privacy controls", *Communications of the ACM*, Vol. 68 No. 8, pp. 34-35.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L.F. and Agarwal, Y. (2015), "Your location has been shared 5,398 times! A field study on mobile app privacy nudging", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI), ACM*, pp. 787-796.

Baek, Y.M., Bae, Y., Jeong, I., Kim, E. and Rhee, J.W. (2014), "Changing the default setting for information privacy protection: What and whose personal information can be better protected?", *The Social Science Journal*, Vol. 51 No. 4, pp. 523-533.

Balebako, R., Jung, J., Lu, W., Cranor, L.F. and Nguyen, C. (2013), "Little brothers watching you": raising awareness of data leaks on smartphones", In: *Proceedings of Symposium on Usable Privacy and Security (SOUPS)*, ACM, pp. 1-11.

Bambauer, D.E. (2013), "Privacy versus security", *J. Crim. L. and Criminology*, Vol. 103 No. 3, pp. 667-683.

Bellman, S., Johnson, E.J. and Lohse, G.L. (2001), "On site: to Opt-In or Opt-Out? it depends on the question", *Communications of the ACM*, Vol. 44 No. 2, pp. 25-27.

Brandimarte, L., Acquisti, A. and Loewenstein, G. (2013), "Misplaced confidences: privacy and the control paradox", *Social Psychological and Personality Science*, Vol. 4 No. 3, pp. 340-347.

Brooks, J. and King, N. (2014), "Doing template analysis: Evaluating an end of life care service", *Sage Research Methods Cases Part 1*.

Chalhoub, G., Kraemer, M.J., Nthala, N. and Flechais, I. (2021), "It did not give me an option to decline: a longitudinal analysis of the user experience of security and privacy in smart home products", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI), ACM*, pp. 1-16.

Chen, Y., Zha, M., Zhang, N., Xu, D., Zhao, Q., Feng, X., Yuan, K., Suya, F., Tian, Y., Chen, K., Wang, X. and Zou, W. (2019), "Demystifying hidden privacy settings in mobile apps", In: *Proceedings of Symposium on Security and Privacy (SP), IEEE*, pp. 570-586.

Communication, Space and Technology Commission (2023), "Saudi internet 2023", available at: www.cst.gov.sa/en/indicators/saudiinternet/saudi-internt-2023.pdf

Distler, V., Fassl, M., Habib, H., Krombholz, K., Lenzini, G., Lallemand, C., Cranor, L.F. and Koenig, V. (2021), "A systematic literature review of empirical methods and risk representation in usable privacy and security research", *ACM Transactions on Computer-Human Interaction*, Vol. 28 No. 6.

Doolan, D.M. and Froelicher, E.S. (2009), "Using an existing data set to answer new research questions: a methodological review", *Research and Theory for Nursing Practice*, Vol. 23 No. 3, pp. 203-215.

Dwairy, M., Achoui, M., Abouserie, R., Farah, A., Sakhleh, A.A., Fayad, M. and Khan, H.K. (2006), "Parenting styles in Arab societies: a first cross-regional research study", *Journal of Cross-Cultural Psychology*, Vol. 37 No. 3, pp. 230-247.

Ellison, N.B., Steinfield, C. and Lampe, C. (2007), "The benefits of Facebook 'friends': social capital and college students' use of online social network sites", *Journal of Computer-Mediated Communication*, Vol. 12 No. 4, pp. 1143-1168.

Emami-Naeini, P., Dixon, H., Agarwal, Y. and Cranor, L.F. (2019), "Exploring how privacy and security factor into IoT device purchase behavior", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI), ACM*, pp. 1-12.

Farke, F.M., Balash, D.G., Golla, M., Dürmuth, M. and Aviv, A.J. (2021), "Are privacy dashboards good for end users? Evaluating user perceptions and reactions to Google's my activity", In: *Proceedings of USENIX Security Symposium*, USENIX, pp. 483-500.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D. (2012), "Android permissions: User attention, comprehension, and behavior", In: *Proceedings of Symposium on Usable Privacy and Security (SOUPS)*, ACM, pp. 1-14.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. and Dell, N. (2018), "'A stalker's paradise': how intimate partner abusers exploit technology", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, *ACM*, pp. 1-13.

General Authority for Statistics (GAS) (2022), "Population by detailed age", available at: www.stats.gov.sa (accessed 29 April 2025).

