Concerned but Ineffective: User Perceptions, Methods, and Challenges when Sanitizing Old Devices for Disposal

Jason Ceci and Hassan Khan, *University of Guelph;* Urs Hengartner and Daniel Vogel, *University of Waterloo*

https://www.usenix.org/conference/soups2021/presentation/ceci

This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

Concerned but Ineffective: User Perceptions, Methods, and Challenges when Sanitizing Old Devices for Disposal

Jason Ceci, Hassan Khan
School of Computer Science
University of Guelph
{jceci, hassan.khan}@uoguelph.ca

Urs Hengartner, Daniel Vogel
Cheriton School of Computer Science
University of Waterloo
{urs.hengartner, dvogel}@uwaterloo.ca

Abstract

Consumers are upgrading their devices more often due to continuous advances in hardware. Old devices need to be sanitized (i.e., personal data removed with low recovery probability) before selling, donating, throwing away, or recycling the device (*"disposal"*), but previous works have shown that users frequently fail to do that. We aim to understand the sources of misconceptions that result in risks to personal data. Through a survey (n=131), we measure where the old devices end up and how they are sanitized. Our survey shows that while most users dispose of their devices, a large proportion of participants (73%) kept at least one old device, often due to data leakage concerns. Among disposed-of devices, 25% of participants reported using methods to erase their data that are insecure. To further explore the processes that were undertaken to sanitize devices and sources of misconception, we invite a subset of respondents (n=35) for interviews. Our interviews uncover the reasons for poor device sanitizing practices—misleading data deletion interfaces and prompts, lack of knowledge, and complex and slow disk wiping procedures. We provide suggestions for device manufacturers and retailers on how to improve privacy, trust, and convenience when sanitizing old devices.

1 Introduction

The past decade has witnessed an explosive growth of personal electronic devices [11]. Most consumers own a smartphone and computer, and many have other devices, such as tablets, cameras, flash drives, and portable hard drives, which also store personal data [4]. With rapid advancements in technology, electronic devices have a relatively short life cycle, and users often upgrade these devices. For example, the average age of smartphones traded in is 3.2 years [21]. When upgrading, consumers have several options for what to do with their old devices, including selling, recycling, donating, discarding by throwing it away, or keeping it even without using it—we refer to these collectively as *"disposal methods"*. Current estimates show that more than 206 million used smartphones were sold worldwide in 2019, and this number is expected to grow to 332 million units by 2023 [14]. Recycling is another environmentally-friendly option to dispose of electronic devices and in 2019, 17.4% of old devices were recycled worldwide [6].

Disposing of old devices introduces privacy and data security risks since these devices often contain a variety of personal data including images, videos, messages, financial information, emails, and internet and location history. For this reason, prior to disposing of a device, the device should be "sanitized," which means removing the personal data on it with a low recovery probability [22]. Previous studies have shown that users often inadvertently leave some personal data or do not sanitize their devices at all before selling them. In a seminal work, Garfinkel and Shelat explored user data removal practices by examining 159 second-hand hard drives and found that 91% contained sensitive data [9].

More recent works have shown that this state of affairs has not changed much over the past two decades for smartphones or other personal devices [7, 23]. Despite the increasing availability of full-disk encryption on some types of devices, proper sanitizing is still important since the decryption key may be derived from a weak password only [10]. Therefore, it is critical to understand why users fail to sanitize their devices to stop this dangerous practice. To the best of our knowledge, our work is the first to explore device sanitizing practices entirely from users' perspectives.

We explore users' decision-making process starting from when they no longer need a device to discover any difficulties or misconceptions they may have in regards to sanitizing

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

their devices. For a holistic exploration, we consider different device types (smartphones, computers, tablets, cameras and drives), where each type differs in the data they contain and the ways to sanitize them properly. Some devices have simple sanitizing procedures (e.g., smartphones), while others may require multiple steps (e.g., cameras). Furthermore, devices may be encrypted, which may affect a user's perception of data privacy and sanitizing methods.

To capture these aspects, we conducted a two-part study. The first part was a survey (n=131) to establish what consumers do with devices when they no longer need them, as well as if and how users remove their data from their old devices. This investigates how people prepare devices for disposal across disposal methods, which has not been investigated previously. Next, in an attempt to understand why many users fail to sanitize their devices properly, we conducted semi-structured interviews (n=35) asking users about the steps they took to sanitize their devices to identify any difficulties or misconceptions. Users were also asked to rate how likely they believed data recovery was after they sanitized the device. This provides information on consumer confidence when they sanitize their devices and helps identify misconceptions. Our work is the first to use qualitative data to uncover users' perceptions, challenges they face, and misconceptions related to sanitizing devices. Our key findings include:

- The majority of respondents (61%) chose the "Factory Reset" feature on smartphones, computers, and tablets to sanitize the device. However, they had low confidence in the security of this feature, with 57% of respondents feeling it was extremely likely that an expert attacker could recover data from their devices. Consequently, 36% of users choose to keep old devices rather than sell or recycle them.
- Unsafe sanitizing practices were common—34% of interview participants reported manually deleting all or some of the data on their devices and considered it to be a secure disk sanitizing method. Manual deletion was also error-prone. During the interview, in 9/33 cases where manual deletion had been employed, participants admitted forgetting to sanitize certain types of data.
- We use our findings to revisit the plausible reasons for poor sanitizing practices for hard drives proposed by Garfinkel and Shelat [9]. Our evidence validates some reasons, including *lack of training, tool error*, and *hardware failure*. However, we found no evidence to support *lack of knowledge* or *lack of tools* as plausible reasons.
- Our interviews uncover other plausible reasons for poor sanitizing practices, including side effects of sanitizing and the time required for sanitizing.

Finally, we provide suggestions for device manufacturers on how and when to present the right information to users for more informed sanitizing decisions. We also highlight the importance of retailers sharing their device sanitizing practices for returned devices to better safeguard users' data.

2 Background and Scope

Before disposing of personal devices, confidential data can be removed in a variety of ways depending on the device type and operating system. Garfinkel and Shelat [9] define sanitizing as removing confidential information from storage before repurposing, retiring, or disposing of electronic devices. Furthermore, confidential information should be removed using processes that result in a low probability of recovery using existing data recovery tools and techniques.

Most modern devices (with the exception of cameras and drives) have a device sanitizing function often labelled as "Factory Reset," "Erase All Content and Settings," or "Secure Wipe" [24, 25, 27]. This function is generally designed to remove all user data and applications while leaving the operating system and factory-installed applications. Apple's support website for iOS explains that deleting files makes files inaccessible but does not remove them from the device, so before selling or giving away a device, "Erase All Content and Settings" should be run [25]. Apple's iOS Security Guide further explains that the "Erase All Content and Settings" option wipes the encryption keys to the user data, leaving all personal data inaccessible. On the other hand, Android and Samsung only mention that a "Factory Reset" will remove all data [24, 26]. Windows 10 provides two "Factory Reset" options and clearly explains what each does [27]. If the user chooses the "Data Erasure" option, it removes files and cleans the drive. It suggests when to use it ("If you're planning to donate, recycle, or sell your PC, use this option") along with a rough time estimate ("This might take an hour or two") along with the advantage ("... it makes it harder for other people to recover files you've removed").

However, these sanitizing functions differ between device types, operating systems, and underlying hardware, and the desired outcome depends on the device's encryption status. This is further complicated by the lack of public information on how a device is sanitized and whether the provided "Factory Reset" function properly sanitizes the device. Shu et al. [22] showed that the "Factory Reset" function on several Android devices fails to sanitize the device. Similarly, Wei et al. [28] identified challenges when sanitizing SSDs, including the requirement of invoking the SSD controller's secure erase function. They also demonstrated that the SSD controller's built-in secure-erase command often fails to sanitize the device.

Simply deleting files, like on a smartphone, is insecure as these files can be easily recovered. Deleting files removes only the record of that file in a table, leaving files data on the drive with the potential to be fully recovered [8]. Manually deleting data prior to disposing of the device is not recommended due to the high probability of data recovery. Standard methods for

formatting drives leave data on the drive recoverable using commercially available software [8].

Given the variety of devices and the lack of publicly available information, it is challenging to identify methods that properly sanitize devices. Therefore, in our study, we refrain from commenting on whether the "Factory Reset" or format option that users employed properly sanitized the device. We instead focus on users' perceptions, practices, and misconceptions when sanitizing old devices for disposal.

3 Related Work

Prior works have investigated specific areas of data deletion and consumer data privacy on second-hand devices and in the cloud. In this section, we discuss prior works that measure device sanitizing practices in-the-wild and users' perceptions of data deletion for online services. One line of research has explored approaches to securely delete digital data given different capabilities of adversaries, as well as how secure deletion approaches can be integrated into systems at different interfaces to protect against specific adversaries [20]. However, these works are only tangentially related since we focus on users' perceptions and practices when disposing of old personal devices. Interested readers are referred to Reardon et al. [19].

3.1 Device Sanitizing In-the-Wild

Previous research into personal data on disposed-of devices has focused primarily on measuring what proportion of disposed-of devices had recoverable personal data. The seminal work in this area was the 2003 study by Garfinkel and Shelat [9], which investigated personal data on second-hand hard drives purchased mostly through online auctions. They reported recovering large amounts of sensitive information. Only 9% of the hard drives had been properly sanitized (zero-filled) with most of the remaining drives having recoverable data, including 675 Microsoft Word documents and thousands of email messages and credit card numbers.

