Bourdoucen, Amel; Lindqvist, Janne

Privacy of Default Apps in Apple's Mobile Ecosystem

Published in:
CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems

Accepted/In press: 01/01/2024

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

The official version of the paper is available as “Amel Bourdoucen and Janne Lindqvist. 2024. Privacy of Default Apps in Apple’s Mobile Ecosystem. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI ’24), May 11–16, 2024, Honolulu, HI, USA. ACM, New York, NY, USA, 32 pages. https://doi.org/10.1145/3613904.3642831”

Please cite this work as above.

Privacy of Default Apps in Apple's Mobile Ecosystem

Amel Bourdoucen
Aalto University
Finland

Janne Lindqvist
Aalto University
Finland

ABSTRACT

Users need to configure default apps when they first start using their devices. The privacy configurations of these apps do not always match what users think they have initially enabled. We first explored the privacy configurations of eight default apps Safari, Siri, Family Sharing, iMessage, FaceTime, Location Services, Find My, and Touch ID. We discovered serious issues with the documentation of these apps. Based on this, we studied users' experiences with an interview study (N=15). We show that: the instructions for setting privacy configurations of default apps are vague and lack required steps; users were unable to disable default apps from accessing their personal information; users assumed they were being tracked by some default apps; default apps may cause tensions in family relationships because of information sharing. Our results illuminate on the privacy and security implications of configuring the privacy of default apps and how users understand the mobile ecosystem.

CCS CONCEPTS

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

KEYWORDS

Privacy, Mobile Devices, Apps, Ecosystems.

ACM Reference Format:
Amel Bourdoucen and Janne Lindqvist. 2024. Privacy of Default Apps in Apple's Mobile Ecosystem. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 32 pages. https://doi.org/10.1145/3613904.3642831

1 INTRODUCTION

Users are not in full control of their privacy preferences in complex mobile devices and cloud ecosystems. The complexity of these systems enables helpful features but at the cost of privacy. Often, many of these features are enabled by default when a user first starts using their device(s). When users purchase new devices, they are often presented with many features to enable or disable. However, our work shows that the privacy implications of these features are not understood, and the settings are not easy to configure.

Studies have discovered several challenges that users face in understanding how their data is handled when using mobile apps, with an emphasis on Android apps [36, 37, 42, 52, 54]. Users are often presented with many permissions requesting approval of access to their personal data. Moreover, prior work suggests that users do not always fully understand the implications of enabling privacy configurations [9, 22]. This confusion is often caused by the architecture of privacy configurations [17]. As a result, users may feel confused [50], surprised [7, 48], anxious [16] and sometimes frustrated [48] when learning what actually happens to their data.

In this paper, we study default apps in Apple's iOS and macOS operating systems. Although past work has investigated the security and privacy of third-party apps, default apps have unique characteristics that are not necessarily applicable to third-party apps. Default apps are i) *sticky*, meaning that many of the default apps cannot be uninstalled without compromising the device's security by either jailbreaking [32] (Apple devices) or rooting (Android devices); ii) the privacy configurations for most of these default apps are prompted to users only once – during initial setup. Therefore, users may later need to navigate settings to view privacy configurations hidden during initial setup; and iii) during setup of the devices, users are prompted by only certain default apps. For example, *Siri* and *Location Services* are prompted to users while other default apps are not.

It is critical to investigate users' perceptions of default apps because these apps are pre-installed and remain on the user's device and cannot be deleted. The privacy settings of default apps may only be viewed once, during initial installation, which means that the user must figure out afterward where the settings can be found to make any changes. Additionally, it is also unclear why some default apps are prompted during the installation stage, while others are not. Some default apps, such as *Siri*, use information retrieved from other apps and services to function; this is problematic because the user may not be aware of what information is being retrieved. Finally, the publicly available documentation for configuring the default apps is ineffective and does not cover all privacy configurations.

User perceptions of default apps, which belong to Apple's mobile ecosystem, remain a mystery. For the following reasons, understanding Apple's mobile ecosystem is essential: i) Apple heavily promotes its platform as privacy-oriented using phrases such as "Privacy. That's Apple" [5]. As a result, iOS users may be less concerned about the privacy implications of default apps than Android users [43]. ii) Due to the closed nature of the ecosystem, verifying data handling practices can be challenging. Finally, iii) in general, Apple's ecosystem is severely understudied in relevant literature. Yet, Apple's mobile ecosystem is very popular.

To illustrate an example of a setup process in the mobile ecosystem, macOS and iOS include setup wizards that guide users in selecting preferences for these default apps when a new device is started. As a concrete example, in the Setup Wizard, one of the features that users can set up is *Siri*. Users are offered the choice to either *Continue* (to set up Siri) or *Set Up Later in Settings*. The phrase *Set Up Later in Settings* may imply that *Siri* is disabled until users set it up later.

CHI '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0330-0/24/05
https://doi.org/10.1145/3613904.3642831

To systematically study these issues, we focused on the following research questions:

RQ1: What privacy configurations are available to control default apps?
RQ2: How can users control the privacy configurations of default apps?
RQ3: How do users understand privacy configurations and their privacy and security implications?
RQ4: How does setting up default features impact the privacy of users?

To answer these research questions, we conducted two studies. In Study 1, we selected eight default apps and features on iOS and macOS: Safari (Web browsing), Family Sharing (Shared Access), Siri (Virtual Assistant), iMessage (Messaging), FaceTime (Video Calls), Location Services, Find My and Touch ID (Fingerprint). We note that apps vary in the complexity of features they provide and how they work. As they are all produced by Apple and pre-installed on users' device(s), this work groups them under the umbrella term of *default apps*. We analyzed Apple's public official documentation and found them seriously lacking in the required details for configuring privacy. Due to this, we conducted a comprehensive system evaluation to understand the privacy configurations for these default apps. We mapped the routes to disable the features of these apps. Building on the results of Study 1, a follow-up interview with Study 2 was conducted to investigate users' understanding of privacy configurations, and the users' answers were compared with Study 1.

We present the following three major contributions:

(1) First, in Study 1, we collected and investigated the privacy configurations of eight default apps of the Apple mobile ecosystem (Section 3). It was essential to complete Study 1 first to allow us to thoroughly assess what user instructions are provided and what is lacking. Because Apple's devices have received little attention in the HCI and usable security literature, this study provides a robust evaluation of the current status of Apple's mobile ecosystem in a single work. The insights from this work serve as a framework for further investigations of other popular mobile ecosystems.
(2) In Study 2, we conducted an interview study to explore users' perceptions of using default apps and configuring their privacy and security settings (Section 4). As part of Study 2, we also asked users to complete real tasks on their devices. We carefully documented the actions they took to complete the work, and we subsequently contrasted those actions with the findings of Study 1 to see if users turned to outside resources (for example, Apple's documentation) for help completing the tasks.
(3) We identity, thereby contribute with a detailed understanding of specific issues users faced with controlling their privacy when using default apps. Based on the findings of both studies, we provide meaningful and informed recommendations for improving user's privacy when using these apps that are better fitted with users' privacy expectations.

2 RELATED WORK

This section first discusses related prior work and reviews studies that explored users' general understanding of privacy in apps. We then describe the challenges faced by users when setting privacy configurations to gain control over their data.

Previous research has addressed problems users encounter on iOS and Android platforms when using default apps. Studies found that users' privacy preferences for default apps are influenced by their lack of understanding of how systems operate.

Our work goes beyond this prior work in several ways:

(1) No prior research has comprehensively analyzed the vendor's instructions for configuring privacy settings. A thorough assessment of the many, ecosystem-specific, privacy-setup options for the default apps is required to provide meaningful recommendations to designers and researchers. Our work covers every default app's privacy setting in Apple's mobile ecosystem. In the future, this work can serve as a foundation for investigating details of other widely used ecosystems.
(2) This research is the first to track and document the steps users take to set up the default applications. We use this evidence to understand, in detail, how users encounter the relevant information to support configuration, in ecological circumstances. By identifying precise issues in this way, our work can support future HCI research in addressing barriers preventing users from customizing the privacy options.

To illuminate our contributions in detail, we have reviewed three studies that are most closely related to our current work. We highlighted research findings and how the methodology and outcomes of our work differentiate it from other studies.

First, Frik et al. [22] explored the relationship between socio-economic factors and users' choices of security and privacy settings. By examining the use of default features on Android and iOS devices, such as passcode, face lock, automatic updates, and password reuse. They found that insufficient awareness about how to configure settings did not protect users against possible harm. Users were found to be concerned about online risk but expected that the default settings of pre-installed apps would take care of this.

According to Frik et al. [22], people may consent to data handling practices they do not comprehend. The study proceeds to recommend user-friendly documentation that is accessible. However, we observed that their study did not assess the usefulness of current material available to users. It is necessary to assess the current instructions and information offered to users to make meaningful recommendations based on what is currently available to users.

To address this gap, we examined and evaluated the documentation provided to users about configuring the settings of default apps. We mapped the privacy configuration paths suggested by the vendor and highlighted what privacy paths were not covered in the documentation. We then talked with users about their understanding of how to configure these settings to their preferred privacy settings and what they think is missing.

Second, Gamba et al. [23] explored pre-installed apps on the Android platform for their app packages, certificates, and third-party libraries. The study by Gamba et al. [23] revealed vulnerabilities that can be found on Android apps. Pre-installed Android apps have

access to personal data and appear to share it with third parties. Pre-installed apps also appeared to contain vulnerabilities that can be potentially used to harm the device while users remain unaware of such vulnerabilities. The study, however, does not investigate what materials users already have, the depth of their understanding, and how to go beyond this.

To go beyond Gamba et al. [23]'s work, research is required to determine whether instructions to configure apps are effectively conveyed to users by the service provider. Additionally, if users currently take any measures to protect their privacy based on their understanding of how the apps work.

To address the points above, our work focuses on the issue of user understanding. We analyzed documents available to users and collected information about what personal data is collected from users. We then conducted a user study to understand users' perceptions about what they think happens to their data once they share it with the ecosystem.

Third, Ramokapane et al. [43] explored users' awareness of some features on both Android and iOS, such as location, ads tracking, usage and diagnostics on Android, and Analytics Data Sharing on iOS. Ramokapane et al. [43] discovered that it was difficult for users to find and modify the settings of default apps or features. The users reported that the settings, when encountered for the first time, are skipped. The study's findings form a starting point for identifying a problem with the existing state of default app settings. However, Ramokapane et al. [43] did not identify the specific failure areas in the process of showing the settings for the first time and then altering them subsequently.

To learn more about what contributes to users' uncertainty about the settings beyond the work by Ramokapane et al. [43], it is necessary to investigate the precise pathways users opted to disable or enable these settings. Understanding the choices of users to achieve their privacy goals is the primary step toward precisely improving approaches for presenting privacy configurations to users.

Our work investigated how users understand data sharing in the mobile ecosystem and examined the paths to adjust every setting. We then talked with users about their perception of altering settings. After this, we assessed the users' ability to find various privacy settings via a series of tasks on their own devices. Finally, we invited them to reflect on the process and analyzed these reflections. This allowed us to clarify the kinds of difficulties users encounter when adjusting privacy configurations to suit their privacy needs.

The uniqueness of Apple's mobile ecosystem. To summarize, previous research recommends that users be informed of the security of default apps with greater transparency. Nevertheless, earlier research has not critically assessed the information users already can access, how this is accessed in practice, and what information is lacking and what is lacking from public documentation of configuring settings. We addressed this via a thorough evaluation of the vendor's official documentation and the information that users can access by installing and subsequently modifying the default apps. Prior research has not examined the privacy settings of apps within a particular ecosystem, and the Apple ecosystem, in particular, has been understudied.

Previous research has indicated that users may have difficulties in locating privacy configurations of default apps. However, prior work has not evaluated the steps that users take to control the privacy configurations of these apps, how they are instructed to do so by the vendor, nor the paths they take in practice when performing these tasks.

Furthermore, previous research has shown that users are unaware of what happens to their data when it is shared with apps. These past studies recruited users who owned one smartphone, either an iOS or Android model. However, these results do not inform us about those many users who own multiple devices within one ecosystem. This common situation is important because it poses particular issues around how users understand the sharing and accessibility of data across devices.

These factors make it imperative to investigate multi-device behavior in a single ecosystem thoroughly, and in particular to focus on Apple's device. This will allow future work to help users better manage their privacy.

Next, we discuss a body of research that has explored the privacy of users when using mobile apps and configuring privacy settings.

User Privacy in Mobile Apps. Prior research has largely explored app permissions in mobile devices. The studies have been motivated by the need to explore users configuring permissions due to the reported difficulties. For several years, researchers have focused on the permissions of apps to explore approaches to improve users' understanding and expectations when setting up privacy configurations of apps. The focus on app permissions was motivated by many studies that demonstrated users' difficulties in understanding privacy configurations of mobile apps [7, 31, 36, 43, 50].

A study on 308 Android users revealed that only 17% of users were attentive to the permissions that were prompted during app installations, thus indicating that permission warnings were not sufficient to ensure informed security decisions [18]. A recent study in 2021 on 4,636 Android users also confirmed that information provided by the system was insufficient for users to make informed decisions on their privacy [47]. Other studies have also shown that users often either ignored or accepted permissions without properly reading the details [19, 20, 43].

Researchers have highlighted factors that influence users' misunderstandings of privacy configurations. Several factors make it difficult for users to know what happens to their personal information when agreeing to permissions or configurations, such as unclear privacy policies [2] and lack of transparency about data collection practices [35]. Earlier studies have investigated approaches to improve privacy policies for better delivery for users [33]. However, recent studies have reported that the unclear nature of privacy policies of apps still contributes to the difficulty users have in grasping what happens to their data [2, 12, 34]. As a result of the unclear nature of privacy policies, users rarely follow privacy policy links to read what part of their information is disclosed [12].