Germain, T. (2022), "Google settings still confusing after $85 million lawsuit over how confusing they were", available at: https://gizmodo.com/google-location-history-setting-confusing-settlement-1849619287

GMI Blogger (2022), "Saudi Arabia social media statistics 2022", available at: www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics

Google (2025), "Google: Browse in private", available at: https://support.google.com/chrome/answer/95464?hl=en&co=GENIE.Platform=Android

Google (2021), "Google", available at: https://google.com

Google (2026), "Google translate", available at: https://translate.google.com

Grammarly (2026), "Grammarly", available at: https://app.grammarly.com

Green, M. (2018), "Why I'm done with chrome", available at: https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome

Gross, R. and Acquisti, A. (2005), "Information revelation and privacy in online social networks", In: *Proceedings of Workshop on Privacy in the Electronic Society*, ACM, pp. 71-80.

Habib, H., Pearman, S., Wang, J., Zou, Y., Acquisti, A., Cranor, L.F., Sadeh, N. and Schaub, F. (2020), "It's a scavenger hunt": usability of websites' Opt-Out and data deletion choices", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, ACM, pp. 1-12.

Habib, H., Pearman, S., Young, E., Saxena, I., Zhang, R. and Cranor, L.F. (2022), "Identifying user needs for advertising controls on Facebook", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 No. CSCW1, pp. 1-42.

Haque, E.U., Khan, M.M.H. and Fahim, M.A.A. (2023), "The nuanced nature of trust and privacy control adoption in the context of google", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, ACM.

Hasegawa, A.A., Inoue, D. and Akiyama, M. (2024), "How WEIRD is usable privacy and security research?", In: *Proceedings of USENIX Security Symposium*, *USENIX*, pp. 1-18.

Haselton, T. (2017), "How to find out what google knows about you and limit the data it collects", available at: www.cnbc.com/2017/11/20/what-does-google-know-about-me.html

Heyman, R., De Wolf, R. and Pierson, J. (2014), "Evaluating social media privacy settings for personal and advertising purposes", *info*, Vol. 16 No. 4, pp. 18-32.

Jung, J., Han, S. and Wetherall, D. (2012), "Short paper: enhancing mobile application permissions with runtime feedback and constraints", In: *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ACM, pp. 45-50.

Kang, C. (2022), "Google agrees to $392 million privacy settlement with 40 states", available at: www.nytimes.com/2022/11/14/technology/google-privacy-settlement.html

Kemp, S. (2022), "Digital 2022: Saudi Arabia", available at: https://datareportal.com/reports/digital-2022-saudi-arabia

King, N. (2025), "Template analysis", available at: https://research.hud.ac.uk/research-subjects/human-health/template-analysis

Kiran, H. (2024), "49 Gmail statistics to show how big it is In 2024", available at: https://techjury.net/blog/gmail-statistics

Kumar, N. (2024), "Gmail statistics 2024: number of users and market share", available at: www.demandsage.com/gmail-statistics

Lau, J., Zimmerman, B. and Schaub, F. (2018), "Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2 No. CSCW, pp. 1-31.

Liu, Y., Gummadi, K.P., Krishnamurthy, B. and Mislove, A. (2011), "Analyzing Facebook privacy settings: user expectations vs. Reality", In: *Proceedings of Internet Measurement Conference (IMC)*, ACM, pp. 61-70.

McDonald, N., Schoenebeck, S. and Forte, A. (2019), "Reliability and inter-rater reliability in qualitative research: norms and guidelines for CSCW and HCI practice", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 3 No. CSCW, pp. 1-23.

Madejski, M., Johnson, M. and Bellovin, S.M. (2012), "A study of privacy settings errors in an online social network", In: *Proceedings of Pervasive Computing and Communications Workshops*, IEEE, pp. 340-345.

Malin, C. (2024), "Transition period for Saudi Arabia's data protection law ends", 2026, available at: www.middleeastainews.com/p/saudi-data-protection-law-enforcement

Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Egelman, S. and Wagner, D. (2019), "Privacy attitudes of smart speaker users", *Proceedings on Privacy Enhancing Technologies*, Vol. 2019 No. 4, pp. 250-271.

Mozilla (2025), "Mozilla: Private browsing, use Firefox without saving history", available at: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history

Nissenbaum, H. (2004), "Privacy as contextual integrity", *Wash. L. Rev*, Vol. 79 No. 1, pp. 119-157.