Several recent efforts have shown that the issue that Garfinkel and Shelat [9] identified has stayed the same. In a 2014 study, researchers from Avast procured 20 Android devices from eBay and found lots of sensitive data on them including pictures (with over 1000 pictures in various states of undress), contacts, chat logs, search history, and location history, among others. In a 2019 study, Jones et al. [15] purchased 100 second-hand phones via eBay and performed forensic analysis to show that 19% of the phones contained data from previous owners. This data included private emails, intimate photos, contact lists, text messages, tax documents, bank account details, web browsing histories, and personal calendars. The same team of researchers bought 100 used memory cards and showed that 67% of the cards had personal data of the previous owners on them [3]. Researchers from Ontrack and Blancco purchased and analyzed 159 used personal devices from the United States, Britain, Germany, and Finland to discover sensitive data on 42% of devices, with 15% containing personally identifiable information [29].

Most of these studies perform analysis of used devices to determine if there is recoverable personal data on them. Only Garfinkel and Shelat propose nine plausible user-centred explanations for the widespread data leakages on disposed-of devices. These include lack of knowledge, lack of tools, lack of training, tool error, and hardware failure (see Section 7). To the best of our knowledge, our work is the first to investigate these aspects entirely from the users' perspective.

3.2 Users' Perception of Data Deletion in Online Services

While no previous work has explored data sanitizing methods for disposed-of devices, researchers have investigated data deletion and expiration aspects from users' perspectives for online services. Ramokapane et al. [18] explored users' understanding and practices of deleting data from cloud storage or services. They found that the lack of information about deletion, incomplete mental models of the cloud and deletion within it, and poorly designed user interfaces for deletion functions lead to users' failure to delete data. Murillo et al. [17] conducted a study and two focus groups to understand online user data deletion, retention, and expiration. They found that the correct understanding depended on whether users think beyond the user interface or not. Habib et al. [13] investigated the usability and interaction paths of data deletion options for 150 websites. They found that while the majority of analyzed websites offered controls, they were inconsistent across websites and sometimes rendered unusable by missing or unhelpful information. Similarly, researchers have explored data deletion and expiration aspects for online social networks, including Twitter and Facebook [1, 2].

While these works may point out issues that may be true for secure data deletion in personal devices, such as missing or unhelpful information, consumers have a lot more control over data deletion processes on personal devices than cloud environments. Therefore, a focused effort needs to be carried out to investigate these aspects for personal devices.

4 Study Design

Our survey of related works shows that device sanitizing aspects from the users' perspective have largely been unexplored. Our main objective is to understand the privacy-related sanitizing practices when users dispose of their old devices. To achieve this objective, we explore the following questions:

- What do people do with their devices when they no longer need them?

- How do people perceive threats to sensitive data on the devices that they dispose of?
- What steps, if any, do people take to remove the sensitive data on their devices before disposing of them?
- Do people trust device sanitizing methods provided by device manufacturers?
- Are people aware of, and do they understand proper device sanitizing practices when disposing of their devices?

There are several challenges to this investigation due to permutations of devices, data, and possible sanitizing methods. First, different types of devices may store different types of data. For example, a smartphone may have personal pictures, whereas a laptop may only have work-related data. Second, different devices may store personal data differently. For example, a smartphone or laptop may store data in an encrypted format, unlike a digital camera with an external storage card. Third, different devices may support different ways to sanitize the device. For example, Windows 10 provides a "Secure Erase" feature, whereas a flash drive may require a tool to zero-fill.

To overcome these challenges, we conducted a two-part study. The first part consisted of a survey, which asked respondents about their device disposal and sanitizing practices. We captured this data across participants who rated themselves at different technology proficiency levels to capture misconceptions for novice, amateur, and technology-proficient users. This enabled us to obtain quantitative data on what consumers do with their devices when they no longer need them, as well as if and how they remove their data from their old devices. To obtain qualitative data, we conducted semi-structured interviews with a subset of survey respondents. We prioritized those participants who agreed to be contacted for the interview, disposed of devices across multiple device types, and represented a reasonable diversity of technology proficiency. The interviews enabled us to explore why many people fail to properly sanitize their devices before disposing of them.

In the following sections, we report the recruitment process, study procedure, and results separately for the online survey and semi-structured interview. Note that we received approval from our IRB for this study.

5 Online Survey

The goals of the survey are to understand how users dispose of their devices and what steps they take to sanitize their device. We limited electronic devices to smartphones, laptop and desktop computers, tablets, digital cameras, memory cards, hard drives, and flash drives as these devices are more likely to contain sensitive data.

5.1 Recruitment and Procedure

For the online survey, we recruited respondents by placing advertisements on Facebook marketplace, Kijiji (the Canadian equivalent of Craigslist), local subreddits, and through word-of-mouth (see advertisement text in Appendix A.1). The inclusion criteria were that the respondents should have recently listed an item for sale on an online buying and selling marketplace. Participants responded to the survey on Qualtrics (see Appendix A.2). The survey collected data from respondents for the following data categories: (a) Demographics and background; (b) Disposal methods and reasons for not disposing of; (c) Sanitizing methods; and (d) Sanitizing perceptions.

At the end of the survey, respondents were asked if they wish to be contacted for a follow-up interview. For the 10-minute online survey, participants were paid $2.

Table 1: Survey Demographics (*UD = Undisclosed)

n = 131							
Gender							
Woman	*Man*	*Other*	*UD*				
68	57	2	4				
Age (in years)							
18–25	*26–30*	*31–35*	*36–40*	*41–45*	*46–50*	*50+*	*UD*
38	27	20	14	15	7	6	4
Self Reported Proficiency in Technology							
Basic	*Intermediate*	*Advanced*	*UD*				
8	86	34	3				

5.2 Results

For test statistics on quantitative data, Pearson's Chi-Squared test was used to compare categorical data, a Kruskal-Wallis one-way analysis of variance was used to compare Likert scale responses between respondent technology proficiency levels, and Wilcoxon Signed-Ranks test to compare Likert scale responses between questions.

5.2.1 Demographics and Background

Respondents were asked about their age, gender, and their level of technology proficiency. The survey was completed by 131 participants. Their demographics are summarized in Table 1. It shows reasonable diversity among respondents in terms of gender. In terms of age, while almost half of the respondents (65/131) are 30 years of age or younger, we have a good representation from other age groups as well. Fewer respondents self-reported a basic proficiency in technology as compared to those who self-reported as intermediate or advanced. This smaller proportion is somewhat expected due to the study being advertised and conducted online and respondents possibly over-reporting their technology proficiency.

5.2.2 Disposal Methods

We asked respondents what they did with electronic devices they no longer used including smartphones, computers, tablets,

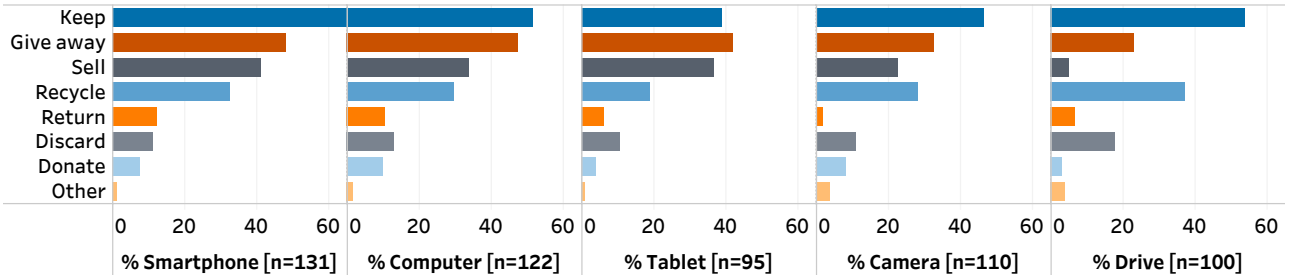


Figure 1: Response of participant ('n') to "What do you do with electronic devices you no longer use? (Choose all that apply)"

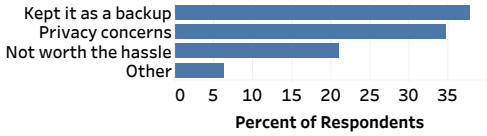


Figure 2: Respondents' responses to "What was the main reason you kept an old electronic device?"

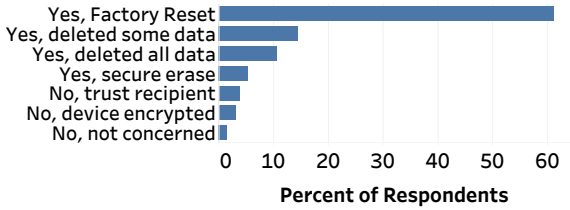


Figure 3: Respondents' responses to "Did you remove any personal data on your old device before selling, giving away, recycling, donating, or returning it?"

digital cameras, hard drives and flash drives (see Figure 1). Keeping the device was the most reported action for all device types (except for tablets), with 73% of respondents keeping at least one device. Giving the device to a friend or family member was the second most reported way to dispose of smartphones, computers, and cameras/memory cards. Giving the device to a friend or family member was the most reported action for tablets and the third-most reported for drives (we use the term "drives" to refer to hard drives and flash drives). Selling and recycling old devices was a common action for all device types, and respondents reported selling more smartphones, computers and tablets than recycling. For cameras and drives, respondents reported recycling more than selling. For each device type, at least ten respondents reported throwing out a device. While some respondents reported returning their smartphones and computers to a provider or IT department, understandably, this action was rare for cameras and drives. The "other" responses were codified, and all responses referred to some way of destroying the device or its storage medium.