To help users better understand how their data is handled, recent work has explored several solutions to help users in making informed decisions [36, 37, 42, 52, 54]. For instance, Smullen et al. [49] deployed machine learning to offer a prospect of mitigating the burden of increased privacy decisions. Lutaaya [38] proposed a prototype that adjusted privileges given to apps on iOS, including the ability to replace real data with mock data. Liu et al. [37]

analyzed the settings of 4.8 million smartphone users and demonstrated several profiles that aim to simplify the decisions mobile users have to make about their privacy.

Impacts of setting privacy configurations. Another line of research has focused on understanding user's concerns when setting privacy preferences [7, 43, 47, 55]. For instance, research has found that users often have misconceptions about the data sharing occurring in smartphone apps [7, 22, 43, 50]. Misconceptions about the handling of personal data can create challenges for users. Tan et al. [50] suggested that users may feel uncomfortable or confused when learning about what occurs to their data. Other studies have suggested that users are often surprised when asked to share their data collected by apps [7, 48].

Users can also experience other emotions, such as confusion about certain personal data that is requested, and sometimes dismay or even outrage [48]. Studies that focused on tracking users by apps [16, 39, 53] have suggested that users can have negative feelings under the perception of being tracked. These feelings can include anger, distrust, and anxiety. Often users would feel acceptance of the fact that they are being tracked under certain conditions [16]. The reactions users had upon learning about how their data is handled can be linked with the insufficient information on mobile apps to help users make informed decisions [43]. Insufficient information provided about data handling may also lead users to assume that these permissions are required for apps to run [49], which influences users' decision to accept them.

Summary. There is extensive prior research on the privacy settings in mobile devices. Examples of these include users' attitudes towards permissions of different apps on mobile devices [19, 20, 43], tracking of apps [16, 39, 53] and privacy configurations of apps [7, 22, 36, 43, 50]. Prior research has concentrated on third-party apps, which are not by default installed. In summary, there is currently no research that focuses on users' concerns with default apps in Apple's mobile ecosystem and the particular challenges that result from configuring their privacy settings.

3 STUDY I: MOBILE ECOSYSTEM EVALUATION

Study 1 analyzes eight main default apps of the Apple iCloud mobile ecosystem. The eight default apps are an integral part of Apple's iOS and MacOS. Importantly, these apps exchange data with each other, and with other apps, across Apple's ecosystem as a basic part of their functionality. As such, they mark a central aspect of security-relevant behavior for most users. The default apps and their configuration are presented to iOS and MacOS users at installation time. The use of simplified user interfaces at this stage of device adoption, which is designed to speed up installation, may have ongoing ramifications for user privacy during the entire remaining life-cycle of the device. As such, it is important to understand (1) whether and how users understand installation-time settings and their privacy implications, (2) whether users understand how to change the settings later, and (3) details of potential barriers to understanding that may impact points 1 and 2.

Currently, there are few popular mobile ecosystems available on the market, such as those by Apple [4], Google [24] and Huawei [28]. As the target of this study, we chose Apple's ecosystem for the following reasons. (1) Apple's devices are popular and purchased worldwide. In 2021, Apple reported a 65.6 billion USD revenue in iPhones only in the first quarter of the same year [27]. (2) Apple's mobile ecosystem is uniquely cohesive, and its integrated model provides a quality experience for users, alongside a stated emphasis on privacy and security [13].

Mobile Ecosystem Structure A mobile ecosystem consists of a set of units (devices) interacting with each other through an exchange of information, resources, and artifacts [10]. For instance, Apple's mobile ecosystem includes iCloud (Apple's Cloud system), which integrates devices such as iPad, iMac, MacBook and iPhone. Default apps are central to users' participation in the ecosystem. In this paper, the apps manufactured by Apple are referred to as *Default apps*. For instance, the popular app *Safari* is used as a browser for Apple devices. Information stored in Safari, such as Bookmarks, are exchanged between devices that are connected to the same iCloud account. Other default apps include *Siri*, Apple's virtual assistant accepts various commands as voice queries. *iMessage* and *Facetime* for messaging and video calls respectively. *Family Sharing*, a shared access family app that allows for sharing media and app store purchases. *Location Services*, allows apps to access user's locations and *Find My*, allows users to track missing devices.

3.1 Method for Study 1

We evaluated the system for the following parameters: defining the mobile ecosystems' structure, privacy configurations of default apps, the number of privacy configurations to disable within an app and types of personal data collected by these default apps, and whether the personal data is transferred outside the device. We then analyzed in depth Apple's eight default apps: Safari, Family Sharing, Find My, iMessage, Facetime, Siri, Location Services, and TouchID. These apps are linked to simple configuration options presented to the user when the user starts using a macOS or an iOS device for the first time.

The following three major tasks were covered in the analysis.

(1) *Analysis of Official Sources.* We first read the official sources provided by Apple [3]. There were several challenges in conducting this analysis. **a.** *Closed Ecosystem.* Apple's ecosystem is *closed*, meaning that some of the specifications are not disclosed concerning the processing of personal data by default apps. Examples of non-disclosure include ambiguous phrases such as "subsets of data stored" [3] without indicating what is included in the subset of data, how is it processed, and for how long the data is retained. **b.** *Scattered information.* When reading Apple's Privacy Policy for the steps to disable a feature, we discovered that the controls of some apps were described within other apps. For example, *Siri* has a specific section that describes its controls. However, *Siri* can also be found under *Safari Search*'s section as well as in *Dictation*. In summary, the public privacy policies are long and do not contain easily accessible information on how to control privacy configurations precisely.
(2) *System Navigation.* To be able to present the steps required to setup a device, we captured the setup and usage processes on sample iOS and macOS devices. We first did factory resets to our test devices before following the steps of the setup wizard

Table 1: Privacy configurations of default apps. N steps for the number of features available for a privacy configuration for a single default app (both documented and not documented by Apple and evaluated by this work). These privacy configurations may lead to personal data of users being transferred outside the device, as shown in the last column. For the full table, refer to Appendix A.3

Default App	N Steps	Privacy Configurations	May transfer to Cloud or Vendor's Servers
Safari	N>12	IP Address	Yes
		Private Browsing	No
		Web Page Translation	Translation locally, other data may leave device
		iCloud Syncing	Yes
		Preload Top Hit in Safari	Information not provided by vendor
		Sending Information to Apple	Yes
		History and Website Data	Yes
Siri	N>9	Ask Siri	Yes
		Integrated apps	Yes
		Siri and Dictation	Yes
		Siri Personalisation	Yes
		iCloud Syncing	Yes
		Location Services	Yes
		Request History	Yes
Facetime	N>7	Enable Facetime	Calls do not leave device, other data may leave device
		Caller ID	Yes
		SharePlay	Information not provided by vendor
		Speaking	Information not provided by vendor
		FaceTime Live Photos	Information not provided by vendor
		Blocked Contacts	Information not provided by vendor

in all possible combinations of scenarios and sequences of steps. The latter process was repeated every time we followed a different sequence of steps to start fresh.

(3) *Mapping of Privacy Configurations.* To obtain information on how many steps are required to disable each app, we mapped the privacy configurations responsible for handling personal data for each app and noted the pathways to each privacy control. We emphasized what privacy control was included and what was not in Apple's sources. We also present the personal data collected from users for each app.

3.2 Results of Study 1

This section presents a summary of the results of Study 1. Further details are given in the appendices.

In early 2020, we analyzed Apple's official documents regarding user privacy and the data collected in the cloud. We also explored settings on both iPhone (iOS) *version 14.0+* and MacBook (macOS) *version 10.15+*. Choosing these two devices allowed us to find participants who owned at least two different Apple devices due to the popularity of the iPhone [13].

Additionally, by the end of 2022, we repeated the same study with more recent versions of iOS *version 16.0+* and macOS *version 13.0+* to confirm any differences with regards to privacy configurations of default apps in the updated operating systems. The findings of this comparison are summarised in Table 16 (see Appendix A.6).

We repeated the same method used previously, that is, we first re-read the official sources provided by Apple and then observed the following minor changes:

(1) *Minor modification in access routes of privacy configurations.* This was observed for Safari and *Siri*. Simple changes included placing Safari settings, for example, within the Settings options, whereas previously in iOS 14.0+, users were able to access the Safari settings from the app itself.
(2) *Syntax and paraphrasing.* This was particularly observed in the privacy policy document. Revisions to privacy policies are needed and expected.
(3) *Use of bulleted lists.* This was only observed in the Location services description. Bullets were added to list the services that are also enabled if and when enabling Location Services.

We observed that even with these changes in newer operating systems, the issues observed in 2020 were still there. This highlights the importance of the issues previously noted in the first version of Study 1.

The detailed results of Study 1 are provided in Table 1 and in Appendices A.3 and A.4). The results point to several issues with information related to privacy and the ways to configure privacy-related settings that we summarize below:

All settings are not documented or are misleading. Apple does not mention all the privacy configurations required to be turned off to disable an app from functioning or sharing user's data, as shown in the summary Table 1 and extended Tables 6, 7 and 8 (see Appendix A.3). This is also the case when setting up devices

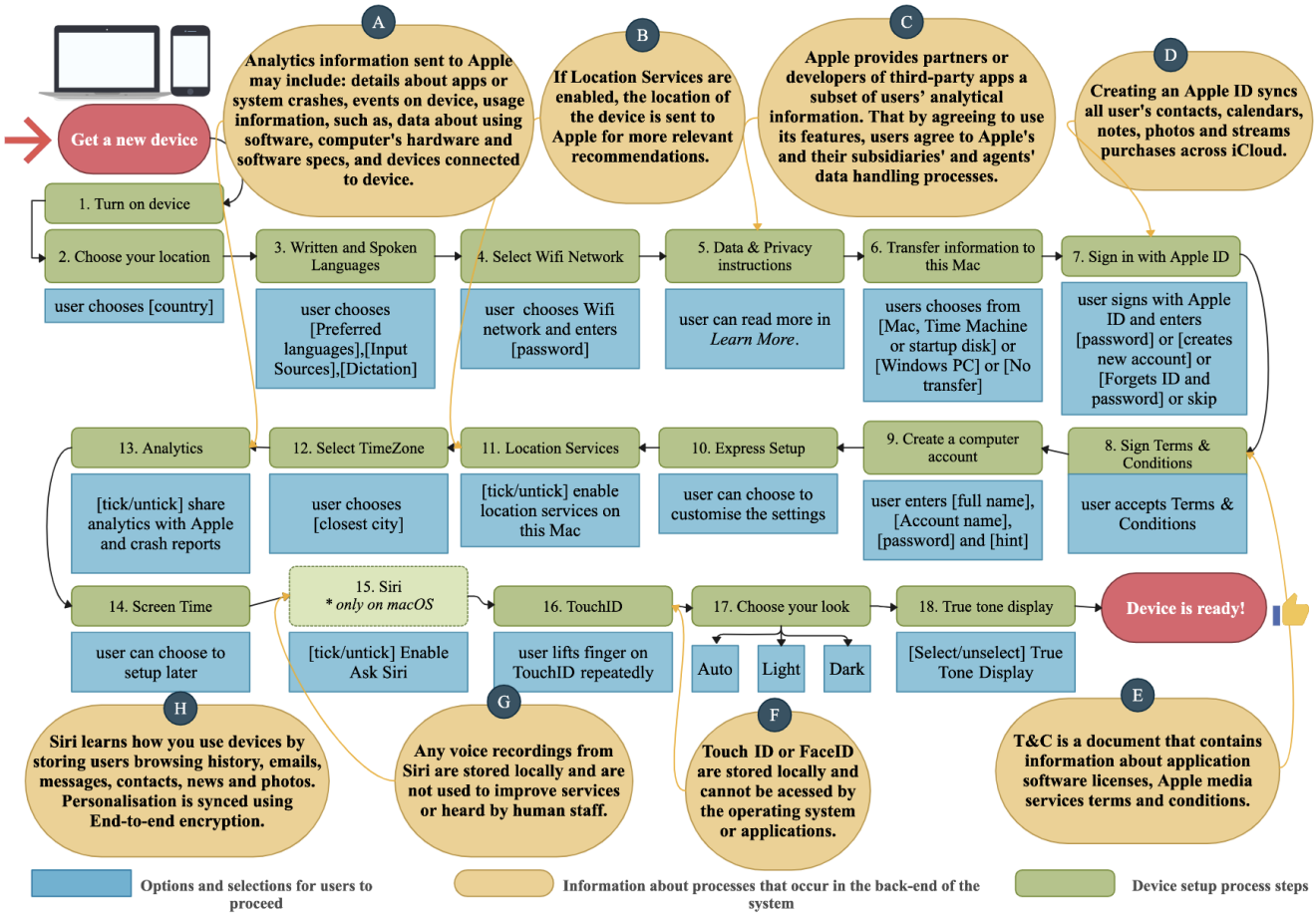

Figure 1: demonstrates the contrast between the steps users experience and the data handling processes involved at various stages of the device setup process. The user begins the process of setting up their device by purchasing a new device. Steps 1 - 18 explain the steps required for a complete setup of a user's device, for instance, a MacBook (macOS 10.15+). Yellow bubbles denoted by letters A - H are summaries of Apple's official privacy policy statement [3]. Bubbles A - H highlight examples of personal information collection occurring at various stages of the setup process. In addition to other data handling procedures, such as the location of the information stored (e.g., in F), users' fingerprints are stored locally on the device. We note that there may be slight variations between the order of the presentations of these settings in iOS and macOS. Additionally, *Siri* (*step 15*) is not prompted during device setup in iPhone (iOS 14.0) The order of the diagram is based on the order of presentation of the settings on macOS.

for the first time, as illustrated in Figure 1. The figure illustrates the steps the user is expected to carry out when first purchasing their device. We highlight what default apps and features are prompted to during setup and the hidden information that is not directly presented to users upon device setup. In the following, *Siri* is taken as the running example.