Olivarez-Giles, N. (2016), "How to use Google's new My activity privacy tool", available at: www.wsj.com/articles/how-to-use-googles-new-my-activity-privacy-tool-1467402973

OPEC (2025), "Saudi Arabia facts and figures", available at: www.opec.org/saudi-arabia.html (accessed 29 April 2025).

Ramokapane, K.M., Mazeli, A.C. and Rashid, A. (2019), "Skip, skip, skip, accept!!!: A study on the usability of smartphone manufacturer provided default features and user privacy", *Proceedings on Privacy Enhancing Technologies*, Vol. 2019 No. 2, pp. 209-227.

Shih, F., Liccardi, I. and Weitzner, D. (2015), "Privacy tipping points in smartphones privacy preferences", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, ACM, pp. 807-816.

Slupska, J. and Tanczer, L.M. (2021), "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things", In: Bailey, J., Flynn, A. and Henry, N. (Eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Emerald.

Stutzman, F.D., Gross, R. and Acquisti, A. (2013), "Silent listeners: the evolution of privacy and disclosure on Facebook", *Journal of Privacy and Confidentiality*, Vol. 4 No. 2, pp. 7-41.

Wang, Y., Leon, P.G., Acquist, A., Cranor, L.F., Forget, A. and Sadeh, N. (2014), "A field trial of privacy nudges for Facebook", In: *Proceedings of Conference on Human Factors in Computing Systems (CHI)*, *ACM*, pp. 2367-2376.

Wikipedia (2025), "Saudi Arabia", available at: https://en.wikipedia.org/wiki/Saudi_Arabia

Yates, D. and Abbas, A. (2024), "Saudi PDPL latest updates, new guidelines, rules and regulations", available at: www.tamimi.com/news/saudi-pdpl-latest-updates-ahead-of-14-september-2024-new-guidelines-rules-and-regulations

Zeng, E., Mare, S. and Roesner, F. (2017), "End user security and privacy concerns with smart homes", In: *Proceedings of Symposium on Usable Privacy and Security (SOUPS)*, *USENIX*, pp. 65-80.

Zheng, S., Apthorpe, N., Chetty, M. and Feamster, N. (2018), "User perceptions of smart home IoT privacy", *Proceedings of the ACM on Human-Computer Interaction*, Vol. 2 No. CSCW, pp. 1-20.

Appendix 1. Additional results

A.1 Demographic details

In this section, we list the participants' demographic details obtained from Alashwali and Cranor (2024).

Table A1. Participants' general demographics

Item	$N = 30$ #	%
Nationality		
Saudi	25	(83)
Other	5	(17)
Gender		
Female	19	(63)
Male	11	(37)
Residence region of Saudi Arabia		
Western	28	(93)
Eastern	0	(0)
Central	2	(7)
Northern	0	(0)
Southern	0	(0)
Other (*required: please specify)	0	(0)
Age		
18–24	10	(33)
25–34	10	(33)
35–44	5	(17)
45–54	5	(17)
55–64	0	(0)
65 or above	0	(0)
Highest degree completed		
Doctorate	2	(7)
Master's	9	(30)
Bachelor	11	(37)
High school	8	(27)
Intermediate school	0	(0)
Elementary school	0	(0)
Other (*required: please specify)	0	(0)
Have CS/IS/IT/CE background?		
Yes	8	(27)
No	22	(73)
Employment status		
Student	11	(37)
Full-time employee	11	(37)
Part-time employee	0	(0)
Self-employed or business owner	2	(7)
Full-time house wife/husband	1	(3)

(*continued*)

Table A1. Continued

Item	$N = 30$ #	%
Unemployed and looking for a job	5	(17)
Unemployed and not looking for a job	0	(0)
Unable to work	0	(0)
Retired	0	(0)
Other (*required: please specify)	0	(0)
Google account age		
At least since a month	0	(0)
At least since 3 months	1	(3)
At least since 6 months	2	(7)
At least since a year	2	(7)
At least since 2 years	4	(13)
At least since 3 years	4	(13)
At least since 5 years	4	(13)
At least since more than 5 years	13	(43)
Other (*required: please specify)	0	(0)
Browser type		
Google Chrome	22	(73)
Firefox	2	(7)
Brave	0	(0)
MS Edge	1	(3)
Safari	5	(17)
Opera	0	(0)
Other (*required: please specify)	0	(0)

Source(s): (Alashwali and Cranor, 2024)