Of the 95 respondents who reported keeping an old electronic device, 38% (36/95) reported keeping it as a backup, 35% (33/95) kept it due to privacy concerns, and 21% (20/95) kept it mainly because it was not worth the hassle to sell, donate or recycle (see Figure 2).

5.2.3 Sanitizing Methods

Respondents were asked if they removed their personal data from the last device they sold, donated, recycled, or returned. We only focused on the last device to simplify the survey and maintain reasonable time constraints. If they did attempt to remove any personal data from the device, they were asked to select the method they used and whether all or only some personal data was removed (see Figure 3). 25% (33/131) used a method that is known to be insecure, such as manually deleting some or all data on the last device they sold, donated, recycled, or returned. Few respondents (11/131) chose not to try to remove their personal data. 62% (80/131) of respondents reported that they used a built-in "Factory Reset" function. Seven respondents used a tool or utility to zero-fill or secure erase the data storage. A Chi-squared test found no significant effect for technical proficiency (basic, intermediate and advanced) and whether they chose to use a secure ("Factory Reset", zero-fill or secure erase) sanitizing method or chose to manually delete data ($\chi^2(2) = 1.00, p = 0.61$).

5.2.4 Sanitizing Perceptions

Respondents were asked how concerned they would be if an untrusted individual was able to access their data on an old device on a 5-point Likert scale. Most respondents reported that they were "most concerned" (60% (78/131)) or "concerned" (24% (32/131)) about their data being accessed while (13%) 17/131 were "somewhat concerned", (2%) 3/131 were slightly concerned, and only (1%) 1/131 was least concerned. A Kruskal-Wallis test examined the effect of respondent technical proficiency on the reported level of concern and found no significant differences ($H(2) = 1.33, p = 0.51$).

Respondents were asked how likely they felt it would be for two theoretical attackers, one with average and one with expert computer skills, to recover any data from their device after their chosen sanitizing method. On a 7-point Likert scale,

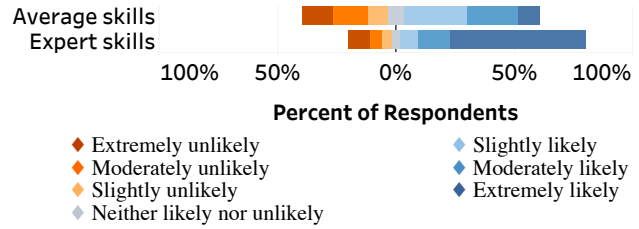


Figure 4: Respondents' responses to "How likely do you believe it would be for a person to be able to recover any personal data from the last device you sold, donated, recycled or returned?"

(57%) 75/131 of respondents felt it was at least slightly likely that an attacker with average computer skills could recover their personal data (see Figure 4). With an expert attacker, (57%) 75/131 respondents felt it was extremely likely that the attacker could recover their personal data. A Wilcoxon Signed-Ranks test indicated that likelihood ratings for an expert attacker were significantly higher than the likelihood ratings for an average attacker ($Z = 8.31, p < 0.001$).

6 Semi-Structured Interview

The goal of the semi-structured interview was to explore why users fail to sanitize their devices properly. All interview participants had already completed the survey, and the interview was treated as an extension to the survey.

6.1 Participants

Respondents who expressed their interest in participating in the follow-up interview and met the inclusion criteria (i.e., had disposed a device across two or more device categories and were interested in a follow-up) were invited to participate. 66 survey respondents met the inclusion criteria and were contacted over email to participate in the interviews (of which two declined, and 29 did not respond).

6.2 Procedure

Due to the pandemic, the interviews were conducted online (using Google Hangouts or Skype). We chose a platform that supported video and screen sharing as it allowed us to share screenshots of common device sanitizing interfaces (more details to follow). We performed audio recording if the participant consented. Otherwise, the researcher took notes. For participating in the interview, participants were paid $20. The interview questions were broadly categorized into the following categories and required both categorical and free form responses (also see questions in Appendix A.3):

- **Demographic and background:** We sought further demographic information and general questions about their electronic devices and the data stored on them.
- **Sanitizing methods:** We asked participants if and how they removed their personal data before the following (when applicable): giving away the device to a friend or family member, selling the device, donating the device, recycling the device and returning the device to a provider, manufacturer, workplace or IT department.
- **Sanitizing non-functioning devices:** We asked participants what they do with the devices that they no longer use that are broken or defective. If they sold, donated, recycled, or threw away the device, they were asked if they attempted to remove any personal data and how.
- **Finding data:** Participants were asked if they ever found another person's data on a device they had purchased.
- **Challenges and misconceptions in device sanitizing:** We asked participants how difficult they think it is to fully remove all data from the different device types included in the study. We also explored the information presented to them when they were using "Factory Reset" or wipe procedures offered to them by the device manufacturer. To refresh their memory, we showed them possible user interfaces (specific to their device/OS) that are presented to the user when they are factory resetting their device. We collected these user interfaces for all common platforms, and they included Disk Format across common platforms (Windows, Mac, Linux) and "Factory Reset" interfaces for Windows, iOS, and Android.
- **Responsibilities:** Finally, we asked participants about the level of responsibility they feel online marketplaces, device manufacturers, and consumers themselves should have when it comes to practices around device sanitizing.

Table 2: Interview Participant Demographics (*UD = Undisclosed)

n = 35							
Gender							
Woman		*Man*		*Other*		*UD*	
20		14		0		1	
Age (in years)							
18–25	*26–30*	*31–35*	*36–40*	*41–45*	*46–50*	*50+*	*UD*
10	9	4	4	3	4	1	0
Annual Household Income (× $1000)							
<$30		*$30–74*		*$75–99*		*>$100*	*UD**
5		14		6		8	2
Highest Education Level							
High School		*Undergraduate*		*Graduate*			
10		20		5			
Self-Reported Proficiency in Technology							
Basic		*Intermediate*		*Advanced*			
4		29		2			

6.3 Results

For qualitative analysis, two researchers independently performed open coding to identify codes or themes in participant responses to free-response questions (Q9, 14, 16, 20, 22 in Appendix A.3). Identified codes were compared and discussed by reviewers until consensus was reached. For the qualitative data from interviews, we report quotes from participants when they represent a theme. In this case, we identify the number of participants who expressed that theme and provide a representative quote. When reporting quotes from participants, the participant number corresponds to the respondent number in the survey.

Table 2 summarizes the demographic information for participants of the semi-structured interviews. Additionally, annual household income levels and highest education level achieved are reported for the interview participants. Overall, our participant pool has good diversity for these demographics, which is important for our investigation.

6.3.1 Sanitizing Methods when Giving Away

Participants were asked if and how they sanitized devices that they gave to a friend or family member. 60% (12/21) reported using a built-in "Factory Reset" option citing its ease, speed, security, and availability. 24% (5/21) manually deleted all personal data and stated that they deleted their contacts, text messages and photos. When asked about certain types of data, 3/5 indicated that they forgot to remove their browsing history, saved passwords, or saved passwords.

> *"I just deleted everything I could find on the phone like apps, contacts, photos and videos. I didn't think about any website passwords or browsing history."* (P89)

For the giving away computers case, 47% (7/15) reported manually deleting data. 5/7 chose this method because it was the only method they knew. 2/7 had the knowledge of more secure methods but did not employ them because they trusted the recipient. Due to trust, 2/15 and 2/15 participants reported only deleting some personal data and no data, respectively. 20% (3/15) participants used the Windows "Reset My PC" function. The last participant manually deleted personal data before wiping the free space with a commercial tool.

When giving away tablets, one participant did a "Factory Reset" while one did not remove any data due to trust in the recipient. For digital cameras, 2/4 formatted the memory card using the camera's user interface, 1/4 used the "Select All" and delete option in the camera, and 1/4 did not remove anything due to trust in the recipient. For drives, 1/4 participants manually deleted data, 1/4 participants formatted the drive, and 2/4 participants did not remove any data due to trust.

6.3.2 Sanitizing Methods when Selling

We asked participants how they sanitized devices prior to selling them (see Figure 5). For smartphones, 93% (14/15) reported using "Factory Reset". However, 53% (8/15) reported manually deleting all personal data before selling computers. 5/15 who reported using a manual delete method did so as they did not know of a better method.

> *"I backed up files and then deleted them to the recycle bin. I didn't know there was anything else to it. I couldn't take the hard drive out because then the laptop won't work."* (P63)

3/15 computer owners considered more secure sanitizing methods but ultimately chose to delete their data as more secure methods were too technical or too slow.

> [On selling their Windows 7 laptop] *"I just deleted all my documents and photos. I couldn't find a factory reset button, so I googled it but wiping it was complicated to do."* (P36)

Only four participants reported selling their tablets —two used a "Factory Reset" option, one deleted some personal data manually, and one participant did not delete anything as they were not concerned about their personal data. With digital cameras, two participants deleted all photos manually, and two participants sold the camera without a memory card. No participants reported selling drives.