On Apple's official Privacy Policy [3], the instructions to disable the privacy configurations of *Siri* can be found for the following features: Ask Siri, Siri and Dictation, Siri Personalisation, iCloud Syncing, and Transcription. Other *Siri* privacy configurations are not mentioned such as Integrated apps, Dictation, Location Services, and Request History.

Further, even if the user disables an app, some settings remain enabled. For example, when first setting up the device, *Siri* is disabled by selecting *Set Up Later in Settings* in the Setup Wizard. Later on in the settings, *Siri* is seen to be disabled, seemingly matching what was selected when first setting up the device. However, this is incorrect, *Siri* continues to learn from app data to provide suggestions to users even if *Siri* is not "summoned". For example, in Table 9 (see Appendix A.3) various controls indicate that *Ask Siri* is controlled from a different configuration and that *Siri* syncing with iCloud. Such that attempting to disable *Ask Siri* does not automatically disable *Siri* from syncing with iCloud or other apps.

The information to control different configurations is also scattered under multiple menus or options. For example, disabling *Siri* can be found under *Safari Search* and *Siri and Search* [3].

Official documents are inconsistent. Efforts to improve the documents provided to users can be observed in Table 16 (see Appendix A.6). However, documents, such as privacy policies, offered for guiding users to learn about controlling their data remain inconsistent. For example, we compared the privacy policy available for users on iOS with the one available on macOS. Although the privacy policies provided to users on iOS and macOS are different, the privacy policy on iOS contains information on how to configure default apps on macOS and vice versa. Another issue we observed is that the privacy configurations of the operating systems are not separated. Rather, they are provided in the same section or even in the same paragraph. Additionally, there was an improvement in the use of bullet points to describe the data collected when using Location Services; however, this is not consistent with other default apps, such as *Siri*.

Unknown number of actions required to completely disable data sharing. As shown in Tables 6, 7, 8, 9 and 10 (see Appendix A.3), the privacy configurations belonging to an app are described with the respective paths to disable them. Importantly, the privacy configurations marked with an asterisk are the only privacy configurations belonging to an app mentioned in Apple's official documents. No information is found about the remaining privacy configurations.

Data handling practices are not disclosed. Even if users do follow this description and disable the provided privacy configurations, users receive no confirmation about the previous data they disabled with the app, nor they are notified whether their data is deleted or stored for longer periods. Additionally, Apple's documentation is missing information about what personal data is transmitted from the device (see Appendix A.3). For reference, users' personal data collected by the default apps are highlighted in Table 11 (see Appendix A.4).

In summary, we have presented a systematic evaluation of default apps and their privacy configurations. We discovered that the features are not clearly documented. Furthermore, we have presented summaries in this section and provided further details in the appendices. Specifically, we discovered that steps required to disable features of default apps are largely undocumented and the data handling practices are not completely disclosed.

4 STUDY II: QUALITATIVE STUDY

To capture users' understanding of privacy configurations of apps within a mobile ecosystem, we conducted a qualitative study.

4.1 Interview Participants

We conducted three pilot studies, which we did to test the interview script's flow, clarity, and topic order. The themes of the interviews were not altered from the pilot interviews. We then recruited 15 participants aged 18 or older across the country. Participants needed to be Apple users to be included in the study. The participants were recruited using the following methods: (1) posts on the university's official LinkedIn page and (2) Facebook paid advertisement for 14 days. Next, 67 volunteer participants completed a survey using the Webprobol online survey tool (See Appendix A.1 for screening survey content). The screening survey contained questions about participants: owning one or multiple devices, default apps they use, age, occupation, gender, and email addresses for contact purposes. The purpose of the screening survey was to diversify participants in terms of background and age groups. We selected 15 participants out of 67 who were later invited to the interview session based on the following conditions: they responded to the interview invitation and agreed to participate in the study, were at least 18 years old, used Apple devices, and were familiar with the usage of at least three default apps.

We interviewed 5 women and 8 men; 2 participants preferred not to disclose their gender. The majority of our participants were 18—29 years old. Participants represented a wide variety of educational and professional backgrounds, including Computer Science and IT, Architecture, Business Administration, Art and Design, Industrial Engineering, Economics, Research and Development, and unemployed participants. We interviewed participants who have at least used three or more default apps. All participants used Safari; 87% used Find My and iMessage (No distinction was made between iMessage Cloud service and regular SMS. Both services can be accessed from the same iMessage app.); 80% used TouchID, Location services, Facetime; and the least often used apps were Siri and Family Sharing, as shown in Table 2. Higher usage of default apps was observed in young adults. This also corresponds with a recent survey in 2019 [51], which estimated that the largest consumption of Apple products exists among young adults at the age of 16–24 years, followed by those at the age of 25–34 years. A summary of user demographics is available in Table 18 in Appendix A.8.

Table 2: Demographic characteristics of interview participants

Attribute	Range	Sample Size (N=15)
Gender	Female	5 (33%)
	Male	8 (53%)
	Not mentioned	2 (13%)
Age	18 - 29	8 (53%)
	30 - 39	5 (33%)
	40 - 49	1 (7%)
	50 - 59	1 (7%)
Default apps	Touch ID	12 (80%)
	Find My	12 (80%)
	Siri	10 (67%)
	Safari	15 (100%)
	Location Services	13 (87%)
	Family Sharing	4 (27%)
	iMessage	13 (87%)
	Facetime	11 (73%)

4.2 Ethical Considerations

Our institution's research ethics committee ruled that this study did not require formal ethical approval prior to conducting the study. Nevertheless, we ensured that we abide by ethical considerations

in Computer Science [6]: (1) All of our participants were provided information sheets containing information about the study, the voluntary nature of participation, and the right to discontinue and withdraw participation, data processing, and protection details. (2) Before the interview session, we read through the information sheets together with the participants to obtain informed consent.

4.3 Limitations

First, due to the qualitative nature of interviews and our constrained (N=15) sample size, the sample size was diverse in terms of age distribution among the highest consumers of Apple products, usage of default apps, and occupations of participants. However, our findings may not generalize beyond Apple's iOS and macOS due to these limitations. Nevertheless, research suggests that self-reported answers can provide valuable insights into users' experiences [44]. Second, the outbreak of COVID-19 contributed heavily to our decision to switch the study from in-person interview sessions to remote sessions. Study 2 could be strengthened if conducted in person, with the ability to observe how participants interact physically with the screens and devices of the ecosystem. Third, this study focused on two operating systems: iOS and macOS. We recruited participants who owned at least both iOS and macOS devices. This allowed us to reach a wider range of participants.

Furthermore, although the primary focus was to inquire about the use of these two devices, the open-ended questions allowed the participants to express their experiences in using other devices, such as iPads, watches, and smart TVs.

We also observed that participants focused more on the app configurations rather than variations in configurations between devices. Follow-up research could focus on a cross-comparison study between different ecosystems. Additionally, participants shared experiences that may not have been specific to default apps.

Possible next steps for this work could include recruiting a combination of non-Apple and Apple users. Users would be asked to configure the privacy settings as part of the tasks. The comparison between the two groups would shed light on user characteristics: for example, those users who are or are not familiar with the system differ from one another. The qualitative questions could be made more open-ended to elicit additional replies about users' experiences with Apple products. However, it is not practical to include many components in interview sessions or to expect users to remember much information on the spot. Due to this, we were concise with the tasks to avoid overwhelming our participants.

4.4 Interview Sessions

The semi-structured interviews were conducted remotely. The interview sessions took approximately 60–90 minutes. Participants were compensated with gift cards worth 20 euros after each interview. Interviews were audio-recorded. *Teams* transcription feature was used to transcribe the audio recordings. The transcripts were then proofread by the first author and checked for any possible syntax issues before analysis. Since the study was conducted during a global pandemic, interview sessions were held remotely. While performing the tasks, participants used a think-aloud protocol to describe the steps involved in executing the tasks.

4.5 Study Design

Topics for the interviews were formulated after reviewing previous work on the topic of privacy configurations in apps [43, 49]. The interview script was then designed to include questions inspired by previous studies and questions suitable to the scope of this study. Central topics discussed in the interviews included (a) the setup process of devices, (b) storage of personal information, (c) synchronization of personal information between devices, and (d) the ability to disable information sharing between devices through apps (also see Table 3). The base interview script can be found in Appendix A.2. The interview structure was divided into two parts: general questions and tasks. In the first part, participants were not informed on how to disable features, or how they actually work, as we aimed to gather their understanding related to the functionalities of default apps. We probed the participants about setting up their devices and perceptions of the process. In the second part (tasks), we asked the participants to try disabling certain features on a MacBook and iPhone. We also asked participants about their perceptions of what happened after they disabled certain features.

The interviews were conducted remotely over Zoom. The participants had their devices within arms reach, which allowed them to navigate their devices during the tasks. During the first part of the questions (general questions), participants were asked to recall their own experiences with Apple products. Next, in the second part of the interviews (practical tasks), participants were allowed to use available resources, if they wished, to complete the tasks. Participants were asked to verbally communicate what they were doing during each task and which settings were they navigating. Participants could also give up at any time and move on to the next task if they wished. At the end of the interview sessions, the participants provided feedback as well about the procedure and how they felt about it.

After interviewing ten participants, we arrived at a point of theoretical saturation. We resumed with five more participants to validate saturation. The interview phase ended with a total of 15 participants. The interviews resulted in 925 minutes of audio and 709 pages of transcripts.

4.6 Qualitative Data Analysis

To analyze and code the interview data, we used a hybrid approach: initial a-priori coding followed by inductive coding. Our coding process is one of many approaches common in HCI to ensure the reliability of data analysis [25]. The first author developed a codebook based on high-level categories, which included user experiences when setting up their devices, their knowledge of different app functionalities and disabling features, and what they know about the handling processes of their personal data by the default apps. Next, the first author coded two interviews under the high-level categories adding inductive codes. The first and second authors then discussed the codebook to resolve any disagreements. The following step was to use the updated codebook to code two more different interviews. The two authors met again for a discussion to agree on a common codebook. Once that was achieved, the coding of the remaining interviews was completed by the first author. We identified and organized categories as well as found relationships in our data. McDonald et al. [40] have studied best practices in HCI

Table 3: Central interview topics, research intentions and sample questions from interview script

Topic	Research Intention	Sample questions from interview script
Setup process	To understand how users think and process the setup of their devices	*Did you setup your [device] by yourself? How was the setup process for you?*
Storage of data	Participants thoughts on where their personal information is stored	*Where do you think your fingerprint information is stored?*
Synchronisation	Participants perception of how their personal information is shared	*Do you share your location on the devices that have the Family Sharing feature?*
Disabling features	To uncover if users are able to stop sharing of their personal information	*Do you know how to disable Safari from sharing your information between your devices on your iPhone?*

for seeking agreement and using inter-rater reliability (IRR). They suggest, for example, that there are justifiable cases, such as ease of coding where computing IRR is not necessary. As such, IRR test was not required for this work. The data was easy to interpret and there were no coding disputes. Furthermore, the transcripts were straightforward and needed little to no interpretation. Due to this, the first author who conducted the interviews reflected and examined them in the coding process, discussed them with the second author, and reached an agreement. These two typical scenarios are justifiable, according to McDonald et al. [40], for not computing IRR. The results of our data analysis are found in the next sections.

5 RESULTS OF STUDY II

In this section, we present the results of our semi-structured interviews. We identified three main themes that explain users' understanding of the privacy configurations and the impacts of making related decisions. The three themes are (1) Understanding of Configurations (2) Structure of Privacy Configurations and (3) Impacts of Setting Privacy Configurations. In addition to these three themes, the section *Verification: Challenges and Misunderstandings* shows the results from tasks asked users to perform. The tasks contributed to confirming users' challenges and misunderstandings about the mobile ecosystem.

Our results show that our participants were surprised that some of their information was shared by default. Participants were not able to disable default features. We also present unexpected results such that participants were also aware that they were being tracked even though were surprised about the extent of it. Participants were also aware that stopping data sharing does not guarantee that it is not shared anymore and that tracking introduced trust issues in family relationships.

Our findings further imply that several factors were found to contribute to the privacy decisions of apps. Users were aware that default apps were tracking them as well as retaining their data. The structure of privacy configurations contributed to the making of privacy decisions, such as the level of clarity of privacy configurations, transparency, and levels of organization. Overall, setting privacy configurations had several impacts on users such as causing a misunderstanding of functionalities, inability to disable them, and finally contributing negatively to relationships.

5.1 Theme 1: Understanding of Configurations

Our analysis revealed perceptions that users have of privacy configurations regarding different default apps. Several participants believed they were being tracked through some default applications. Such that data from Location services, Siri and Safari were collected from users. These data types included usage data of apps, GPS location, and voice data. Others were aware that stopping data sharing does not guarantee that their data is not shared anymore. Here data sharing can imply sharing with the service provider (Apple) or within the devices in an ecosystem.

Eleven out of 15 participants believed they were being tracked when using Location services, Siri and Safari. We have collected these answers from participants before sharing information related to default apps. Participants expressed that they knew that they were being tracked while using the mobile ecosystem. Participants elaborated that **tracking is useful sometimes but can also be invading.** They shared their experiences with default apps tracking them and how that impacted the situation; Participants thought that in certain instances, the tracking was useful for locating lost devices. Other times, it was rather invading. Participants expressed their awareness that Location services, Siri and Safari were tracking them. The participants referred to this as tracking repeatedly.