A.2. Google's Activity controls extra verification feature

Figure A1 illustrates the extra verification feature to manage the *Web & App Activity*. The same feature is also available on the other logs: the *YouTube History* and *Location History*. Source: (Google, 2021)

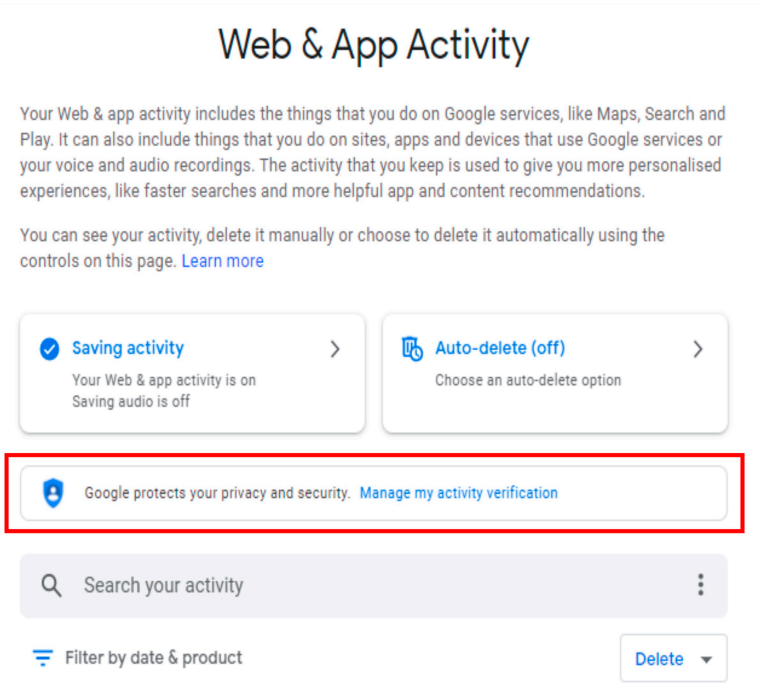

Figure A1. The extra verification feature in the *Web & App Activity* (Google, 2021)

Appendix 2. Interview questions

In this section, we list the interview questions related to this paper, obtained from Alashwali and Cranor (2024). Interviews were conducted in Arabic. The following version is a translated version from Arabic to English. Text between square brackets was not shown to participants (added for clarification). There are more instructions and figures, and demographic, debriefing and other minor questions, which we omit here for brevity (Alashwali and Cranor, 2024).

B.1 Users' experiment

[Questions about awareness of Google's Activity Controls]

- **Q. 1:** Which choice appears to you in the shaded areas numbers: 1, 2, and 3, in front of the following items: Web & App Activity, Location History, and YouTube History?
  Answers: ○ "Stop," [4] ○ "On," ○ "Paused"
  Related figures: Figure A2
- **Q. 2:** Were you aware of Google's Activity Controls that enable you to control the activities that Google saves about you such as the Web & App Activity, YouTube History, and Location History? (yes/no, elaborate if possible)?
  Answers: ○ "Yes," ○ "No," ○ "I heard about such a thing," ○ "I expected there is such a thing"
- **Q. 3: [If Q. 2 answer is "yes," "I heard about such a thing," or "I expected there is such a thing"]** How did you know about, heard of, or expected the existence of Google's Activity Controls?
  Answers: Open

[Questions about usage of Google's Activity Controls]

- **Q. 4:** Have you ever used Google's Activity Controls? (yes/no, elaborate if possible).
  Answers: ○ "Yes," ○ "No," ○ "I do not remember"
- **Q. 5: [If Q. 4 answer is "yes"]** Why did you use Google's Activity Controls?
  Answers: Open
- **Q. 6: [If Q. 4 answer is "yes"]** What changes did you make using Google's Activity Controls?
  Answers: Open
- **Q. 7: [If Q. 4 answer is "no"]** If you have not used the Activity Controls before, it means you are keeping the default settings regarding the activities that Google saves about you, such as the Web & App Activity and the YouTube History. What are your reasons for not using Google's Activity Controls and keeping the default settings?
  Answers: Open

[Questions about preferences and attitudes towards Google's data practices and Activity Controls]

- **Q. 8: [If Q. 1 answer is at least one "on"]** What are the checked choices in your [Web & App Activity | YouTube History | Location History] [5] ?
  Answers:
  [If we proceeded to the Web & App Activity advanced settings, the following answers were shown]

□ “Include Chrome history and activity from sites, apps, and devices that use Google services,” □ “Include audio recordings,” □ “None of the above,” □ “Other (*required: please specify)”

[If we proceeded to the YouTube History advanced settings, the following answers were shown]

□ “Include the YouTube videos you watch,” □ “Include your searches on YouTube,” □ “None of the above,” □ “Other (*required: please specify)”

Related figures: Figure A3 and Figure A4

[If we proceeded to the Location History advanced settings]

[No choices were presented as the Location History has no advanced options]

- **Q. 9: [If Q.1 answer is at least one “on”]** What is the status of the Auto-delete that appears to you [5]?