Participants were asked on a 7-point Likert scale how likely they felt it would be for two theoretical attackers, one with average and one with expert computer skills, to recover any data from the different device types that they sold (see Figure 6a and Figure 6b, respectively). Note that, to avoid priming the participants, we chose not to define the "average" and "expert" attackers. While participants may attribute impossible abilities to the expert attacker, this question was intended to gauge the confidence of participants in the security of their chosen sanitizing method. For smartphones, when participants were asked about an average attacker, 50% (8/16) participants reported a successful attack to be slightly or extremely unlikely, whereas the remaining participants reported it to be at least slightly likely. For an attacker with expert computer skills, 37% (6/16) participants felt it was "extremely likely" that they could recover data.

More than half of the participants felt data recovery was likely on computers by both types of attackers (75% (12/16) perceived likelihood of an expert attacker recovering data was at least slightly likely). For cameras, the likelihood of data recovery was reported as "extremely unlikely" or "moderately unlikely."

6.3.3 Sanitizing Methods when Recycling or Donating

Participants were asked if and how they sanitized devices that they had donated or recycled in the past. Participants reported donating 23 devices in total and at least one device for each device type. Participants reported using a "Factory Reset" method on 58% (7/12) smartphones, 1/5 computers, and 1/2 tablets before disposal. 2/5 participants reported removing the hard drive of a computer before donating, and one participant

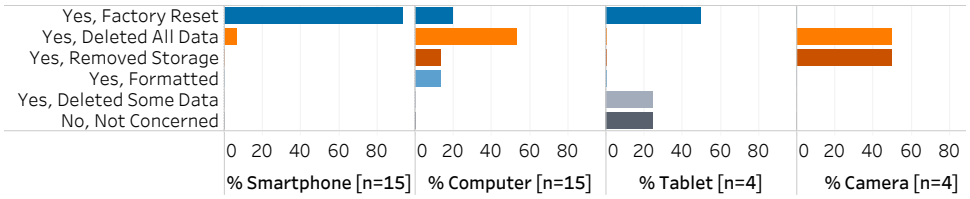
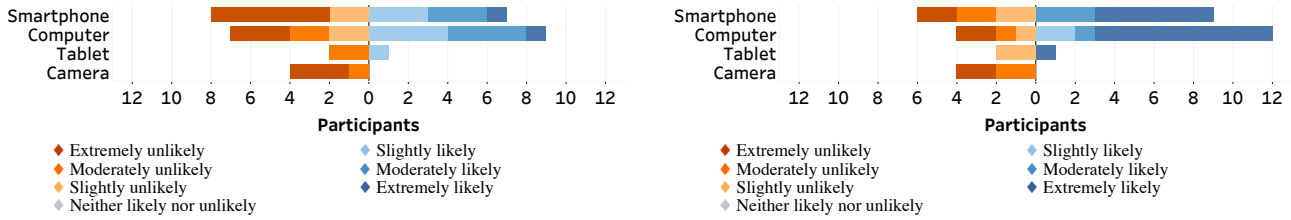


Figure 5: Participants' responses to "Did you remove any data from the device before selling it?"



(a) Average attacker.

(b) Expert attacker.

Figure 6: Participants' responses to "How likely do you believe it would be for a person with (a) average or (b) expert computer skills to be able to recover any personal data from the last device you sold?"

reported reinstalling the OS of the tablet before donating. The rest of the participants either reported using unsafe methods or were not concerned about threats to personal data. For a detailed breakdown, see Figure 9 in Appendix A.4.

Unlike when selling, giving away or returning a device, the device does not have to be functional when donating or recycling the device. Four participants, two with smartphones and two with digital cameras, reported not removing any data from their devices prior to donating or recycling them.

> *"The battery was dead, and I didn't have the charger, so I just donated it as is"* (P15)

We further explore users' sanitizing behaviours with non-functioning devices in Section 6.3.5.

6.3.4 Sanitizing Methods when Returning

We explored sanitizing practices for devices that are returned to a service provider, IT department, manufacturer, or retailer. For smartphones, 3/10 participants reported using a "Factory Reset" while 1/10 reported wiping the device in the recovery mode. 3/10 reported manually deleting some or all data. 3/10 also reported not removing any data because either they felt that it did not have personal data on it or they believed the store would sanitize the device.

> *"I returned my iPhone to the store to upgrade to a new model, like a trade-in. They said they wipe them, so I just gave it to them without doing anything."* (P67)

Seven participants returned computers to IT departments or retailers. 5/7 reported not removing any data because removal was too inconvenient, and they hoped that the retailer would sanitize the device before reselling them.

> *[On returning their laptop to the retailer] "I was going to remove some data, but it got way too inconvenient to try and delete everything before returning it for a trade-in. I think they delete everything there."* (P90)

2/7 reported removing all their personal data manually. When asked about how they manually removed all their personal data, one participant responded:

> *"I made a new user account and removed the old one in the control panel. I had to leave the laptop after an internship, but I had put a lot of my personal stuff on it, and it was linked to my phone."* (P21)

This method of removing personal data was a unique one in this study. For a detailed breakdown, see Figure 10 in Appendix A.4.

6.3.5 Sanitizing Methods for Non-Functioning Devices

Participants were asked how they disposed of and sanitized non-functional devices. We defined non-functional devices as devices that were broken, damaged, or defective in a way that impacted the usage of the device, including damaged screens, defects in data storage, battery or input, and devices that would not power on. Participants' responses are summarized in Figure 7. Across all device types, the majority of the participants chose to keep their non-functional devices. Less popular choices included throwing away the device, selling the device or destroying the device. Of participants that chose to keep non-functioning devices, 60% kept them out of concern for their personal data.

> *"I kept my broken tablet because I had my kid's pictures on it. I kept it for privacy reasons."* (P30)

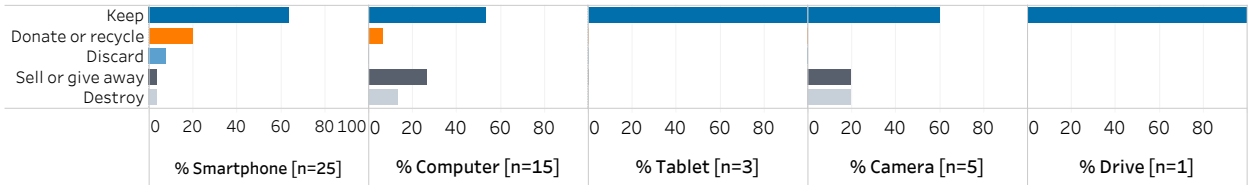


Figure 7: Participants' responses to "What do you do with non-functioning (broken) devices that you no longer use?"

For some participants, keeping non-functioning devices became impractical due to the space used, resulting in the devices being recycled without any sanitizing and with the potential for a personal data breach.

> *"My wife wanted me to get rid of our pile of old smartphones, so I just threw them all out. They wouldn't turn on anyway; the batteries were dead. I have no idea what was left on them; some are my daughter's and son's phones, so I don't know."* (P129)

Participants that had disposed of a non-functioning device were asked if they attempted to sanitize the device first. For smartphones, 4/9 participants attempted to remove data, while only 2/7 participants attempted to remove data from their broken smartphone prior to disposing of it. For a detailed breakdown, see Figure 11 in Appendix A.4.

6.3.6 Data Left on Resold Devices

We ask participants if they had ever bought a device that had the personal data of the previous owner on it. 12 participants (34%) reported finding the previous owner's personal data on a device that they purchased. Personal data that was reported to be found included photos, documents, and application login credentials. These findings validate previous reports of a major retailer selling a refurbished laptop with the previous owner's personal data [5]. 4/12 participants reported purchasing these devices from major electronics retailers.

> *"I had bought an open box laptop from [a major retailer] that had a lot of someone's files like photos and documents. Their OneDrive account was also logged in on the laptop."* (P67)

6.3.7 Participant Views on Device Sanitizing

To further understand participants' perception of the device sanitizing process, we asked them the level of difficulty ("Easy", "Intermediate", "Difficult/Impossible") they faced when they sanitized a device in the past for all the device types that they sanitized in the past (see Figure 8). For smartphones, 43% (15/35) participants felt it was "Easy", 46% (16/35) felt it was "Intermediate" and 11% (4/35) felt it was "Difficult/Impossible" to securely remove all data. For tablets,

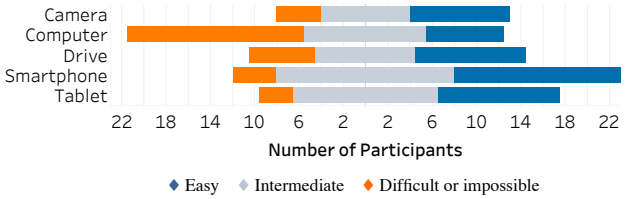


Figure 8: Participants' responses to "How difficult do you believe it is to securely remove all data from these devices?"

participants' responses were similar to those for smartphones. For computers, only 20% (7/35) found it "Easy," 31% (11/35) found it "Intermediate," and 49% (17/35) found it "Difficult/Impossible. For digital cameras and drives, 43% (9/21) and 40% (10/25) participants felt it was easy to securely remove all personal data, respectively. However, no participant previously reported using a secure sanitizing method (excluding participants that removed the memory card). This indicates that secure sanitizing procedures are not widely known for digital cameras and drives, and as a result, users falsely believe that manually deleting all data is adequate for sanitizing.

To assess the impact of usable device sanitizing methods, we asked participants if the difficulty to securely remove data has ever made them reluctant to sell or donate a device. 74% (26/35) participants answered "yes," and 26% (9/35) answered "no." 57% (20/35) strongly agreed that they would be more likely to purchase a device that they knew had a feature to securely remove all personal data, compared to one that did not. Finally, to determine the impact of a secure data removal feature on the future sale of a used device, participants were asked if they would be more likely to sell a device if it had a feature to securely remove all personal data. 77% (27/35) strongly agreed, and 14% (5/35) somewhat agreed.