Participants explained that they are aware that different apps using location services are tracking them. For example, P01 explained that when using Maps in airplane mode she cannot be tracked anymore, then realized that her location was still traceable: *"I thought previously that when I turned airplane mode on, they could not track me anymore. But now like I was walking around a [city] the other day with airplane mode and like it could still track me down every street. So clearly that doesn't work, yeah, but I was not happy to find out about that."* - P01.

P01, P04, and P09 thought tracking on Find My could be useful in finding missing persons. One participant shared a personal incident that recently happened to him while hitchhiking in a city losing his phone as well as his family members and being able to track him based on his last location: *"and they had stopped to a MacDonald's so they didn't hear with their thing ringing .. I got my phone back but yeah it was great because I didn't have any of their contact information otherwise."* - P09

P01, P10, and P11 were concerned that Siri was tracking their activity on their devices. This was evident in tailored and restricted content when using other apps on their devices that Siri learns from: *"It hasn't only been the voice, but it also does with the search.*

Like when you start to search for something .. the app suggestions are mostly quite accurate, but the other things are not like sending an email to or contacting this person or your album or whatever. I don't think those are accurate and I don't like it." - P10.

Nine out of 15 participants were aware stopping data sharing does not guarantee it will not be shared anymore. We asked the participants about their thoughts about data retention before telling them information about it. Participants were aware that **data sharing was not completely disabled and data was not completely deleted from Safari, Siri and Location Services.**

One participant shared their concerns that it is challenging for users to validate whether their data is not shared anymore with the mobile ecosystem: *"I can't knock on Apple store to be like hey, did you actually do this but are better to have the possibility of it being disabled then? Knowing 100% that's not disabled?"* - P01.

Another participant shared concerns that Siri is never really completely turned off even if it seems disabled: *"It shouldn't be listening what you do. And then it's not shown on the menu bar and and it won't react to your hey Siri or whatever command you have on for accessing Siri .. at the same time, we don't know whether it's actually turned off, or whether Siri is listening.."* - P04.

5.2 Theme 2: Structure of Privacy Configurations

Participants want to know what happens to their information. Eleven out of 15 participants want more transparency from the ecosystem. They want to know **what privacy configurations are enabled by default and the user data stored and collected as a result.** Participants thought that more transparency in instructions could be useful. Participants also explained that privacy configurations can be too scattered.

P01 explained that there should instructions related to privacy configurations should be adjusted depending on the audience who will read them: *"You want that balance, right? because you'll have people who are very ignorant and they don't think about this .. that information should be given to them."* - P01.

P02 was asked about the privacy configurations of the apps. The participant described the organization of the default apps privacy configurations as "cloudy" and scattered: *"Because I do think that iCloud settings are a little bit kind of cloudy about what they actually do."* [sharing an experience specific to Siri as an instance of agreeing to data retention for improving the app] *"I already got Siri, so that's why I think it's quite fine with them collecting my personal data to improve the experience. But I do think that it should be a little bit more transparent about what kind of data they are collecting to improve my experience."* - P02.

P02, P04, and P12 agreed that users need more information about data handling practices from mobile ecosystem service providers. P04 was asked if Apple were transparent with their users: *"Every instance can be more transparent with the stuff nowadays. Especially the ones [meaning leading mobile companies] aiming to have some financial advantage over others to make money. Everybody could improve on that."* - P04

Four out of 15 participants thought that privacy **configurations of default apps are not organized clearly**. It was difficult to find certain settings at times. This had direct effects on being able to configure these privacy settings or re-configure them later. For example, P01 attempted to change the owner of the second-hand iPhone she received. She explained that she thought it was an intuitive process but it turned out to be otherwise: *".. I kept trying to change the owner of the phone. So like I think it's the associated Apple ID or the associated icon like who owns that phone. I kept changing it to me .. still kept defaulting to my sister's and my sister was getting all of the account notifications on things that were supposed to come to me. I don't know how that was eventually resolved, but I sort of just kept doing it and then it fixed itself .. I thought it was intuitive, but it clearly didn't work."* - P01.

P02 thought that it was confusing that System Preferences contains security settings as well as iCloud on MacBook: *".. way too scattered, for example, especially in this system preference on the MacBook, I would say that OK, so we've got Apple ID and then we've got iCloud, but then we also got Security and privacy as one option .. It's very scattered."* - P02.

5.3 Theme 3: Impacts of Setting Privacy Configurations

We asked the participants about what surprised them when using the mobile ecosystem. These questions were asked after we told the participants information about default apps. Participants were surprised that Siri, Safari, and Location Services enabled certain data sharing by default. Nine out of 15 participants expressed that **they were surprised that these privacy configurations did not match what they really wanted**.

Participants were surprised to learn that small subsets of requests that have been reviewed from Siri may be kept for more than two years as officially stated by Apple. P11 and P09 were specifically surprised to learn the list of apps that Siri collects data from: *"Why is it that Siri gets all that data and not just straight up Apple?"* - P09.

Similar to other apps such as Siri, location, and Photos. For example, Safari may send browsing information such as location, topics of interest, search queries and suggestions to Apple: *"I wasn't aware of that .. if I would search for anything sensitive, then I would switch browser."* - P06.

Family sharing app was considered useful yet still invading. Showing that the traditional criteria used to assess usability still does not seem to balance out users' privacy concerns. We asked the participants who have used Family Sharing about their experiences. Seven out of 15 participants thought Family Sharing as a default app could be useful. Family Sharing enables members to share their location, purchases, and other useful things. Participants believed this could introduce distrust in families and relationships because of the monitoring. Participants found family sharing to be useful, and in other instances rather invading.

P02, P07, and P013 found Family Sharing to be useful for multiple purposes; for example, safety or with finances: *"I think it's just kind of saved money in some way just by sharing, because you can share some purchases and stuff like that."* - P02; and family safety: *".. because it's just my child and I want her to be able to know where I am so. I share my location with her."* - P07.

P01, P13, and P15 found Family Sharing to introduce issues to family relationships. They shared their experiences on how they

thought monitoring other family members could cause trust issues as well as accidental sharing of personal content with other members. P01 was concerned that Family Sharing can affect teens' privacy: *"I know it has caused a lot of tensions in new avenues of how families and friendship tensions can develop and manifest [..] I mean, I think the overlap between like the parents genuine concern and like teenagers being responsible enough and trustworthy enough."* - P01.

5.4 Verification: Challenges and Misunderstandings

In the second part of the interviews, we verified users' knowledge of the privacy configurations of different default apps. In this section, we include the challenges and misunderstandings that users have about the eight default apps: TouchID, Family Sharing, Siri, Safari, Find My, iMessage, Facetime, and Location Services. Participants were confused about what happened to their information. We asked the participants about their understanding of the functionalities of the default apps. We collected their answers during the tasks. **All participants were unsure what privacy configurations did and how the ecosystem works** in Siri, Location Services, iMessage, Facetime, and Safari.

We recorded the pathways participants followed in Tables 12, 13, 14, and 15 in detail in Appendix A.5. The following is a summary of the main findings.

(1) Most participants start with OS settings first to disable default apps. When that did not disable default apps, they checked several different settings until they found something relevant. Alternatively, they used online help, such as *Google* or *Siri*.
(2) Participants resorted to online help after multiple failed attempts to find the solution to the task. They did not use Apple's official documentation.
(3) Participants generally did not use Apple ID or Cloud settings to attempt the tasks. They were generally confused about what disabling the cloud means to disabling the function of the app.
(4) For *Siri*, many participants believed that turning off *Hey Siri* was sufficient to disable the app completely.
(5) Participants generally gave up after one or two attempts at a given task and were unaware whether they succeeded at the task or not.

We provide below examples of the tasks participants struggled with.

P04 and P10 were unsure if disabling location services meant that their location could not be shared anymore. We asked the participants about what they thought about their location data and what happens if they disable it: *"Well, the phone itself has GPS operations going on anyway. Even when I have the data center off. So of course you could find a location for the iPhone device .."* - P04.

Participants expressed a lack of standardization over iOS and macOS privacy configuration menus. P11 was trying to disable iMessage and Facetime on his iPhone. When trying on his Macbook: *"I was just going to say that with Apple it's nice work, same way in different places, but not at this time."* He tries to access it from the iCloud then explains in confusion: *"The not in iCloud .. it has its own settings. Yeah, that's funny, right? Because it's .. the messages are in iCloud, but that's .. little bit illogical."* - P11.

Six participants out of 15 were unsure what happens when disabling Safari. We asked the participants what they thought happened with Safari and where their data was going. Participants expressed that when they delete information from one device it should be removed from all devices. Participants were also confused about whether deleting History, Bookmarks and Cache were enough to disable sharing: *"I'm not sure that if I disable the safari bookmarks, does it stop sharing everything?"* - P11.

All participants were unaware how to disable data sharing on Safari, Siri, Location Services, iMessage, Facetime, and Family Sharing. We collected participants' frustrations while performing the tasks. For example, P01 tried to disable Safari from sharing her data on her iPhone. She first went to Settings > Privacy and Security > Advanced. She shares: *"I'm trying to find if there's like a specific like security option on the iPhone."* She goes back to Settings and navigates: *"so I'm back in the settings page and I'm trying to find .. So earlier I was under Safari app. Now I'm trying to find like the general iPhone .. Security is what I'm intuitively trying to do.."* She finally shares her final assumption: *"Yeah no, I have no idea. This is where I would know I don't know."* - P01.

Similar challenges were faced by participants when attempting to disable Siri. P05 tries to access on her iPhone, General > Siri & Search > Suggestions on Lock Screen. Then she navigates the apps under Siri sub-menu and shares: *"Then there's press home for Siri and allow Siri. When locked, there are these trade toggles. I think that if I were to toggle them off, Siri would not show up, I think."* - P05.

6 DISCUSSION

We suspected before starting this work that Apple users are not aware of many of the implications on how their devices are setup. The authors did not have the complete picture either. To understand this better, we conducted Study 1, during which we identified several problems with the way these apps are explained to operate. Based on Study 1 findings, we were informed how to conduct Study 2 and the questions to ask users.

As outlined in the introduction, we divided our suspicions into four distinct research questions **RQ1)** What privacy configurations are available to control default apps, **RQ2)** How can users control the privacy configurations of default apps, **RQ3)** How do users understand privacy configurations and their privacy and security implications and **RQ4)** How does setting up default features impact the privacy of users?

We have presented two complementary studies that show the challenges in configuring desired privacy settings in the Apple iCloud mobile ecosystem. We have identified several issues with the current ways information is conveyed to users about configuring default apps. We have then found several problems with using the available information to modify the privacy settings of their apps.

6.1 Challenges with privacy configurations (RQ1, RQ2)

In this section, we discuss issues with how default apps work (Study 1) and how users understand them (Study 2).

We discovered in Study 2 that users do not understand how data is gathered, shared, and removed by default apps. For example, when a feature was disabled, users were uncertain whether this meant that their information was no longer shared. Our tasks confirmed that none of the default apps could be disabled by users. Additionally, having multiple steps required to disable app features is confusing and time-consuming. This is especially problematic when no confirmation messages indicate that certain features are completely disabled. Multiple locations to access the privacy configurations of a default app proved to be unhelpful to users.

According to our results, users have a difficult time finding privacy settings. In Study 2, users were unable to locate the privacy configurations easily after device setup. Presenting adequate descriptions of privacy controls is of key importance. Privacy configurations of default apps are typically hidden behind multiple screens, making them more difficult to access later on. Past research has shown that users do not change settings initially set up by them while being under the illusion that they are trusted recommendations from the service provider [1, 43]. To illustrate with examples from the analysis of privacy configurations of default apps and the paths to disable them (See tables 6, 7, 8, 9 and 10 in Appendix A.3), we provide Siri as an example: To configure Siri, users can find several privacy configurations under Settings > Siri & Search. Official documents only point to Ask Siri, Suggestions on Lock Screen. However, in Table 6, there are more settings that users are not informed by, such as Integrated apps, Dictation, and others. Settings > Siri & Search is not the only place in which users can find Siri settings, other routes include Settings > iCloud and Settings > Screen time. Interview data has also shown that the scattered nature of the privacy configurations has created challenges in configuring default apps for users.

Tables 12, 13 and 14 (See Appendix A.5) provide examples of a few specific routes that participants opted for when performing the practical tasks of the interview sessions. We compared the routes available to users versus what they have followed and found several issues with the routes followed by users: i) users opted to visit central OS settings (main iOS and macOS settings) as the first attempt to disable default apps, ii) a large number of participants scrolled randomly until something made sense to them, iii) there was clear confusion whether to disable the default apps directly from iCloud Settings, and whether this was enough to disable the app, and iv) participants had an expectation that privacy configurations would be located under the Privacy & Security tab rather than the central OS Settings tab.

6.2 Coping with challenges to configure default apps (RQ3, RQ4)

During the practical tasks, users frequently got stuck and tried various approaches to complete the tasks. Users sought online resources for assistance or relied on their own presumptions about how default apps operated when navigating the settings.

Participants did not turn to Apple's privacy policies for instructions on how to disable privacy configurations. Users preferred alternative assistance options, such as Siri or Google, to complete the tasks. Similarly and lacking in many aspects even in third-party apps, there was a lack of valuable information offered to users, which would be beneficial in assisting them in navigating privacy configurations.

For example, in this work, 6 out of 15 participants used online help to learn about how to disable data sharing on Safari. Prior work by Ramokapane et al. [43] found that all 11 users of iOS out of 20 participants used the internet to cope with configuration challenges, thus suggesting that users preferred search engines to navigate policies or service agreements. Another example is tracking by apps, in which we found that (11/15) participants were aware were being tracked when using default apps within the ecosystem. Frik et al. [22] found that between 38% and 65% of the study participants did not block tracking features, such as browsing or analytics, on their smartphone devices. We suggest that even though participants are aware that data is collected for tracking purposes, it can be useful to share data with the ecosystem to serve certain functionalities, such as Location Services.