  Answers: ○ “On,” ○ “Off,” ○ “Not applicable,” ○ “Stop,” [4] ○ “Other (*required: please specify)”

  Related figures: Figure A3 and Figure A4

- **Q. 10: [If Q. 9 answer is “on”]** How long does Google save your data before automatic deletion? [5]?

  Answers: ○ “3 months,” ○ “18 months,” ○ “36 months,” ○ “Other (*required: please specify)”

  Related figures: Figure A3

- **Q. 11: [If Q.1 answer is at least one “on”]** Have you found [previous searches or so | geographic locations] from the [Web & App Activity | YouTube History | Location History] [5]? (yes/no, elaborate if possible).

  Answer: ○ “Yes,” ○ no

  Related Figures: Figure A3 and Figure A4

- **Q. 12: [If Q.11 answer is “yes”]** Describe your feeling after you found [Web & App Activity | YouTube History | Location History] [5] data about you?

  Answers: Open

- **Q. 13: [If Q.11 answer is “yes”]** Were you aware that Google saves the [Web & App Activity | YouTube History | Location History] [5] data about you?

  Answer: ○ “Yes,” ○ “No,” ○ “I expected that, but I am not certain,” ○ “I heard about that, but I am not certain”

- **Q. 14: [If Q. 13 answer is “no”]** Do you have a suggestion if Google implemented, it would have informed you about the saving of your data?

  Answers: Open

- **Q. 15: [If Q. 13 answer is “yes”]** Did you know that you can review the [Web & App Activity | YouTube History | Location History] [5] data that Google saves about you?

  Answers: ○ “Yes,” ○ “No”

- **Q. 16: [If Q.15 answer is “yes”]** Approximately, how often do you review these data?

  Answers: ○ “At least once a day,” ○ “At least once a week,” ○ “At least once a month,” ○ “At least once every 3 months,” ○ “At least once every 6 months,” ○ “At least once a year,” ○ “Less than once a year,” ○ “I never reviewed them,” ○ “I do not remember”

- **Q. 17: [If Q.13 answer is "yes"]** Did you know that you can manually delete some or all of the [Web & App Activity | YouTube History | Location History] [5] data that Google saves about you?
- **Q. 18: [If Q.17 answer is "yes"]** Approximately, how often do you manually delete these data?

  Answers: ○ "At least one a day," ○ "At least once a week," ○ "At least once a month," ○ "At least once every 3 months," ○ "At least once every 6 months," ○ "At least once a year," ○ "Less than once a year," ○ "I never deleted them," "I do not remember"
- **Q. 19: [If Q.13 answer is "yes"]** Did you know about the Auto-delete feature which allows you to specify how long Google saves the [Web & App Activity | YouTube History | Location History][5] note1 data before they are automatically deleted? (yes/no, elaborate if possible)

  Answers: ○ "Yes," ○ "No"

A.2 Auto-delete

- **Q. 20:** Do you think that the default retention period specified by Google (18 months, i.e. 1.5 years) to save the Web & App Activity data at Google before auto-deletion is suitable? (yes/no, elaborate if possible)

  Answers: ○ "Yes," ○ "No"
- **Q. 21 [If Q. 20 answer is "no"]** What period do you suggest for saving the Web & App Activity data before Google automatically deletes them?

  Answers: Open
- **Q. 22:** Do you think that the default retention period specified by Google (36 months, i.e. 3 years) to save the YouTube History data is suitable? (yes/no, elaborate if possible)

  Answers: ○ "Yes," ○ "No"
- **Q. 23 [If Q. 22 answer is "no"]** What period do you suggest for saving the YouTube History data at Google before Google automatically deletes them?