Participants were asked whether the information conveyed by the "Factory Reset" feature assisted them when they were selling their device. Only 7/30 and 3/23 participants agreed that it assisted them when selling their smartphones or computers, respectively. For a detailed breakdown, see Figure 12 in Appendix A.4. Participants were asked to determine where the responsibility lay for their data privacy when selling devices. 94% (33/35) somewhat or strongly agreed that online marketplaces should explain the risks associated with selling used devices and how to securely sanitize used devices. 80%

(28/35) strongly believed that device manufacturers should make it easier to securely remove all personal data.

7 Discussion

We summarize and apply our results in two ways. First, we revisit the reasons for poor sanitizing practices among users hypothesized by Garfinkel and Shelat [9] in light of our findings. Second, we report new reasons for poor device sanitizing. Finally, we provide suggestions for improvement.

7.1 Revisiting Garfinkel and Shelat

Garfinkel and Shelat propose nine possible reasons why users frequently fail to sanitize their disk drives. While we cover devices of different types, their possible reasons may be applicable in a broader sense given the nature of storage mediums. We use the qualitative and quantitative findings from our study to validate their explanations (quoted verbatim in headings and italics).

Lack of knowledge. *("The individual simply fails to consider the problem.")* We find no evidence to support lack of knowledge as a source of poor device sanitizing practices. While participants displayed a *lack of concern* and *lack of training or incompetence*, all participants appeared to understand the problem well. It is plausible that awareness of the problem has increased due to media coverage or the overall improvement in the technology proficiency of the population.

Lack of concern for the problem. *("The individual considers the problem, but does not think the device actually contains confidential information.")* We find some evidence for this: 2% (3/131) survey respondents reported not removing data from the last device that they disposed of (to untrusted recipients) because they were not concerned. Interview participants were asked this question for each device type, and nine participants reported disposing of a device without removing data for at least one device type because they were not concerned. The codified responses indicate that 3/9 participants did so because they did not consider data to be sensitive, for example:

> *"I bought a new laptop but it broke and I had to return it for a new one. I only had it for a few weeks so I wasn't concerned"* (P60)

Lack of concern for the data:. *("The individual is aware of the problem—that the drive might contain confidential information—but doesn't care if the data is revealed.")* During the survey, no participant answered "least concerned" if an untrusted individual was able to retrieve data off of their devices and only 3% answered "slightly concerned." The rest (97%) answered "moderately" to "very concerned." However, the interview responses of participants who disposed of a device because they were not concerned, suggest otherwise. 3/9 participants indicated that they did so because of the lack of concern for data. Their responses were similar to:

> *"I was not concerned with the info on this phone, I just used it for calls, emails and texts, what would anyone do with that? "* (P129)

Failure to properly estimate the risk. *("The individual is aware of the problem, but doesn't believe that the device's future owner will reveal the information")* 3/9 interview participants who did not sanitize their device reported not being concerned partially due to the hope that the future owner will sanitize it and not reveal their information. Their responses were similar to:

> *"I only used it for web browsing and email so I didn't care about erasing it. I think the person who bought it will reset it."* (P23)

Seven participants also reported that they relied on retailers to sanitize their returned devices. This choice is also influenced by other factors, such as the amount of effort required to sanitize. Their comments were similar to:

> *"I was going to remove some data but it got way too inconvenient to try and delete everything before returning it for a trade-in. I think they delete everything there."* (P90)

Despair. *("The individual is aware of the problem, but doesn't think it can be solved.")* The majority of survey participants (60%) believed that a person with average computer skills would be able to retrieve data from a sanitized device. Despite the belief that sanitizing methods were imperfect, participants still sanitized their devices. During the interview, we asked participants how difficult they believe it was to fully remove all personal data from devices ("Easy," "Intermediate," "Difficult/Impossible"). While 4/35, 4/35, and 3/35 participants reported it to be "Difficult/Impossible" for smartphones, cameras, and drives, respectively, 20 participants reported it to be "Difficult/Impossible" for computers. This despair may be driven by a lack of training.

Lack of tools. *("The individual is aware of the problem, but doesn't have the tools to properly sanitize the device.")* Since Garfinkel and Shelat's work, free disk sanitizing tools have become widely available. However, these tools may not be readily accessible to the users and resources and information about these tools may be difficult to comprehend by non-expert users. These aspects are more related to the training or competence of the users and are discussed below.

Lack of training or incompetence. *("The individual attempts to sanitize the device, but the attempts are ineffectual.")* Even though deleting data does not sanitize disks, 25% of survey respondents deleted some or all data from their devices before disposal. 34% of interview participants made the same mistake and trusted this unsafe method for device sanitizing. During interviews, five participants reported that deleting files was the only sanitizing method known to them. Even with the knowledge that manual data deletion may not be the best option, one participant reported using it due to their inability to make a more secure method work:

[On selling their Windows 7 laptop] *"I just deleted all my documents and photos. I couldn't find a factory reset button so I Googled it but wiping it was complicated to do"* (P36)

Tool error. *("The individual uses a tool, but it doesn't behave as advertised.")* The wide use of manual delete coupled with the misunderstanding of participants that it is a secure device sanitizing choice is due to tool error. Four participants even reported using manual delete specifically because they believed it was secure. The prompt shown to users when emptying the "recycle bin" on Microsoft Windows reads: "Are you sure you want to *permanently* delete all of these items?"(emphasis ours). This seemed to be a source of confusion for several participants.

"It said it would be permanently deleted if I emptied the recycle bin" (P104)

Garfinkel and Shelat make this observation as well, noting that users falsely believed the format command removed all data from the drive because of the warning that "ALL DATA ON NON-REMOVABLE DISK DRIVE C: WILL BE LOST".

Hardware failure. *("...a computer failure might make it seem that the hard drive has also failed, when in fact it has not")* Six interview participants reported disposing of devices that no longer function without attempting to sanitizing them. However, these participants acknowledged that the device may still contain data, but believed it would be unlikely for someone to recover the data on a broken device with comments like:

"I had a laptop with a broken trackpad. I recycled it at [Major Retailer]. It was too hard for me to delete anything with the keyboard and the battery was dead so I just recycled it without the charger hoping it wouldn't be recovered." (P68)

7.2 Barriers to Secure Sanitizing

Our study shows that the majority of Garfinkel and Shelat's plausible explanations contribute to poor device sanitizing practices. We also note the following contributing factors.

Side effects of sanitizing. During interviews, 2/35 participants complained that if they were to use an existing tool to secure erase their computer, they would be left with an unbootable computer that would be difficult to sell. Reinstalling the operating system and drivers is outside the expertise of most users. Additionally, most computers now ship without the operating system installation disks and instead rely on recovery partitions on the computer's hard drive. Using disk wiping software would effectively erase this partition requiring the creation of installation media on another computer (which the user may not have access to) [12]. For example:

"There is a wipe software called DBAN my IT friend said to use but if I use that the computer won't boot anymore because Windows will be wiped out. I wouldn't have sold it if it didn't work."(P19)

Removing the storage media before disposing of the device is a secure method. However, three participants reported issues selling or donating without the storage media, such as the device no longer being operational or having less resale value. One participant commented:

"I used the delete all button on a Canon camera before donating. I donated it with my memory card so someone could actually use it."(P109)

Slow sanitizing process. Secure erase requires zero-filling storage media (the process for SSDs is more complicated and involved (see Wei et al. [28]). Five interview participants choose to use a less secure sanitizing method because a more secure one would take too long. For example:

"It takes way too long to delete everything, even removing programs took forever so I deleted the "My Documents" folder then gave it away." (P68)

Missed data. While manually deleting data is not a secure erase method, it provides some protection against new owners who are not actively looking for data remnants. During the interviews, participants who manually deleted data were asked about their deletion process and how they deleted certain types of data. Their responses indicate that while they deleted their personal data, they often forgot about data saved in applications such as browsing history, saved passwords in the browser's password manager, and application credentials. This oversight was reported by seven participants.

7.3 Improving Device Sanitizing Practices

When discussing potential improvements, we focus on widely used device types and platforms, specifically: Windows and macOS for computers and Android and iOS for smartphones. We discuss potential ways device manufacturers, retailers, and used marketplaces can help improve sanitizing practices.

Device Manufacturers. Device manufacturers can influence poor sanitizing practices that are due to the lack of training or incompetence and tool errors. When emptying the "recycle bin" or formatting the drive on Windows 10, users are informed that the "data will be permanently deleted." iOS (v14.4) and Android (v10) provide similar messages ("This photo will be deleted. This action cannot be undone." and "Permanently delete 1 image?", respectively). These messages warn users so they do not accidentally delete data making it (possibly) non-recoverable. However, such prompts create confusion from a sanitizing perspective. Apple's support website provides a more informed message saying: "...deleting files makes files inaccessible but does not remove them from the device" [25]. A message that warns users about their data being inaccessible without creating confusion regarding

device sanitizing is much needed. However, more exploration is needed to ensure that such a message is appropriate for users with different technology proficiency levels.

The message provided on Apple's support website is informative, but it is not presented to users at the *right* moment. This message needs to be presented to users when they empty the "recycle bin" or format devices or operating systems. Perhaps AI tools could be used to address this gap by detecting patterns of deletion that characterize device sanitizing and suggesting secure erase methods. Another possibility is to remind users to sanitize their devices when they unlink accounts from a device, as this is often done before disposal.