Our results show that users were unable to distinguish between what information is shared within the mobile ecosystem (device to device) and between the ecosystem and service provider (Apple). This confusion led some users to use their techniques to protect their information, such as switching browsers (from Safari to another browser). Prior research suggests that users leave default feature configurations unchanged if they are confused about what the configurations do [15]. Our findings also revealed that most participants assumed they were being tracked when using different default apps within the mobile ecosystem. Our findings support previous research that suggested that users are aware of location services being turned on due to the requests they received from apps [14, 43].

Our results show that privacy configurations of apps, such as Family Sharing, can introduce tensions in family relationships. The distrust and tension may also be attributed to various social contexts and norms in which technologies operate. For example, in some countries, cultural beliefs and practices dictate that women are expected to share their devices with members of the family [45].

6.3 Recommendations

We present recommendations for resolving issues with default apps. The recommendations are necessary because, despite the time between the repetition of the study, the issues we discovered persisted in the latest updates. These suggestions should help designers and future research work in this area improve the current state of privacy around default apps.

We discovered that Apple has not changed the descriptions of default apps or the structure of settings over two years. After repeating our study with the recent operating system versions, our findings remained. We also found that issues remained valid even across these updates. We summarised several efforts from Apple to add more data types collected by default apps, as shown in Table 16 (see Appendix A.6). We observe that there are still serious issues around properly informing users about how to configure default apps. Our findings show that existing instructions do not effectively inform users about how to configure their privacy on default apps.

Below we offer some recommendations that we propose through this work to improve access to privacy configurations for users:

Our findings indicated that users turned to central OS settings as their first choice when attempting to disable privacy settings. This is one way to re-think the organization of privacy configurations of default apps. We suggest that changing the location of Safari settings from Safari app to central OS settings in recent operating systems may be a good start for better allocation of privacy configurations. This change seems aligned with the data collected from users in the interview study (see Appendix A.5) where we found that many users followed the Settings app path to find Safari settings, which was not the case earlier when the study was conducted in 2020. Similarly for other apps, we observed that users' first instinct is to visit the central OS settings to access any 'settings' related to their apps or devices in general. All default apps should adhere to this guideline to make it easier for users to navigate the settings of apps.

Past research emphasizes the importance of avoiding privacy fatigue to assist users in making useful privacy decisions [21, 26, 41]. While we did not assess this topic in our participants' responses, prior work agrees with our recommendation to give a standard location for controls to prevent user fatigue [26].

Apart from central OS settings, we suggest the following changes to the settings structure based on interview data. We found that participants often expected default app privacy configurations to be either in Settings or Privacy & Security tabs. However, this is not a standard feature across all default apps and operating systems. For example, i) on macOS, Safari settings are accessed only when users launch the app from the home screen. On iOS, users are not able to do the same by launching the app and navigating the settings. ii) Participants specifically found iOS to be the easier option in the case of iMessage and Facetime. iii) All default apps can be controlled from System Settings > Apple ID on macOS and Settings > Apple ID on iOS. It was a major confusion to users if they also needed to disable default apps from Apple ID or iCloud in addition to the options they have toggled in Settings. Thus, we recommend standardized interfaces for users on various platforms within the ecosystem. An example that seemed to work for users was accessing the privacy configurations of iMessage and Facetime directly from Settings. This is in contrast to Safari or Siri, which presented more challenges to configure, as denoted by the complexity of these apps.

Currently, default apps fail to notify users of what happens when attempting to disable certain privacy configurations. The lack of user instruction on data handling practices by apps is a prevalent issue [22, 33]. Therefore, notifications or pop-ups are much needed to alert users after performing a personal information-related process.

Data from this study revealed the lack of clarity in instructions provided to users about configuring default apps, such as inconsistent documents provided by the vendor, and challenges with allocating data and understanding data handling practices in the mobile ecosystem. Although default apps differ from third-party apps, as this work highlights early on (see Section 1), other work suggests a few challenges with controlling their privacy when using third-party apps that we have observed to be similar to default apps. We summarise the main connects and disconnects with prior work (see Table 17 in Appendix A.7). Next, we draw from recommendations of relevant work.

The current state of how to control privacy default apps confuses users. This was observed when participants learned about the data handling practices in a mobile ecosystem. In Study 1, we concluded that the majority of the default app configurations are found in Apple's privacy policies. Previous work on privacy policies suggested that users find privacy policies challenging in many ways, and they are often ignored by users [2, 12, 23, 34]. Privacy policies are often filled with legal jargon due to the complex nature of the rules and regulations of the region [11], regardless whether they have proved to be sufficient to inform users or not. In our study, participants were unable to clearly answer questions related to what happens to their data when they alter a specific configuration. Prior work has also suggested that displaying controls early on during the lifetime of a device might not be enough for users [43]. In fact, users have often been found to ignore end-user license agreements that are required to be signed before using the device(s) [8].

To further improve usability, we recommend that vendors not rely on privacy policies to include details on how users can configure default apps. We encourage designers of mobile ecosystems to provide meaningful illustrations or simple graphics to simplify how users' data is shared within the ecosystem before agreeing to use a default app. Additionally, friendly defaults or reminders [22] should be added: that clearly highlight the additional resources that the default app will use. We suggest that these reminders allow users the option to enable or disable the privacy configuration during this prompt. For example, by displaying a dialogue box that offers a shortcut to the privacy configuration so that the user is easily able to toggle the button.

To improve users' awareness of privacy controls, we suggest periodic prompts for privacy controls. These prompts should be aimed to assist users in understanding different ways that users can control their privacy in the platform. Prompts could also explain how data is handled by the ecosystem and how users can control different aspects of their data-sharing process. Currently, Apple has adapted Privacy Nutrition Labels [29] to inform users of the data gathered by apps. Additionally, these labels are offered on the vendor's own website and on the App Store. This is not helpful for default apps because they are *pre-installed*, and users are unlikely to verify this information during the course of their app usage. To help users better understand the kinds of data gathered by apps, Apple may periodically add these labels to their apps, after which they will be used. Using prompts is beneficial to remind users about available settings [22].

Additionally, personalized privacy interfaces that allow users to make decisions about their privacy have been studied with Android permissions and may be adopted in Apple's context [30]. Multi-layered privacy notices that appear to users at different times and contexts may be useful [46]. For example, it is expected that Siri needs to collect voice data among other forms of data to analyze user requests – as this is the main purpose of the application. Thus, this may not require frequent reminders about current information being collected. However, Siri also collects more than voice data. Siri also collects other user information, such as contact names, nicknames and relationships, music and podcast information and others [3]. This data is less expected to be collected; thus, appropriate notice to users must be given for an informed choice.

7 CONCLUSIONS

We found that the seamless integration of smart devices with the cloud reduces users' privacy. Our work shows that users may disable default apps, only to discover later that the settings do not match their initial preference. In this paper, we presented two studies. First, we evaluated the privacy configurations of default apps. Second, we conducted interviews to understand users' perceptions of these privacy configurations. Our results demonstrate users are not correctly able to configure the desired privacy settings of default apps. In addition, we discovered that some default app configurations can even reduce trust in family relationships.

ACKNOWLEDGMENTS

This work was funded by the Research Council of Finland via grant numbers 345991 and 345992. We are grateful to all study participants for their time, experiences, and insights. We note that *Privacy of Default Apps in Apple's Mobile Ecosystem* is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc.

REFERENCES

[1] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347 (2015), 509 – 514.

[2] Manar Alohaly and Hassan Takabi. 2016. Better Privacy Indicators: A New Approach to Quantification of Privacy Policies. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 7 pages.

[3] Apple. 2021. *Apple Privacy Policy*. Apple Inc. Retrieved September 9, 2021 from https://www.apple.com/legal/privacy/en-ww/ Web link.

[4] Apple. 2022. *Apple Ecosystem*. Apple Inc. Retrieved February 18, 2022 from https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf Web link.

[5] Apple. 2022. *Privacy*. Apple Inc. Retrieved December 12, 2022 from https://www.apple.com/privacy/ Web link.

[6] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. 2012. The Menlo Report. *IEEE Security & Privacy* 10, 2 (2012), 71–75.

[7] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. "Little Brothers Watching You": Raising Awareness of Data Leaks on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 12, 11 pages.

[8] Rainer Böhme and Stefan Köpsell. 2010. Trained to Accept? A Field Experiment on Consent Dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2403–2406. https://doi.org/10.1145/1753326.1753689

[9] Frank Breitinger, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2019. A survey on smartphone user's security choices, awareness and education. *Computers & Security* 88 (10 2019), 101647.

[10] P. R. J. Campbell and Faheem Ahmed. 2010. A Three-Dimensional View of Software Ecosystems. In *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume* (Copenhagen, Denmark) *(ECSA '10)*. Association for Computing Machinery, New York, NY, USA, 81–84.

[11] Fred H. Cate. 2010. The Limits of Notice and Choice. *IEEE Security & Privacy* 8, 02 (mar 2010), 59–62. https://doi.org/10.1109/MSP.2010.84

[12] Rena Coen, Jennifer King, and Richmond Wong. 2016. The Privacy Policy Paradox. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 3 pages.

[13] Competition and GOV.UK Markets Authority. 2021. *Mobile ecosystems Market Study*. GOV.UK. Retrieved June 7, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1048746/MobileEcosystems_InterimReport.pdf Web link.

[14] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Portland, Oregon, USA) *(CHI '05)*. Association for Computing Machinery, New York, NY, USA, 81–90.

[15] Gregory Conti and Edward Sobiesk. 2010. Malicious Interface Design: Exploiting the User. In *Proceedings of the 19th International Conference on World Wide Web* (Raleigh, North Carolina, USA) *(WWW '10)*. Association for Computing Machinery, New York, NY, USA, 271–280.

[16] Kovila P.L. Coopamootoo, Maryam Mehrnezhad, and Ehsan Toreini. 2022. "I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 287–304.

[17] Serge Egelman, Adrienne Felt, and David Wagner. 2013. Choice Architecture and Smartphone Privacy: There's A Price for That. *The Economics of Information Security and Privacy* 1, 1 (10 2013), 211–236. https://doi.org/10.1007/978-3-642-39498-0_10

[18] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. 2011. Android Permissions Demystified. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '11)*. Association for Computing Machinery, New York, NY, USA, 627–638. https://doi.org/10.1145/2046707.2046779

[19] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (Raleigh, North Carolina, USA) *(SPSM '12)*. Association for Computing Machinery, New York, NY, USA, 33–44.

[20] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages.

[21] Yuanyuan Feng, Yaxing Yao, and Norman Sadeh. 2021. A Design Space for Privacy Choices: Towards Meaningful Privacy Control in the Internet of Things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 64, 16 pages. https://doi.org/10.1145/3411764.3445148

[22] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users' Expectations About and Use of Smartphone Privacy and Security Settings. In *CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 407, 24 pages.

[23] Julien Gamba, Mohammed Rashed, Abbas Razaghpanah, Juan Tapiador, and Narseo Vallina-Rodriguez. 2020. An Analysis of Pre-installed Android Software. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, an Francisco, USA, 1039–1055. https://doi.org/10.1109/SP40000.2020.00013

[24] Google. 2022. *Google Products*. Google. Retrieved February 18, 2022 from https://about.google/products/ Web link.

[25] Greg Guest, Arwen Bunce, and Laura Johnson. 2006. How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods* 18, 1 (2006), 59–82.

[26] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a Scavenger Hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376511

[27] Avery Hartmans. 2021. *Apple said the Pro models of the iPhone 12 sold the best last quarter as a record number of people upgraded their devices*. Business Insider. Retrieved February 7, 2022 from https://www.businessinsider.com/apple-iphone-12-pro-pro-max-sold-best-in-q1-2021-1?r=US&IR=T Web link.

[28] Huawei. 2022. *Huawei Ecosystem*. Huawei. Retrieved February 18, 2022 from https://consumer.huawei.com/en/community/details/Huawei-Ecosystem-Interconnectedness-of-my-devices/topicId_148614/ Web link.

[29] Apple Inc. 2023. *Privacy Nutrition Labels*. Apple Inc. Retrieved September 13, 2023 from https://www.apple.com/privacy/labels/ Web link.

[30] Corey Brian Jackson and Yang Wang. 2018. Addressing The Privacy Paradox through Personalized Privacy Notifications. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 2, Article 68 (jul 2018), 25 pages. https://doi.org/10.1145/3214271

[31] Haojian Jin, Minyi Liu, Kevan Dodhia, Yuanchun Li, Gaurav Srivastava, Matthew Fredrikson, Yuvraj Agarwal, and Jason I. Hong. 2018. Why Are They Collecting My Data? Inferring the Purposes of Network Traffic in Mobile Apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 173 (dec 2018), 27 pages. https://doi.org/10.1145/3287051

[32] Kaspersky. 2022. *What is Jailbreaking – Definition and Explanation*. Kaspersky. Retrieved December 5, 2022 from https://www.kaspersky.com/resource-center/definitions/what-is-jailbreaking Web link.

[33] 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* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages.

[34] Patrick Kelly, Sunny Consolvo, Lorrie Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *International Conference on Financial Cryptography and Data Security*, Vol. 7398. Springer, Berlin, Heidelberg, 68–79.

[35] Yuanchun Li, Fanglin Chen, Toby Jia-Jun Li, Yao Guo, Gang Huang, Matthew Fredrikson, Yuvraj Agarwal, and Jason I. Hong. 2017. PrivacyStreams: Enabling Transparency in Personal Data Processing for Mobile Apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 3, Article 76 (sep 2017), 26 pages. https://doi.org/10.1145/3130941

[36] Ilaria Liccardi, Joseph Pato, Daniel J. Weitzner, Hal Abelson, and David De Roure. 2014. No Technical Understanding Required: Helping Users Make Informed Choices about Access to Their Personal Data. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (London, United Kingdom) *(MOBIQUITOUS '14)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, BEL, 140–150.