  Answers: Open
- **Q. 24:** Do you think that the default retention period specified by Google (18 months, i.e. 1.5 years) to save the Location History data is suitable? (yes/no, elaborate if possible)

  Answers: ○ "Yes," ○ "No"
- **Q. 25 [If Q. 24 answer is "no"]** What period do you suggest for saving the Location History data at Google before Google automatically deletes them?

  Answers: Open

A.3 Your data privacy and sensitivity

- **Q. 26:** If Google saves the following data: Web & App activity, Location History, and YouTube History. Rank them according to the degree of privacy (no. 1 High Privacy, 2 Medium, 3 Low). Note: you can choose more than one item with an equal degree of privacy.

  Answers: ○ "1 (High)," ○ "2 (Medium)," ○ "3 (Low)"
- **Q. 27:** To what extent do you consider your [Web & App Activity, YouTube History, Location History] [6] data at Google services sensitive?

Answers: ○ "They are all sensitive," ○ "Some are sensitive," ○ "All are insensitive," ○ "Other (*required: please specify)"

A.4 Acceptability for saving your Web and App Activity

- **Q. 28:** To what extent would you accept if Google saves, processes, and analyzes your Web & App activity data, for the purpose of improving the services provided to you, such as speeding up your searches, providing you with better recommendations, and more personalized experiences at Google services?

  Answers: ○ "Very acceptable," ○ "Somewhat acceptable," ○ "Neutral," ○ "Somewhat unacceptable," ○ "Completely unacceptable"

- **Q. 29:** to what extent would you accept if Google saves, processes, and analyzes your Web & App activity data, for the purpose of displaying ads to you on Google services such as Google search engine or YouTube?

  Answers: ○ "Very acceptable," ○ "Somewhat acceptable," ○ "Neutral," "Somewhat unacceptable," ○ "Completely unacceptable"

- **Q. 30:** To what extent would you accept if Google saves, processes, and analyzes your Web & App activity data, for the purpose of displaying ads to you on non-Google websites and apps that have a partnership with Google (such as newspaper websites and gaming apps)?

  Answers: ○ "Very acceptable," ○ "Somewhat acceptable," ○ "Neutral," ○ "Somewhat unacceptable," ○ "Completely unacceptable"

A.5 Privacy concerns

- **Q. 31:** Previously, did you have any concerns regarding your privacy while using Google services, such as the Google search engine, Google Maps, or YouTube?

  Answers: ○ "Yes," ○ "No," ○ "Neutral"

- **Q. 32: [If Q. 31 answer is "yes"]** If your answer is yes, what are these concerns?

  Answers: Open

- **Q. 33:** Have you ever taken any steps to protect your privacy online while using Google services, such as the Google search engine, Google Maps, or YouTube?

  Answers: Open with ○ "Yes," ○ "No"

- **Q. 34:** [If Q. 33 answer is "yes"] If your answer is yes, what are these steps?

  Answers: Open

- **Q. 35:** Do you plan to take any additional steps to protect your privacy online while using Google services, such as the Google search engine, Google Maps, or YouTube?

  Answers: Open with ○ "Yes," ○ "No"

- **Q. 36:** [If Q. 35 answer is "yes"] If your answer is yes, what are these steps?

  Answers: Open

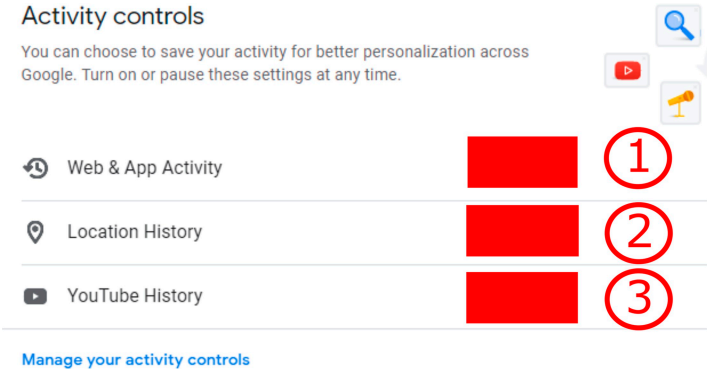

Figure A2. The Activity Controls basic settings (Google, 2021). Participants were asked to report their accounts' current settings (either "on" or "paused"). We covered our settings in the figure to avoid bias or confusion

Source: Alashwali and Cranor (2024)