Finally, the information provided for the "Factory Reset" method needs reconsideration. During interviews, only 7/30 and 3/23 participants agreed that the information provided by the "Factory Reset" method assisted them when selling their smartphones or computers, respectively. The support websites of Android and Samsung only mention that a "Factory Reset" will remove all data without providing further details [24, 26]. Apple's iOS support page provides more details about the secure erase of the decryption key. The "Reset Device" interface of Windows 10 provides an elegant solution. The user is presented with two options—"Data Erasure on" or "Data Erasure off". Between them, it clearly explains the purpose (device reset due to issues vs. preparing to sell) and advantages (fast vs. making data recovery difficult) of each. Such options may help users make more informed choices.

Retailers and Used Marketplaces. During the interviews, several users said that they relied on the retailers to sanitize their used devices after they returned or exchanged them. However, the policies and procedures adopted by retailers to sanitize the device are not communicated to people and are imperfect [5]. When accepting used devices, retailers should provide information regarding how devices will be sanitized, potentially informing about the data erasure standard that will be followed (e.g., NIST 800-88 [16]).

Participants were asked to determine where the responsibility lay for their data privacy when selling devices. 94% (33/35) somewhat or strongly agreed that online marketplaces should explain the risks associated with selling used devices and how to sanitize used devices. While arguably these marketplaces have an ethical responsibility to inform the sellers about potential risks and ways to sanitize their devices, the economics of this action needs more investigation. On the one hand, transparency about such risks may stop sellers from selling their devices and on the other hand, with the availability of information on how to sanitize the devices, more people may be willing to sell their used devices.

8 Limitations

This study has several reasonable limitations intrinsic to studies on human participants. First, it relies heavily on self-reported information, which may be limited by the participants' memory or subjective views. Second, participants may be inclined to provide biased responses to avoid embarrassment or to provide what they feel are favourable responses. Furthermore, due to the pandemic, advertising for and participation in the study was exclusively online. This may have reduced the number of older participants or participants with basic technology proficiency. As these limitations are not easily preventable, we focus on limitations specific to this study.

During the study, there was a gap of up to a month between the survey and the interview for some participants. This gap was introduced since we waited for all surveys to be completed before the interview. During this gap, participants may have changed their device sanitizing methods. However, as the majority of the devices discussed in the interviews were sold before the survey, this gap is unlikely to have a significant impact on our findings. Furthermore, participants reported their disposal methods and experiences that happened several months ago. Their recall of the disposal methods may not have been accurate. While we presented them with "factory reset" interfaces for specific platforms (if needed), they likely experienced an interface with some variation. Finally, the behaviour of some participants may be influenced by the presence of device encryption, but we did not explore this. Exploring how device encryption changes users' behaviour is a possible future work.

9 Conclusion

We conducted a survey with 131 participants and a semi-structured interview to understand why users adopt unsafe practices when disposing of their old devices. Our investigation provides evidence that the unsafe practices are due to the lack of knowledge, misleading prompts and descriptions provided by device manufacturers, time constraints, possible side effects of sanitizing, and the delegation of sanitizing to retailers without a clearly defined policy from them. Our study provides little or no evidence for some of the previously suggested reasons for improper device sanitizing practices. Finally, we suggest possible improvements in user prompts and descriptions that can be adopted by the device manufacturers to mitigate the misconceptions of users. With the more frequent disposal of devices containing personal data, our findings will help researchers, device manufacturers, and retailers improve device sanitizing practices for consumers.

Acknowledgements

This material is based upon work supported by NSERC under Grant No. RGPIN-2019-05120. We thank Jonah Stegman for his feedback on the survey and assistance.

References

[1] Hazim Almuhimedi, Shomir Wilson, Bin Liu, Norman Sadeh, and Alessandro Acquisti. Tweets are forever: A large-scale quantitative analysis of deleted tweets. In *2013 Conference on Computer Supported Cooperative Work*, pages 897–908, 2013.

[2] Lujo Bauer, Lorrie Faith Cranor, Saranga Komanduri, Michelle L Mazurek, Michael K Reiter, Manya Sleeper, and Blase Ur. The post anachronism: The temporal dimension of Facebook privacy. In *12th ACM Workshop on Privacy in the Electronic Society*, pages 1–12, 2013.

[3] Paul Bischoff. Two-thirds of secondhand USB drives still contain previous owners' data: study. https://www.comparitech.com/blog/information-security/secondhand-usb-drive-memory-stick-study/, March 2019. Last accessed: 02/2021.

[4] Pew Research Center. Demographics of mobile device ownership and adoption in the United States. https://www.pewresearch.org/internet/fact-sheet/mobile/, Jun 2020. Last accessed 02, 2021.

[5] John Ferguson. How Best Buy's computer-wiping error turned me into an amateur blackhat. https://arstechnica.com/information-technology/2015/06/how-best-buys-computer-wiping-error-turned-me-into-an-amateur-blackhat/, Jun 2015. Last accessed 02, 2021.

[6] Vanessa Forti, Cornelis Peter Balde, Ruediger Kuehr, and Garam Bel. The global e-waste monitor 2020: Quantities, flows and the circular economy potential. http://ewastemonitor.info/wp-content/uploads/2020/12/GEM_2020_def_dec_2020-1.pdf, 2020. Last accessed 02, 2021.

[7] Josh Frantz. Exfiltrating remaining private information from donated devices. https://blog.rapid7.com/2019/03/19/buy-one-device-get-data-free-private-information-remains-on-donated-devices/, Aug 2019. Last accessed 02, 2021.

[8] Simson L. Garfinkel. Carving contiguous and fragmented files with fast object validation. *Digital Investigation*, 4:2–12, 2007.

[9] Simson L. Garfinkel and Abhi Shelat. Remembrance of data passed: a study of disk sanitization practices. *IEEE Security & Privacy*, 1(1):17–27, 2003.

[10] Johannes Götzfried and Tilo Müller. Mutual authentication and trust bootstrapping towards secure disk encryption. *ACM Transactions on Information and System Security (TISSEC)*, 17(2):1–23, 2014.

[11] Grand View Research. Consumer Electronics Market Report for Personal Electronics Industry. https://www.grandviewresearch.com/industry-analysis/personal-consumer-electronics-market, 2020. Last accessed June, 2020.

[12] Blancco Technology Group. Dban help center, Feb 2018. Last accessed 02, 2021.

[13] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[14] IDC. Worldwide market for used smartphones forecast to grow to 332.9 million units. https://www.idc.com/getdoc.jsp?containerId=prUS45865720, Jan 2020. Last accessed 02, 2021.

[15] Andrew Jones, Olga Angelopoulou, and L. Noriega. Survey of data remaining on second hand memory cards in the UK. *Computers & Security*, 84:239–243, 2019.

[16] Richard Kissel, Matthew A Scholl, Steven Skolochenko, and Xing Li. Sp 800-88 rev. 1. guidelines for media sanitization, 2006.

[17] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. "If I press delete, it's gone" — user understanding of online data deletion and expiration. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 329–339, 2018.

[18] Kopo Marvin Ramokapane, Awais Rashid, and Jose Miguel Such. "I feel stupid I can't delete...": A study of users' cloud deletion practices and coping strategies. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 241–256, 2017.

[19] Joel Reardon, David Basin, and Srdjan Capkun. SoK: Secure data deletion. In *2013 IEEE Symposium on Security and Privacy*, pages 301–315. IEEE, 2013.

[20] Joel Reardon, David Basin, and Srdjan Capkun. On secure data deletion. *IEEE Security & Privacy*, 12(3):37–44, 2014.

[21] Linda Serges and Hyla Mobile Inc. Q3 2020 mobile trade-in data. https://blog.hylamobile.com/q3-2020-mobile-trade-in-data, Nov 2020. Last accessed 02, 2021.

[22] Junliang Shu, Yuanyuan Zhang, Juanru Li, Bodong Li, and Dawu Gu. Why data deletion fails? A study on deletion flaws and data remanence in Android systems. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(2):1–22, 2017.

[23] Avast Software. Selling your smartphone could mean selling your identity. Avast finds used smartphones still contain personal information and data. https://press.avast.com/selling-your-smartphone-could-mean-selling-your-identity-avast-finds-used-smartphones-still-contain-personal-information-and-data, Feb 2016. Last accessed 02, 2021.

[24] Android Support. Reset your Android device to factory settings. https://support.google.com/android/answer/6088915. Last accessed: 02/2021.

[25] Apple Support. Erase iPhone. https://support.apple.com/en-ca/guide/iphone/iph7a2a9399b/ios. Last accessed: 02/2021.

[26] Samsung Galaxy Support. Perform a factory reset on your Galaxy phone. https://www.samsung.com/ca/support/mobile-devices/galaxy-phone-perform-a-factory-reset/. Last accessed: 02/2021.

[27] Windows Support. Recovery options in Windows 10. https://support.microsoft.com/en-us/windows/recovery-options-in-windows-10-31ce2444-7de3-818c-d626-e3b5a3024da5. Last accessed: 02/2021.

[28] Michael Yung Chung Wei, Laura M. Grupp, Frederick E. Spada, and Steven Swanson. Reliably erasing data from flash-based solid state drives. In *USENIX Conference on File and Storage Technologies*, 2011.