[37] Bin Liu, Jialiu Lin, and Norman Sadeh. 2014. Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?. In *Proceedings of the 23rd International Conference on World Wide Web* (Seoul, Korea) *(WWW '14)*. Association for Computing Machinery, New York, NY, USA, 201–212.

[38] Michael Lutaaya. 2018. Rethinking App Permissions on IOS. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI EA '18)*. Association for Computing Machinery, New York, NY, USA, 1–6.

[39] Aleecia McDonald and Lorrie Faith Cranor. 2010. Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising. In *TPRC Conference*. TPRC, USA, 1–31.

[40] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (nov 2019), 23 pages. https://doi.org/10.1145/3359174

[41] Sanju Menon, Weiyu Zhang, and Simon T. Perrault. 2020. Nudge for Deliberativeness: How Interface Features Influence Online Discourse. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376646

[42] Jeffrey Palmerino. 2018. Improving Android Permissions Models for Increased User Awareness and Security. In *Proceedings of the 5th International Conference on Mobile Software Engineering and Systems* (Gothenburg, Sweden) *(MOBILESoft '18)*. Association for Computing Machinery, New York, NY, USA, 41–42.

[43] Kopo M. Ramokapane, Anthony C. Mazeli, and Awais Rashid. 2019. Skip, Skip, Skip, Accept: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proceedings on Privacy Enhancing Technologies* 2019, 2 (April 2019), 209 – 227.

[44] Elissa M. Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L. Mazurek. 2018. Asking for a Friend: Evaluating Response Biases in Security User Studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1238–1255.

[45] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchil. 2018. "Privacy is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 127–142.

[46] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A Design Space for Effective Privacy Notices. In *Symposium on Usable Privacy and Security (SOUPS)* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 1–17.

[47] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can Systems Explain Permissions Better? Understanding Users' Misperceptions under Smartphone Runtime Permission Model. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, virtual event, 751–768. https://www.usenix.org/conference/usenixsecurity21/presentation/shen-bingyu

[48] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2347–2356.

[49] Daniel Smullen, Yuanyuan Feng, Shikun Aerin Zhang, and Norman Sadeh. 2020. The Best of Both Worlds: Mitigating Trade-offs Between Accuracy and User Burden in Capturing Mobile App Privacy Preferences. *Proceedings on Privacy Enhancing Technologies* 2020, 1 (2020), 195–215.

[50] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. 2014. The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 91–100.

[51] Petroc Taylor. 2021. *Smartphone OS in 2019, by age group*. Statista. Retrieved February 8, 2022 from https://www.statista.com/statistics/1133193/smartphone-os-by-age/ Web link.

[52] Christopher Thompson, Maritza Johnson, Serge Egelman, David Wagner, and Jennifer King. 2013. When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, UK) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 1, 14 pages.

[53] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 4, 15 pages.

[54] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, and Nigel Shadbolt. 2017. Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 5208–5220.

[55] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. 2018. Contextualizing Privacy Decisions for Better Prediction (and Protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13.

A APPENDIX

A.1 Appendix A: Online Survey

This is a screening survey for our research study. Please fill out this survey and we will contact you if you are eligible for the study. The actual study is in the form of an interview. The interview will take place over Zoom. Participation in this study will take approximately 1 hour. The session will be voice-recorded. To participate in this survey, please provide us with the following information. (Mandatory fields are marked with an asterisk (*) and must be filled in to complete the form.)

1. Do you own both an iPhone and a Macbook? *
   - I use both an IPhone and a Macbook
   - I use an iPhone only
   - I use a Macbook only
   - I do not use an iPhone or a Macbook
2. Your iPhone Model
   - iPhone 11, 11 Pro, 11 Pro Max
   - iPhone XS and XS Max
   - iPhone XR
   - iPhone X
   - iPhone 8
   - iPhone 8 Plus
   - iPhone 7
   - iPhone 7 Plus
   - iPhone 6S
   - iPhone 6S Plus
   - iPhone SE (2020)
   - iPhone SE (2016)
   - I do not use an iPhone

3. Your iPhone Operating System Version (To check, go to Settings > General > About > Software Version): *type here operating system version.*
4. Your Macbook Model
   - MacBook: 2015 and later
   - MacBook Air: 2012 and later
   - MacBook Pro: 2012 and later
   - I do not use a MacBook

5. Your Macbook Operating System Version (To check, go to the top left apple symbol on your menu bar and select About this Mac): *type here operating system version.*
6. Do you use the following applications? (Please select all that apply)
   - TouchID
   - Find My
   - Siri
   - Safari
   - Location Services
   - Family Sharing
   - iMessage
   - Facetime
7. What is your gender (or write "prefer not to say")?
8. Age *
   - 18 - 29
   - 30 - 39
   - 40 - 49
   - 50 - 59
   - 60+

9. Occupation *: *enter occupation here*
10. Your email address we can use to contact you if you are chosen for the interview *: *enter your email here*

A.2 Appendix B: Interview Guide

You have been invited to participate in a research study. Participation in this study is voluntary. You can discontinue your participation in the study at any time. Should you discontinue your participation, you will not be subject to any negative consequences. The interview is divided into two parts: General questions and Practical tasks. You may use your personal devices for the practical tasks. Please feel free to ask during the interview process and enquire about the questions.

(Participants signed a consent form before proceeding to the interviews, read information sheet about the study and the privacy policy for handling data)

A.2.1 General Questions:

(1) What is the model of your iPhone?
(2) What is the model of your Macbook?
(3) Do you have an iCloud Account?
(4) Do you have an Apple ID?
(5) Did you set up your iPhone by yourself?
(6) Did someone else help you setup your iPhone?
(7) Did you setup your MacBook by yourself?
(8) Did someone else help you setup your MacBook?
(9) How was the setup for you? [Follow up question: What did you think of the instructions that were provided to guide you? Did you notice any instructions about collecting your personal information?]
(10) Are you using TouchID?
(11) Where do you think your fingerprint information is stored? For instance, on the drive or on the Cloud? Follow up question: Do you remember reading anything about this when setting up your fingerprint? How do you wish that you were informed?
(12) What apps that were already on your iPhone were you using? [Follow up question: Do you think they are useful?]
(13) What apps that were already on your MacBook were you using? [Follow up question: Do you think they are useful?]
(14) Are you using FindMy on your iPhone?
(15) Are you using FindMy on your MacBook?
(16) Do you know what FindMy is used for? [Follow up question: Have you ever been in a situation where you had to use FindMy? How was that experience? Do you think FindMy can be improved to be more effective?]
(17) Do you know what is Siri?
(18) Do you know what Siri is used for?
(19) If you use Siri, how does Siri help you? [Follow up question: Do you know the type of information Siri collects?]
(20) Does Siri collect your voice recordings? [follow up question: Do you think Siri is collecting more that it needs?]

(21) Are you okay with Siri collecting your voice recordings? [Follow up question: How do you think Siri can be improved to not collect so much?]
(22) Do you use Location Services on your iPhone?
(23) Do you use Location Services on your MacBook?
(24) Does your iPhone store the place that you have visited? [Follow up questions: Is it always enabled? What do you think about a device knowing your whereabouts?]
(25) Would you be okay with your location being stored? [Follow up questions: What situations do you think this can prove to be useful the most?]
(26) Do you know which applications collect your location data? [Follow up questions: Is it easy to find?]
(27) Do you know what Apple Analytics are?
(28) Do you think apple collects your personal information? [Follow up questions: Is there some information that you don't want to be collected? Do you know how to stop apple from collecting that information? How do you wish you were informed about not sharing some data? How would you want to see this option?]
(29) What kind of information do you think Apple Collects?
(30) Do you store your pictures, videos on your phone? [Follow up questions: Do the photos and videos that you store contain sensitive information? Do you use any techniques to protect these photos and videos?]
(31) Do you know that Apple has access to the information you store on the Cloud such as your Photos, videos etc.?
(32) Apple claims that it collects your personal information to improve your experience. What are your thoughts about this?
(33) Can you stop data sharing? [Follow up questions: Do you think Apple makes it clear on how to stop data sharing? How do you think that can be improved?]
(34) Is your data stored anywhere else other than your phone? [Follow up questions: This could be the Cloud or on your Phone?]
(35) What happens to your data once you stop sharing it with Apple? [Follow up questions: Do you think there are other ways to let you know about the fate of your data? Do you remember reading this anywhere? Do you think users should be compensated for their data?]
(36) Do you use iMessage?
(37) Do you use Facetime?
(38) Are you aware that iMessage and Facetime delete your messages and calls after some time? [Follow up questions: Do you know that you can control the time your messages and calls are stored?]
(39) Do you use family sharing?
(40) Do you use Family sharing feature on your iPhone?
(41) Do you use Family sharing feature on your MacBook?
(42) If so, how many family members have access to the Family Shared devices?
(43) Do you have the Public Sharing feature in Family sharing enabled?
(44) Do you know that the family members using the Family feature can see your purchases, location etc.?
(45) Do you share your location on the devices that have the Family Sharing feature?
(46) Do you use Safari on your iPhone?
(47) Do you use Safari on your MacBook?
(48) Do you share your browsing information across your devices on your iPhone?
(49) Do you share your browsing information across your devices on your MacBook? [Follow-up question: How does that affect your experience?]
(50) Do you know what information Safari shares across your devices?
(51) Are you okay with Safari sharing information about your browsing across devices?

A.2.2 Practical Questions. These questions should be performed on both the iPhone and the MacBook.

(1) Do you know how to disable Safari from sharing your information between devices on your iPhone?
(2) Do you know how to disable Safari from sharing your information between devices on your MacBook? [Follow up questions: Can you talk about your feelings after completing this process?]
(3) What do you think happened now that you have disabled sharing? [Follow up questions: How do you think this can be communicated to you in a better way?]
(4) Do you think that turning off sharing in Safari across the devices guarantees that no data is shared anymore across these devices? [Follow up questions: How do you think this can be communicated to you in a better way? Do you think the current terms and conditions statement can be improved?]
(5) Do you know how to delete history/bookmarks and other information from Safari on your iPhone?
(6) Do you know how to delete history/bookmarks and other information from Safari on your MacBook? [Follow up questions: Can you talk about your feelings after completing this process?]
(7) What do you think happened now that you have deleting your stored information?
(8) Do you think your history from your previous search has been deleted? [Follow up questions: Do you think it is Apple's responsibility to notify users when their data has been completely deleted?]
(9) Do you know how to turn off Apple Pay in Safari on your iPhone?
(10) Do you know how to turn off Apple Pay in Safari on your MacBook?
(11) Apple Pay is turned on by default for Safari. Tell me your thoughts about that?
(12) Do you know that your device may send information such as location, topics of interest, search queriers, suggestions you have selected and related usage data to Apple?
(13) Do you know how to disable the public sharing in Family Sharing on your iPhone?
(14) Do you know how to disable the public sharing in Family Sharing on your MacBook?
(15) Do you know how to hide your purchases in Family Sharing on your iPhone?

(16) Do you know how to hide your purchases in Family Sharing on your MacBook?
(17) Do you know how to hide your location in Family Sharing on your iPhone?
(18) Do you know how to hide your location in Family Sharing on your MacBook?
(19) Do you know that if Purchase Sharing is enabled, members of your family will automatically be able to access many of your past and future App Store, Apple Books and Apple Music purchases, unless you choose to hide those purchases? How do you feel about that?
(20) Do you know how to disable iMessage on your iPhone?
(21) Do you know how to disable iMessage on your MacBook?
(22) Do you know how to disable Facetime on your iPhone?
(23) Do you know how to disable Facetime on your Macbook?
(24) Do you know that iMessage and Facetime use end-to-end encryption?
(25) Do you know what end-to-end encryption means? [Follow up question: Do you know that iMessage and Facetime use end-to-end encryption?]
(26) Do you know that Apple can't read the contents of your conversations when they are in transit between devices? How do you feel about that?
(27) Do you know that iMessage messages can be set to be deleted after 30 days, a year or stored forever? How do you feel about that?
(28) Are you okay with apps sharing your information with Siri?
(29) Do you know how to disable Siri from collecting data from apps on your iPhone?
(30) Do you know how to disable Siri from collecting data from apps on your Macbook?
(31) Do you know how to disable Siri on your iPhone?
(32) Do you know how to disable Siri on your MacBook?
(33) Do you know that the things you say, and dictate will be sent to Apple to process your requests? How do you feel about that?
(34) After six months, your request history is dissociated from the random identifier and may be retained for up to two years to help Apple develop and improve Siri. What do you think about that?
(35) Do you think your older voice data is deleted once you have disabled Siri?
(36) Do you know that a small subset of requests that have been reviewed may be kept beyond two years without the random identifiers for ongoing improvement of Siri?
(37) Do you know that apps contribute information to personalize Siri?
(38) Do you know how to check which application collects your location data on your iPhone?
(39) Do you know how to check which application collects your location data on your MacBook?
(40) Do you know how to disable Location on your iPhone?
(41) Do you know how to disable Location on your MacBook? [Follow-up question: What do you think happened?]
(42) Do you know that you can disable the live locations for applications separately? How do you feel about that? Does it make sense?
(43) Do you think that upon disabling Location services that Apple cannot obtain your location anymore?
(44) Apple doesn't completely anonymize your data, leaving in things like location. How do you feel about that?
(45) How accurate do you think your location that is collected is?
(46) Your device reminds you from time to time that an application is using your location. How do you feel about that?
(47) To deliver relevant suggestions, Apple may use the IP address of your internet connection to approximate your location. How do you feel about that? [Follow up question: What are your thoughts?]