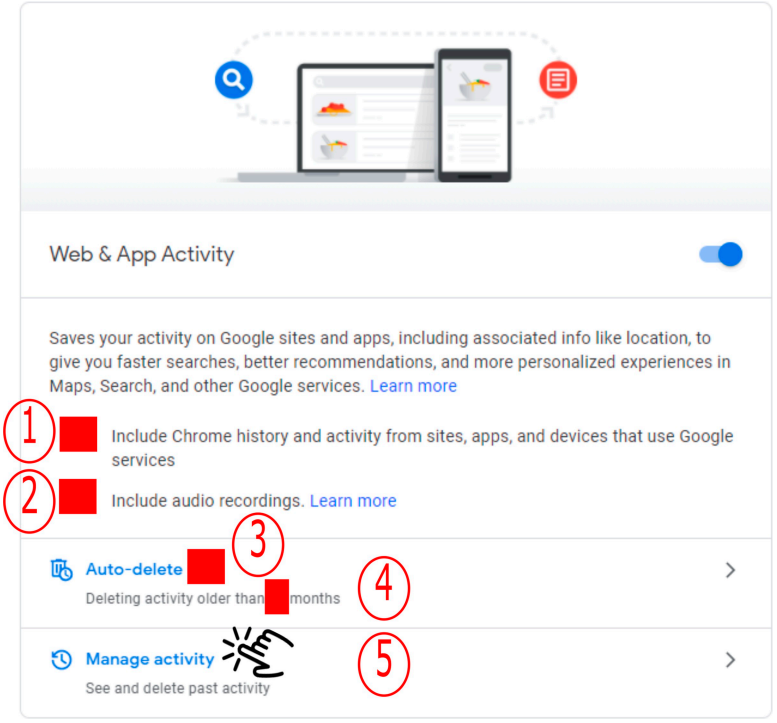

Figure A3. The advanced options of the Web & App Activity (Google, 2021). Participants were asked to report their settings (either checked "✓" or unchecked). We covered our settings in the figure to avoid bias or confusion

Source: Alashwali and Cranor (2024)

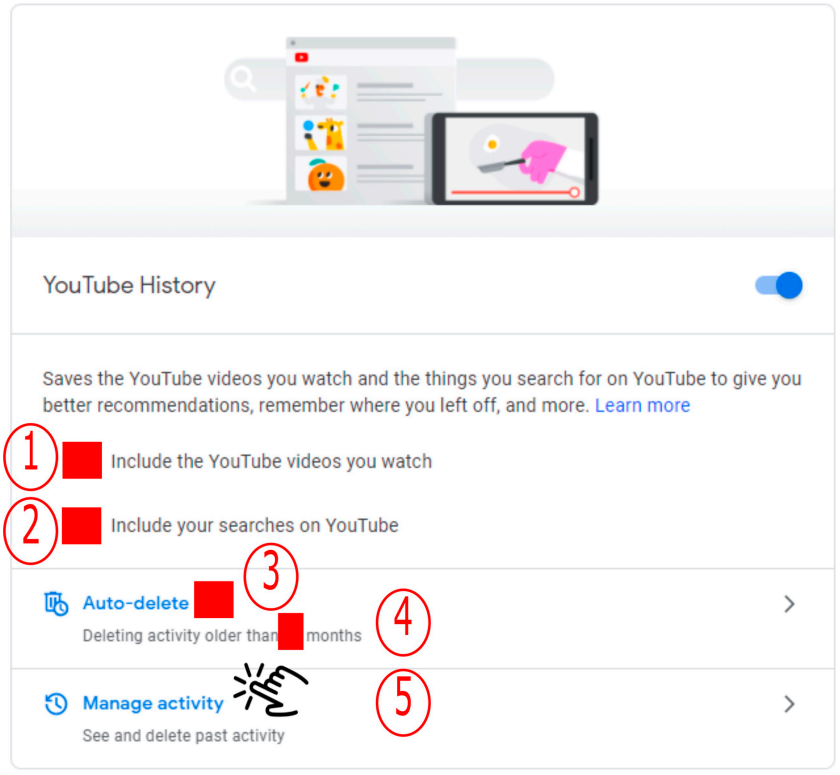

Figure A4. The advanced options of the YouTube History (Google, 2021). Participants were asked to report their settings (either checked "✓" or unchecked). We covered our settings in the figure to avoid bias or confusion

Source: Alashwali and Cranor (2024)

Corresponding author
Eman Alashwali can be contacted at: ealashwali@kau.edu.sa