[29] Davey Winder. Researchers find 'dangerous levels' of sensitive data for sale on eBay. https://www.forbes.com/sites/daveywinder/2019/04/25/researchers-find-dangerous-levels-of-sensitive-data-for-sale-on-ebay/, April 2019. Last accessed: 02/2021.

A Appendices

A.1 Recruitment Advertisement

The following text was used to recruit participants from Facebook Marketplace, Kijiji, and local sub-reddits.
Title: Help with a research study and earn $2 for your participation
Body: Researchers from the University of Guelph are looking for participants for a study on understanding threats to personal data in the second-hand economy. You are eligible to participate in this study if you:

- are 18 years or older
- have currently listed an item for sale on online buying and selling market place like Facebook Marketplace or Kijiji

The study will be performed as an online survey that will take approximately 10 minutes and you will receive $2 for your participation. This research has received ethics approval (Research Ethics Approval Number 19-06-009). If you are interested in participating, please send an email to jceci@uoguelph.ca

A.2 Online Survey

The following multiple choice questions were asked during the online survey.
Demographic Information.

1 How old are you?
(a) 18-25 years old; (b) 26-30 years old; (c) 31-35 years old; (d) 36-40 years old; (e) 41-45 years old; (f) 46-50 years old; (g) Over 50 years old; (h) Choose not to respond

2 What is your gender?
(a) Woman; (b) Man; (c) My gender identity is not listed above; (d) Choose not to respond

3 Which of the following best describes your level of proficiency with technology like smartphones or laptops?
(a) Basic (I can perform basic tasks such as sending emails or browsing the internet);
(b) Intermediate (I can perform intermediate tasks such as changing the settings or installing new applications);
(c) Advanced (I am capable of writing source code)

Electronic Device Lifecycle. For this study, electronic devices refers specifically to electronic devices that can hold personal data such as cell phones, smartphones, laptops, desktop computers, tablets, portable hard drives/flash drives, memory cards and cameras.

4 When you no longer use an old device for any reason, what actions have you taken with your old device? (choose all that apply) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) Sell; (b) Give to friend/family; (c) Return/exchange to provider/IT department; (d) Recycle; (e) Throw in garbage; (f) Donate; (g) Keep; (h) Other; (i) I have never stopped using a device of this type.

5 You have answered other to one or more of the above. Please list the other actions you have done with old devices below. (*A box for free form text input is provided*)

6 On a scale from 1 to 5, how concerned would you be if someone (who was not a trusted friend or family member) was able to retrieve the data off of your old devices? (*5-point Likert scale "Least Concerned" - "Most Concerned"*)

Personal Data and Old Devices.

7 **[IF sold, donated, recycled or returned an old device]** You previously answered that you have sold, donated, recycled or returned an old device. Did you remove or attempt to remove your personal data before selling it? (If you have sold, donated, recycled or returned multiple devices, answer for the most recent.)
(a) No, I trust the recipient;(b) No, I am not concerned about the personal data on the device; (c) No, the device is encrypted so my personal data is safe; (d) Yes, I did a "factory reset" or "erase all content"; (e) Yes, I did a zero-fill or secure erase; (f) Yes, I deleted all data manually (i.e., deleting all files); (g) Yes, I deleted some sensitive data.

8 **[IF disposed a device]** How likely do you believe it would be for a person with AVERAGE computer/IT skills to be able to recover any personal data from the device you sold, donated, recycled or returned? (If you have sold, donated, recycled or returned multiple devices, answer for the most recent.) (*7-point Likert scale "Extremely Likely" - "Extremely Unlikely"*)

9 **[IF disposed a device]** How likely do you believe it would be for a person with EXPERT computer/IT skills to be able to recover any personal data from the device you sold? (If you have sold, donated, recycled or returned multiple devices in the same category, answer for the most recent.) (*7-point Likert scale "Extremely Likely" - "Extremely Unlikely"*)

10 **[IF kept an old device]** You previously answered that you kept an old device, what was the main reason you kept the device? (if you have kept multiple devices, answer for the most recent.)

(a) Not worth the hassle of selling or donating; (b) Privacy concerns; (c) Kept it as a backup; (d) Other (*A box for free form text input is provided to specify other*)

A.3 Semi-Structured Interview

The semi-structured interview contained both multiple choice questions (an extension of the online survey) and free form responses to questions that further explored the responses of the participants.

Additional Demographic Information. First, I am going to ask you some additional demographic information about yourself.

1 Which of the following best describes your HIGHEST level of education?
(a) Some high school; (b) Completed high school; (c) Some college/university; (e) Apprenticeship training and trades; (f) Completed college/university; (g) Some graduate education; ; (h) Completed graduate education; (i) Professional degrees; (j) Choose not to answer

2 Which of the following best represents your annual household income?
(a) Less than $30,000 ; (b) Between $30,000 and $74,999; (c) Between $75,000 and $99,999; (d) Over $100,000; (e) Choose not to answer

3 Which of the following best describes your level of proficiency with technology like smartphones or laptops?
(a) Basic (I can perform basic tasks such as sending emails or browsing the internet);
(b) Intermediate (I can perform intermediate tasks such as changing the settings or installing new applications);
(c) Advanced (I am capable of writing source code)

Electronic Device Lifecycle. Next, I am going to ask you about what you do with old devices you no longer use. For this study, electronic devices refers specifically to electronic devices that can hold personal data such as cell phones, smartphones, laptops, desktop computers, tablets, portable hard drives / flash drives, memory card and cameras.

4 What type of data do your old devices contain or previously contained? (choose all that apply) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) N/A; (b) Contacts; (c) Emails; (d) Photos; (e) Adult Content; (f) Personal adult content (myself or partner); (g) banking info / credit card; (h) Text and instant messages; (i) Passwords; (j) Personal videos; (k) Browser history.

5 On a scale from 1 to 5, how concerned would you be if someone was able to retrieve the data off of your old devices? (choose all that apply; choose N/A for devices you have not owned) (*5-point Likert scale "Least Concerned" - "Most Concerned"; User provides answer for each of the following categories: smartphones, laptops, tablets, cameras and memory cards, hard drives/flash drives*)

[IF gave a device away] Giving Devices Away.

6 You previously answered that you have given an old device to a friend or family member. Did you attempt to remove your personal data before giving it to them? (If you have given away multiple devices in the same category, answer for the most recent.) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) No, I trust the recipient;(b) No, I am not concerned about the personal data on the device; (c) No, the device is encrypted so my personal data is safe; (d) Yes, I did a "factory reset" or "erase all content"; (e) Yes, I did a zero-fill or secure erase; (f) Yes, I deleted all data manually (i.e., deleting all files); (g) Yes, I deleted some sensitive data; (h) N/A.

7 If response was yes to previous question, researcher asked how was the data erased or how was the device wiped or reset. If applicable, researcher asked participants to tell the steps taken for each device type and ask why participants used a certain method.

[IF sold a device] Selling Old Devices.

8 You previously answered that you have sold an old device. Did you remove or attempt to remove your personal data before selling it? (If you have sold multiple devices in the same category, answer for the most recent.) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) No, I trust the recipient;(b) No, I am not concerned about the personal data on the device; (c) No, the device is encrypted so my personal data is safe; (d) Yes, I did a "factory reset" or "erase all content"; (e) Yes, I did a zero-fill or secure erase; (f) Yes, I deleted all data manually (i.e., deleting all files); (g) Yes, I deleted some sensitive data; (h) N/A.

9 If response was yes to previous question, researcher asked how was the data erased or how was the device wiped or reset. If applicable, researcher asked participants to tell the steps taken for each device type and ask why participants used a certain method.

10 How likely do you believe it would be for a person with AVERAGE computer/IT skills could recover any personal data from the device you sold? (If you have sold

multiple devices in the same category, answer for the most recent.) (*7-point Likert scale "Extremely Likely" - "Extremely Unlikely"*)

11 How likely do you believe it would be for a person with EXPERT computer/IT skills could recover any personal data from the device you sold? (If you have sold multiple devices in the same category, answer for the most recent.) (*7-point Likert scale "Extremely Likely" - "Extremely Unlikely"*)

12 You previously answered that you have sold an old device in the past, which personal data category would you be most worried about a buyer accessing? (If you have sold multiple devices in the same category, answer for the most recent.)
(a) N/A; (b) Contacts; (c) Emails; (d) Photos; (e) Adult Content; (f) Personal adult content (myself or partner); (g) banking info / credit card; (h) Text and instant messages; (i) Passwords; (j) Personal videos; (k) Browser history.

[IF donated or recycled a device] Donating or Recycling Devices.

13 You previously answered that you have donated or recycled at least one old device. Did you remove or attempt to remove your personal data before donating or recycling it? (If you have sold multiple devices in the same category, answer for the most recent. Answer N/A if you have not donated or recycled a device of that type.) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) No, I trust the recipient;(b) No, I am not concerned about the personal data on the device; (c) No, the device is encrypted so my personal data is safe; (d) Yes, I did a "factory reset" or "erase all content"; (e) Yes, I did a zero-fill or secure erase; (f) Yes, I deleted all data manually (i.e., deleting all files); (g) Yes, I deleted some sensitive data; (h) N/A.

14 If response was yes to previous question, researcher asked how was the data erased or how was the device wiped or reset. If applicable, researcher asked participants to tell the steps taken for each device type and ask why participants used a certain method.

[IF returned a device] Returned Devices.