A.3 Appendix C: Privacy Controls

Table 4: Privacy Configurations for each default app: Safari, Siri, iMessage and Facetime. Last column suggests whether users' personal data may leave their devices. Yes/No: Apple mentions this information in their privacy Policy documents, Information not provided by vendor: there is currently no information on Apple's privacy policy or resources if this data category leaves users' device or not. Not Applicable: no known personal data involved.

App	N Steps	Privacy Configurations	May transfer to Cloud or Vendor's Servers
Safari	N>12	IP Address	Yes
		Fradulent Website Warning	Not Applicable
		Privacy Preserving Ad Measurement	Yes
		Check for Apple Pay	Yes
		Private Browsing	No
		Web Page Translation	Translation locally, other data may leave device
		Web Extensions	Yes
		iCloud Syncing	Yes
		Search Engine Suggestions	Yes
		Preload Top Hit in Safari	Information not provided by vendor
		Sending Information to Apple	Yes
		History and Website Data	Yes
Siri	N>9	Ask Siri	Yes
		Integrated apps	Yes
		Dictation	Yes
		Siri and Dictation	Yes
		Siri Personalisation	Yes
		iCloud Syncing	Yes
		Transcription	Yes
		Location Services	Yes
		Request History	Yes
iMessage	N>5	Messages in iCloud	Yes
		Delete Messages	Yes
		iCloud Backup	Yes
		Shared with You	Yes
		Shared with Apps	Yes
Facetime	N>7	Enable Facetime	Actual calls No, Otherwise Yes
		Caller ID	Yes
		SharePlay	Information not provided by vendor
		Speaking	Information not provided by vendor
		FaceTime Live Photos	Information not provided by vendor
		Eye Contact	Information not provided by vendor
		Blocked Contacts	Information not provided by vendor

Table 5: Privacy Configurations for each default app: Touch ID, Location, Find My. Last column suggests whether users' personal data may leave their devices. Yes/No: Apple mentions this information in their privacy Policy documents, Information not provided by vendor: there is currently no information on Apple's privacy policy or resources if this data category leaves users' device or not. Not Applicable: no known personal data involved.

App	N Steps	Privacy Configurations	May transfer to Cloud or Vendor's Servers
Touch ID	N>9	Passcode	No
		Add fingerprint (1,2,..N=5 max)	No
		Delete fingerprint	No
		Device Unlock	No
		iTunes and App Store	No
		Wallet and Apple Pay	No
		Password AutoFill	No
		Voice Dial	No
		Allow Access to Apps	Information not provided by vendor
Location	N>6	Enable Location	Yes
		Tracking	Yes
		Allow Apps to Track	Yes
		Analytics and Improvements	Yes
		Apple Advertising	Yes
		App Privacy Report	Yes
Find My	N>4	Enable Find My	Yes
		My Location	Yes
		Share My Location	Yes
		Family	Yes

Table 6: Privacy Configurations of default apps on iOS: Safari and Siri and paths to disable these settings. Paths marked by (*) are provided in Apple's Privacy Policy. The remaining paths are not provided for users.

Default App	Privacy Configurations	Path to disable
Safari	Hide IP Address*	Settings > Safari > Hide IP Address
	Fradulent Website Warning*	Settings > Safari > Fradulent Website Warning
	Privacy Preserving Ad Measurement*	Settings > Safari > Privacy Preserving Ad Measurement
	Check for Apple Pay*	Settings > Safari > Privacy and Security
	Private Browsing	Safari > Tabs > Private
	Web Page Translation	Settings > Safari > Advanced > Website data > Search "translate" or "Google"
	Web Extensions*	Settings > Safari > Extensions
	iCloud Syncing*	Settings > [your name] > iCloud > Safari
	Search Engine Suggestions	Settings > Safari > Search > Safari Suggestions
	Preload Top Hit in Safari	Settings > Safari > Search > Preload Top Hit
	Siri Suggestions*	Settings > Safari > Safari Suggestions
	Clear History and Website Data	Settings > Safari > Clear History and Website Data
Siri	Ask Siri*	Settings > Siri and Search > Listen for "Hey Siri" Settings > Accessibility > Always Listen for "Hey Siri"
	Integrated apps	Settings > Siri and Search > [app name] > Use with Ask Siri
	Dictation	Settings > General > Keyboard > Enable Dictation
	Suggestions on Lock Screen*	Settings > Siri and Search > Turn off suggestions on Lock Screen
	Location Services for Siri Suggestions*	Settings > Privacy > Location Services > System Services > Location-Based Suggestions
	Siri and Dictation*	Settings > Screen Time > Content and Privacy Restrictions > Allowed apps
	Siri Personalisation*	Settings > [your name] > iCloud > Siri
	iCloud Syncing*	Settings > [your name] > iCloud > Siri
	Transcription*	Settings > Privacy > Speech Recognition
	Location Services	Settings > Privacy > Location Privacy
	Request History	Settings > Siri and Search > Siri and Dictation History

Table 7: Privacy Configurations of default apps on iOS: iMessage, Facetime, Family Sharing and Touch ID and paths to disable these settings. Paths marked by (*) are provided in Apple's Privacy Policy. The remaining paths are not provided for users.

Default App	Privacy Configurations	Path to disable
iMessage	Messages in iCloud*	Settings > Messages > iMessage
	Delete Messages	Settings > Messages > iMessage > Message History
	iCloud Backup	Settings > Messages > iMessage > Enable Messages in iCloud
	Shared with You*	Settings > Messages > Shared with You
	Shared with Apps	Settings > Messages > Shared with You > Apps
Facetime	Enable Facetime*	Settings > FaceTime > Toggle FaceTime
	Caller ID	Settings > FaceTime > Caller ID
	SharePlay	Settings > FaceTime > SharePlay
	Speaking	Settings > FaceTime > Automatic Prominence > Speaking
	FaceTime Live Photos	Settings > FaceTime > FaceTime Live Photos
	Eye Contact	Settings > FaceTime > Eye Contact
	Blocked Contacts	Settings > FaceTime > Calls > Blocked Contacts
Family Sharing	Family Setup	Settings > Apple ID > Family
	Apple Subscription	Settings > Apple ID > Family > Apple Subscriptions
	Ask to Buy	Settings > Apple ID > Family > App Store Subscriptions
	Screen Time	Settings > Apple ID > Family > Screen Time
	Purchase Sharing	Settings > Apple ID > Family > More to Share > Purchase Sharing
	iCloud+	Settings > Apple ID > Family > More to Share > iCloud+
Touch ID	Passcode	Settings > Touch ID and Passcode > Turn Passcode Off
	Add fingerprint (1,2,..N=5 max)	Settings > Touch ID and Passcode > Fingerprints
	Delete fingerprint	Settings > Touch ID and Passcode > Fingerprints
	Device Unlock	Settings > Touch ID and Passcode > Use Touch ID For
	iTunes and App Store	Settings > Touch ID and Passcode > Use Touch ID For
	Wallet and Apple Pay	Settings > Touch ID and Passcode > Use Touch ID For
	Password AutoFill	Settings > Touch ID and Passcode > Use Touch ID For
	Voice Dial	Settings > Touch ID and Passcode > Voice Dial
	Allow Access to Apps	Settings > Touch ID and Passcode > Allow Access When Locked

Table 8: Privacy Configurations of default apps on iOS: Location and Find My and paths to disable these settings. Paths marked by (*) are provided in Apple's Privacy Policy. The remaining paths are not provided for users.

Default App	Privacy Configurations	Path to disable
Location	Enable Location*	Settings > Privacy > Location Services
	Tracking	Settings > Privacy > Location Services > Location Alerts
	Allow Apps to Track	Settings > Privacy > Tracking > Allow Apps to Request Track
	Analytics and Improvements	Settings > Privacy > Analytics and Improvements
	Apple Advertising	Settings > Privacy > Apple Advertising
	App Privacy Report	Settings > Privacy > App Privacy Report
Find My	Enable Find My*	Settings > Apple ID > Find My
	My Location	Settings > Apple ID > Find My > My Location
	Share My Location	Settings > Apple ID > Find My > Share My Location
	Family	Settings > Apple ID > Find My > Family

Table 9: Privacy Configurations of default apps on macOS: Safari, Siri and iMessage and paths to disable these settings. Paths marked by (*) are provided in Apple's Privacy Policy. The remaining paths are not provided for users.

Default App	Privacy Configurations	Path to disable
Safari	Hide IP Address*	Safari > Settings > Hide IP Address
	Fradulent Website Warning*	Safari > Settings > Fradulent Website Warning
	Privacy Preserving Ad Measurement*	Safari > Settings > Privacy-preserving measurement of ad effectiveness
	Check for Apple Pay*	Safari > Settings > Privacy > Allow websites to check for Apple Pay
	Private Browsing	Safari > Tabs > Private
	Web Page Translation	Safari > Settings > Advanced > Website data > Search "translate" or "Google"
	Web Extensions*	Safari > Settings > Extensions
	iCloud Syncing*	Settings > [your name] > iCloud > Safari
	Search Engine Suggestions	Safari > Settings > Search > Safari Suggestions
	Preload Top Hit in Safari	Safari > Settings > Search > Preload Top Hit
	Siri Suggestions*	Safari > Settings > Safari Suggestions
	Clear History and Website Data	Safari > History > Clear History and Website Data
Siri	Ask Siri*	Settings > Siri & Spotlight > Listen for "Hey Siri" Settings > Accessibility > General > Type to Siri
	Integrated apps	Settings > Siri & Spotlight > [app name] > Use with Ask Siri
	Dictation	Settings > General > Keyboard > Enable Dictation
	Location Services for Siri Suggestions*	Settings > Privacy > Location Services > System Services > Location-Based Suggestions > Allowed apps
	iCloud Syncing*	Settings > [your name] > iCloud > Siri
	Location Services	Settings > Privacy > Location Privacy
	Request History	Settings > Siri & Spotlight > Siri history > Delete Siri & Dictation History
iMessage	Messages in iCloud*	Settings > Messages > iMessage
	Delete Messages	Messages > Settings > Conversation > Delete Conversation
	iCloud Backup	Messages > Settings > General > Enable Messages in iCloud
	Shared with You*	Messages > Settings > Shared with You
	Shared with Apps	Messages > Settings > Shared with You > Apps

Table 10: Privacy Configurations of default apps on macOS: Facetime, Family Sharing, Touch ID, Location and Find My and paths to disable these settings. Paths marked by (*) are provided in Apple's Privacy Policy. The remaining paths are not provided for users.

Default App	Privacy Configurations	Path to disable
Facetime	Enable Facetime*	FaceTime > Toggle FaceTime
	iCloud	Facetime > Settings > Enable this account
	Live Photos	Facetime > Settings > Allow live photos to be captured
	Speaking	Facetime > Settings > Automatic Prominence > Speaking
	Location	FaceTime > Settings > Location
	Blocked Contacts	Facetime > Settings > Blocked
Family Sharing	Family Setup	Settings > Apple ID > Family
	Apple Subscription	Settings > Apple ID > Family > Apple Subscriptions
	Ask to Buy	Settings > Apple ID > Family Sharing > Child > Ask To Buy
	Screen Time	Settings > Apple ID > Family Sharing > Screen Time
	Purchase Sharing	Settings > Apple ID > Family Sharing > Purchase Sharing
	iCloud+	Settings > Apple ID > Family Sharing > More to Share > iCloud+
Touch ID	Passcode	Settings > Touch ID and Passcode > Turn Passcode Off
	Add fingerprint (1,2,..N=5 max)	Settings > Touch ID and Passcword > Add Fingerprint
	Device Unlock	Settings > Touch ID and Password > Use Touch ID to unlock your Mac
	Autofill	Settings > Touch ID and Password > Use Touch ID for autofilling passwords
	Apple Pay	Settings > Touch ID and Password > Use Touch ID for purchases
	Password AutoFill	Settings > Touch ID and Password > Use Touch ID for Autofill
	User Switching	Settings > Touch ID and Password > Use Touch ID for user switching
Location	Enable Location*	Settings > Privacy > Location Services
	Tracking	Settings > Privacy > Location Services > Location Alerts
	Allow Apps to Track	Settings > Privacy > Tracking > Allow Apps to Request Track
	Analytics and Improvements	Settings > Privacy > Analytics and Improvements
	Apple Advertising	Settings > Privacy > Apple Advertising
	App Privacy Report	Settings > Privacy > App Privacy Report
Find My	Enable Find My*	Settings > Apple ID > Find My
	My Location	Settings > Apple ID > Find My > My Location
	Share My Location	Settings > Apple ID > Find My > Share My Location
	Family	Settings > Apple ID > Find My > Family

A.4 Appendix D: User data collected from default apps

Table 11: Users' personal data collected from default apps. Users are not able disable the collection of some of the data below for an app to function [3].

Default app	Users' personal data collected (not limited to list below)
Safari	IP address, sites you visit; open tabs, tab groups, AutoFill information, Bookmarks, Reading List and History, attribution reports, payment method information.
Siri	Contact names, nicknames and relationships, Music and Podcasts, Names of your and your Family Sharing members' devices, Accessories, Homes, Scenes and Members of Shared Home in Home app, Labels for Items (e.g., people's names in Photos and Alarms), Name of apps and shortcuts.
iMessage	Articles, TV shows, Music and Photos.
Facetime	Facetime Calls (e.g., who was invited to call, device network configurations), Apps using Facetime, Phone numbers, email addresses associated with account.
Family Sharing	Apple Watch serial number, cellular hardware identifiers, family member's health, location and contact data, view logs and screenshots from Apple Watch.
Touch ID	360-degree orientation fingerprint data, passcode.
Location	Location data, Location Search Query, Geo-tagged locations of nearby WiFi hotspots, GPS data, travel speed, barometric pressure, places you recently been, IP.
Find My	Participation in Find My network, device location, information about device, information about account.