15 You previously answered that you have return at least one old device to the provides, IT department or manufacturer. Did you remove or attempt to remove your personal data before returning it? (If you have returned multiple devices in the same category, answer for the most recent. Answer N/A if you have not donated or recycled a device of that type.) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) No, I trust the recipient;(b) No, I am not concerned about the personal data on the device; (c) No, the device is encrypted so my personal data is safe; (d) Yes, I did a "factory reset" or "erase all content"; (e) Yes, I did a zero-fill or secure erase; (f) Yes, I deleted all data manually (i.e., deleting all files); (g) Yes, I deleted some sensitive data; (h) N/A.

16 If response was yes to previous question, researcher asked how was the data erased or how was the device wiped or reset. If applicable, researcher asked participants to tell the steps taken for each device type and ask why participants used a certain method.

[IF disposed a non-functioning device] Non-Functioning Devices.

17 For each device type, which of the following best describes what you have done with a **non-functioning** (broken, damaged) device you no longer use? (If you have had multiple non-functioning devices in the same category, answer for the most recent. Answer N/A if you do not have not had a non-functioning device of that category.) (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) Donate or recycle it; (b) Destroy it; (c) Throw it in the trash; (d) keep it; (e) Sell or give it away; (f) N/A.

18 You have previously answered that you have donated, recycled, sold, or given away a non-functioning device before, did you attempt to remove your personal data first? (If you have had multiple non-functioning devices in the same category, answer for the most recent. Answer N/A if you do not have not had a non-functioning device of that category.)
(a) No, I believe it would require too much effort for someone to retrieve my personal data; (b) No, my device was encrypted; (c) No, I haven't considered my personal data privacy in this case; (d) No, I don't know how to or it was too difficult to remove my personal data; (e) Yes, I removed or attempted to remove my personal data.

19 You previously answered that you have thrown away a non-functioning device before, did you attempt to remove your personal data first? (If you have had multiple non-functioning devices in the same category, answer for the most recent. Answer N/A if you do not have not had a non-functioning device of that category.)
(a) No, I believe it would require too much effort for someone to retrieve my personal data; (b) No, my device

was encrypted; (c) No, I haven't considered my personal data privacy in this case; (d) No, I don't know how to or it was too difficult to remove my personal data; (e) Yes, I removed or attempted to remove my personal data.

20 If response was yes to previous question, researcher asked how was the data erased.

Personal Data on Purchased Devices.

21 Have you ever purchased an electronic device that had personal data from the previous owner/user?
(a) Yes; (b) No; (c) Maybe

22 If response to the last question is yes, the researcher asked what type of data did they find from the previous owner? What device or device type was it? (iPhone, laptop, etc.)

Protecting Personal Data.

23 How difficult do you currently believe it is to fully remove all personal data from the following devices? (*Each of the following action is asked for the following device types: Smartphones, Laptops, Tablets, Cameras and memory cards, and Hard drives/flash drives*.)
(a) Easy; (b) Intermediate; (c) Difficult or Impossible; (d) N/A

24 I think the following is true about the "Reset Device" feature on my laptop or personal computer:
(a) It does not provide information that assists me in selling the device to a stranger; (b) It provides information that assists me in selling the device to a stranger; (c) N/A or Unknown

25 I think the following is true about the "Reset Device" feature on my smartphone:
(a) It does not provide information that assists me in selling the device to a stranger; (b) It provides information that assists me in selling the device to a stranger; (c) N/A or Unknown

26 When users are selling a used electronic device, I feel it is the responsibility of the following entities to inform users about the threats to personal data on the device: (*4-point Likert scale responses"Strong responsibility", "Some responsibility", "No responsibility but should assist", "No responsibility"*)
(a) Online platform/store (e.g., Kijiji or eBay); (b) Sellers themselves; (c) Device manufacturers (e.g., Apple or Samsung)

27 Has the difficulty to remove data from a device ever made you reluctant to sell or donate that device?
(a) Yes; (b) No

28 I believe that classifieds/online marketplaces should explain the risks associated with selling used devices and how to properly wipe used devices. (*5-point Likert scale "Strong agree" - "Strongly disagree"*)

29 I believe that device manufacturers should make it easier to securely remove all personal data from electronic devices. (*5-point Likert scale "Strong agree" - "Strongly disagree"*)

30 If an electronic device had a feature to securely remove all personal data, I would be more likely to purchase that device compared to a device that did not. (*5-point Likert scale "Strong agree" - "Strongly disagree"*)

31 If an electronic device had a feature to securely remove all personal data, I would be more likely to sell the device when I no longer required it. (*5-point Likert scale "Strong agree" - "Strongly disagree"*)

32 The researcher asked participants to rank the following terms in regards to how effective they are at removing and preventing recovery of personal data from a computer or electronic device before selling or recycling it: "Clean the drive", "Delete all files", "Erase the hard drive", "Secure erase the hard drive". (If two choices are equally effective, they were asked to assign them the same rank. The researchers noted the confusions that participants had regarding the use of these terms.)

A.4 Detailed Interview Findings

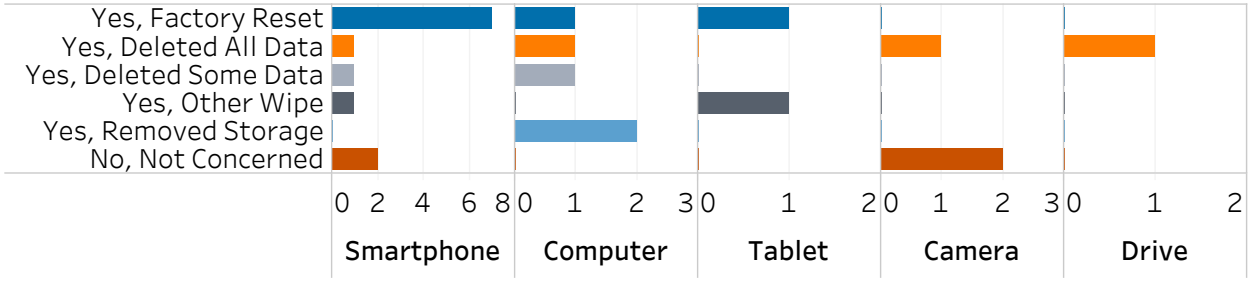


Figure 9: Participants' responses to "Did you remove any data from the device before donating or recycling it?"

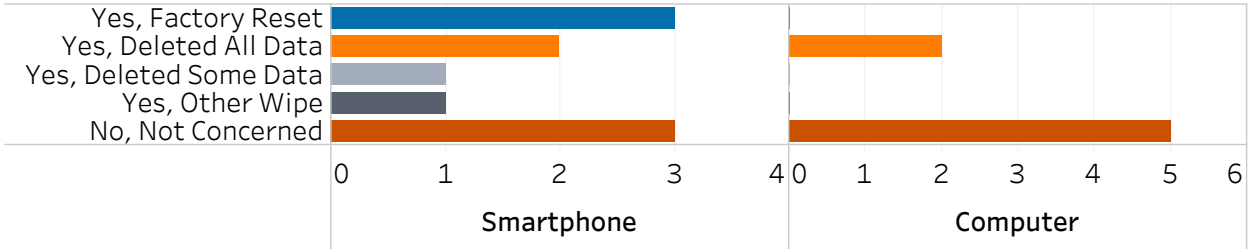


Figure 10: Participants' responses to "Did you remove any data from the device before returning it to a provider, IT department, manufacturer or retailer?"

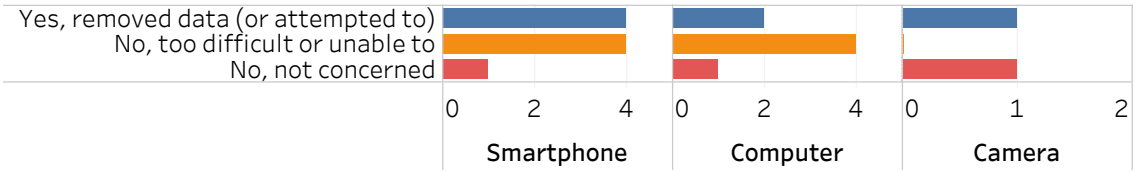


Figure 11: Participants' responses to "Before you sold, gave away, returned, threw away, recycled or donated the broken device, did you remove any data from it?"

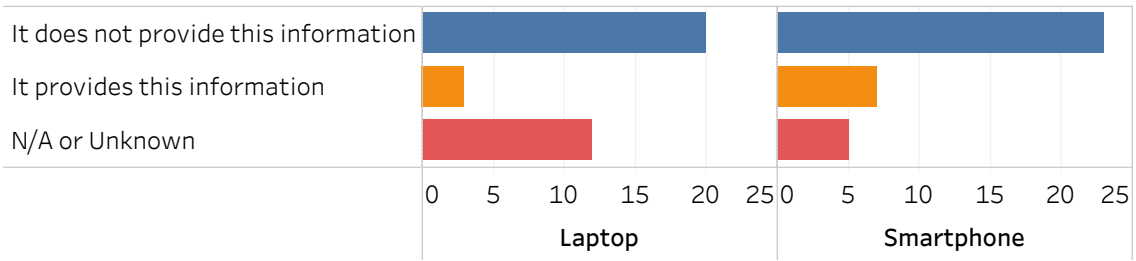


Figure 12: Participants' responses to "If you have used the reset feature in the past, did it provide you with any information that assists you when selling the device to a stranger? For example, if information is recoverable."