A.5 Appendix E: Privacy configurations pathways in user interviews

Table 12: Illustrates privacy configuration pathways participants attempted to perform the tasks on default apps (Safari) on operating systems (iOS and macOS). N: number of participants out of 15 who navigated a pathway while attempting to perform the task. Most participants resorted to central OS settings to access privacy configurations related to the default apps. We observed that participants also relied on online sources (for e.g., Google) or Siri to assist with the tasks or launch the app to access its privacy settings.

Default app	Task	iOS	N	macOS	N
Safari	*Disabling data sharing*	Settings > Safari	(11/15)	System Settings	(12/15)
		Home > Launch app	(2/15)	Home > Launch app	(4/15)
		Settings > Privacy & Security Settings	(4/15)	Safari > Settings > Privacy	(5/15)
		Use online help (Google, Siri)	(6/15)	Use online help (Google, Siri)	(4/15)
		Settings > Scroll randomly till something relevant	(9/15)	System Settings > Scroll randomly till something relevant	(2/15)
		Settings > Apple ID	(11/15)	System Settings > Apple ID	(10/15)
		Settings > Control center	(1/15)	System Settings > Privacy & Security > Location Services	(1/15)
	Delete history and bookmarks	Settings > Safari	(12/15)	System Settings	(3/15)
		Home > Launch app	(3/15)	Home > Launch app	(12/15)
		Settings > Privacy & Security Settings	(2/15)	Safari > System Settings > Privacy	(2/15)
		Use online help (Google, Siri)	(1/15)	Use online help (Google, Siri)	(0/15)
		Settings > Safari > Clear history & website data	(11/15)	Safari > History > Clear history	(10/15)
		Settings > Safari > Block All Cookies	(1/15)	Safari > Bookmarks > Edit Bookmarks (delete one by one)	(3/15)
		Settings > Scroll randomly till something relevant	(2/15)	System Settings > Scroll randomly till something relevant	(0/15)
	Turn off Apple Pay	Settings > Safari	(3/15)	System Settings	(3/15)
		Settings > Apple ID	(1/15)	Home > Launch app	(3/15)
		Settings > Privacy & Security Settings	(1/15)	System Settings > Privacy & Security	(2/15)
		Use online help (Google)	(1/15)	System Settings > Wallet & Apple Pay	(3/15)

Table 13: Illustrates privacy configuration pathways participants attempted to perform the tasks on default apps (iMessage, Facetime, Siri) on operating systems (iOS and macOS). N: number of participants out of 15 who navigated a pathway while attempting to perform the task.

Default app	Task	iOS	N	macOS	N
iMessage	*Disable iMessage*	Settings > iMessage	(11/15)	System Settings	(4/15)
		Home > Launch app Try to Sign out	(1/15) (1/15)	Home > Launch app Try to Sign out	(5/15) (5/15)
		Settings > Apple ID	(2/15)	System Settings > Apple ID	(4/15)
		Settings > iMessage > Turn off iMessage	(11/15)	Messages > Settings	(2/15)
				Settings > Privacy & Security Settings	(1/15)
				Think about deleting app	(1/15)
Facetime	*Disable Facetime*	Settings	(11/15)	System Settings	(4/15)
		Home > Launch app	(0/15)	Home > Launch app	(4/15)
		Settings > Apple ID	(1/15)	System Settings > Apple ID	(2/15)
		Settings > Facetime > Turn off Facetime	(9/15)	Facetime > Turn off Facetime	(1/15)
				System Settings > Privacy & Security Setting	(1/15)
				Think about deleting app	(1/15)
Siri	*Disable Siri*	Settings > Siri	(13/15)	System Settings > Siri	(13/15)
		Siri & Search > Turn off *Hey Siri*	(6/15)	Say *Hey Siri* > Launch app	(2/15)
		Siri & Search > Turn Siri learning from each app	(7/15)	Siri & Spotlight> Turn Siri learning from each app	(2/15)
		Siri & Search > Delete Siri & Dictation history	(2/15)	Siri & Spotlight> toggle Ask Siri	(3/15)
		Siri & Search > Siri Suggestions	(2/15)	Siri & Spotlight> Siri Suggestions	(1/15)
		Siri & Search > Scroll randomly till something relevant	(2/15)	System Settings > Privacy & Security Setting	(3/15)

Table 14: Illustrates privacy configuration pathways participants attempted to perform the tasks on default apps (Location Services and Family Sharing) on operating systems (iOS and macOS). N: number of participants out of 15 who navigated a pathway while attempting to perform the task.

Default app	Task	iOS	N	macOS	N
Location Services	*Disable Location*	Settings > Location Services	(12/15)	Systems Preferences > Location	(8/15)
		Location Services > Go to each App permissions	(8/15)	Privacy & Security Settings > Location settings	(7/15)
		Location Services > Turn off Location Services	(6/15)	Location settings > Go to Each app permissions	(6/15)
		Settings > Apple ID	(2/15)	System Settings > Apple ID	(1/15)
Family Sharing	*Disable public sharing*	Settings > Apple ID	(4/15)	System Settings > Apple ID	(1/15)
		Apple ID > Family Sharing	(4/15)	Apple ID >Family Sharing	(3/15)
		Family Sharing > Turn off everything	(1/15)	Family Sharing > Turn off everything	(3/5)
				Remove family members	(1/15)
	Hide purchases	Settings > Apple ID	(3/15)	System Settings > Apple ID	(3/15))
		Apple ID > Family Sharing	(3/15)	Apple ID > Family Sharing	(3/15)
		Family Sharing > Media & Purchases	(3/15)	Family Sharing > Media & Purchases	(3/15)
	Hide location	Apple ID > Family Sharing	(4/15)	Apple ID > Family Sharing	(3/15))
		Apple ID > Family Sharing	(4/15)	Apple ID > Family Sharing	(3/15)
		Family Sharing > Find My	(4/15)	Family Sharing > Find My > Turn off Find My	(3/15))

Table 15: Number of attempts participants used to perform tasks on each operating system before giving up. Attempts are counted each time a participant would go back in the menu to a different pathway.

			Attempts			
Default app	**Task**	**OS**	**0**	**1 - 2**	**3 - 4**	**5+**
Safari	*Disabling data sharing*	iOS	(1/15)	(3/15)	(9/15)	(2/15)
		macOS	(0/15)	(8/15)	(5/15)	(2/15)
	Delete history/bookmarks	iOS	(2/15)	(12/15)	(1/15)	(0/15)
		macOS	(3/15)	(12/15)	(0/15)	(0/15)
	Turn off Apple Pay	iOS	(9/15)	(5/15)	(1/15)	(0/15)
		macOS	(10/15)	(3/15)	(2/15)	(0/15)
iMessage	*Disable iMessage*	iOS	(3/15)	(12/15)	(0/15)	(0/15)
		macOS	(4/15)	(7/15)	(4/15)	(0/15)
Facetime	*Disable Facetime*	iOS	(7/15)	(8/15)	(0/15)	(0/15)
		macOS	(7/15)	(7/15)	(1/15)	(0/15)
Siri	*Disable Siri*	iOS	(2/15)	(11/15)	(2/15)	(0/15)
		macOS	(2/15)	(12/15)	(1/15)	(0/15)
Location Services	*Disable Location*	iOS	(2/15)	(10/15)	(3/15)	(0/15)
		macOS	(3/15)	(12/15)	(0/15)	(0/15)
Family Sharing	*Disable public sharing*	iOS	(11/15)	(4/15)	(0/15)	(0/15)
		macOS	(12/15)	(3/15)	(0/15)	(0/15)
	Hide purchases	iOS	(12/15)	(3/15)	(0/15)	(0/15)
		macOS	(12/15)	(3/15)	(0/15)	(0/15)
	Hide location	iOS	(11/15)	(4/15)	(0/15)	(0/15)
		macOS	(12/15)	(3/15)	(0/15)	(0/15)

A.6 Appendix F: Cross-comparison of privacy settings in Study 1 conducted in 2020 and in 2022.

Table 16: Cross-comparison between privacy settings of default apps in Study 1 conducted in 2020 and the updated version of the Study 1 conducted in 2022. In 2020, the system evaluation was performed on iOS 14.0+ and macOS 10.15+. In 2022, the study was repeated with iOS 16.0+ and macOS 13.0+. This table presents differences that observed in the privacy configurations of the same default apps analysed in 2020.

Default app	Modifications
Safari	
iOS	*iOS 16.0+*. (1) General syntax modifications; (2) Added access routes to disable/enable privacy configurations of Safari (e.g., Hide IP Address and Fraudulent Website Warnings.)
macOS	*macOS 10.15+*. Absence of dedicated Safari privacy configuration documentation. Users may see some information in the "Search" portion of the privacy policy.
	macOS 13.0+. (1) Dedicated Safari tab now available in the privacy policy; (2) similarly to iOS 16.0+, added access routes to enable some privacy configurations.
Siri	
iOS	*iOS 16.0+*. (1) Minor addition of two data types collected in search queries: visual search and context; (2) Addition of three devices listed to contribute data to Siri: Apple Watch, HomePod or supported HomeKit accessory; (3) Added Access routes to Personalisation and apps, Learning from apps and App clips.
	macOS 13.0+. General syntax modifications.
Location	
iOS and macOS	*iOS 16.0+ and macOS 13.0+*. (1) Use of bulleted lists in the services enabled when Location is enabled; (2) Minor addition to information about users providing permission to apps or websites prior to Location Sharing.
iMessage	
iOS and macOS	*iOS 16.0+ and macOS 13.0+*. General syntax modifications.
Facetime	
iOS	*iOS 16.0+*. General syntax modifications.
macOS	*macOS 13.0+*. (1) General syntax modifications; (2) Added minor detail that SharePlay as a feature of Facetime calls.
Touch ID, Find My & Family Sharing	
iOS and macOS	*iOS 16.0+ and macOS 13.0+*. No modifications.

A.7 Appendix G: Similarities and disconnects with prior work

Table 17: We summarise the results of our work and highlight similarities and disconnects with closely related prior work on third-party apps (Frik et al. [22], Gamba et al. [23], Ramokapane et al. [43]). Our work highlights issues that may be specific to default apps unlike other studies conducted with third-party apps.

Results	Similar themes in prior work	Disconnects with prior work
Data handling practices are not disclosed	"Lengthy privacy policies" and "ambiguous outline of implications of apps" in [43].	Even if users follow provided instructions to disable data sharing, users do not receive confirmation or information about data handling practices of the vendor.
Challenges to disable apps from collecting and sharing user data	"Anticipated difficulties with configuring settings" in Frik et al. [22].	Users are not able to disable default apps from collecting and sharing their data.
Instructions to enable/disable features are missing	"Users not aware that these instructions are available or not" in Frik et al. [22].	Users are not able to find these instructions and are not easily available to users. Instruction on how data is shared in the ecosystem is missing as well.
Understanding of functionality of apps	"Usage or awareness of apps does not imply that users understand implications" and "users attribute their challenges of configuring apps to complex app requests and hidden app controls" in Ramokapane et al. [43] and "Android users are unaware of pre-installed software on Android devices and associated risks" in Gamba et al. [23].	Users confused about what happens to their information when sharing with default apps. Users also do not understand what is shared with the mobile ecosystem or what stays in the default app itself.
Awareness of tracking by apps	"Aware of privacy and security risks, but did not know how privacy settings can protect them" in Frik et al. [22].	Users were aware they were being tracked by default apps in a mobile ecosystem.
More transparency from apps	"Early display of privacy settings during setup does not equal transparency" in Ramokapane et al. [43].	Ambiguous details with regards to privacy configurations of default apps.

A.8 Appendix H: Participants details

Table 18: Results of the screening survey show participants' occupations, iPhone Model, MacBook Model and default apps used. All iPhones used in this expirement run iOS 14.0+ and all Macbooks run macOS X 10.15+. Key for the default apps (last column): 1-TouchID, 2-FindMy, 3-Siri, 4-Safari, 5-Location Services, 6-Family Sharing, 7-iMessage, 8-Facetime.

P#	Occupation	iPhone Model	Macbook Model	Default apps
P01	PhD candidate Computer Science	iPhone 6S	MacBook Pro: 2012+	1,4,7,8
P02	Software Developer	iPhone X	MacBook: 2015+	1- 5,7,8
P03	Industrial Engineering researcher	iPhone SE (2016)	MacBook Pro: 2012+	4,5,7,8
P04	GIS specialist / Msc student in forestry	iPhone 7	MacBook Pro: 2012+	1-5,7,8
P05	Educational Sciences student	iPhone SE (2020)	MacBook Air: 2012+	1,2,4,5,8
P06	UI/UX Designer, front-end web developer	iPhone 11, Pro, Pro Max	MacBook Pro: 2012+	2-8
P07	Hospitality Management student	iPhone 7	MacBook: 2015+	1-4, 6-8
P08	Architect	iPhone 7	MacBook Pro: 2012+	1-5, 7,8
P09	Economist	iPhone SE (2016)	MacBook: 2015+	1 - 4, 7
P10	Assisstant	iPhone 11, Pro, Pro Max	MacBook: 2015+	1-5, 7,8
P11	Graphic designer	iPhone XR	MacBook Air: 2012+	1,2,4,5,7
P12	Unemployed	iPhone 11, Pro, Pro Max	MacBook Air: 2012+	2 - 5,
P13	Program manager	iPhone 11, Pro, Pro Max	MacBook Pro: 2012+	1,2,4-8
P14	Labratory Technician (Sculptor)	iPhone 11, Pro, Pro Max	MacBook Pro: 2012+	1-5, 7,8
P15	Document Controller	iPhone 11, Pro, Pro Max	MacBook: 2015+	1-8