

# Security and Privacy with Second-Hand Storage Devices: A User-Centric Perspective from Switzerland

Kavous Salehzadeh Niksirat  
University of Lausanne / EPFL  
kavous.salehzadehniksirat@unil.ch

Diana Korka  
University of Lausanne  
diana.korka@gmail.com

Quentin Jacquemin  
University of Lausanne  
quentin.jacquemin@unil.ch

Céline Vanini  
University of Lausanne  
celine.vanini@unil.ch

Mathias Humbert  
University of Lausanne  
mathias.humbert@unil.ch

Mauro Cherubini  
University of Lausanne  
mauro.cherubini@unil.ch

Sylvain Métille  
University of Lausanne  
sylvain.metille@unil.ch

Kévin Huguenin  
University of Lausanne  
kevin.huguenin@unil.ch

## ABSTRACT

Second-hand electronic devices are increasingly being sold online. Although more affordable and more environment-friendly than new products, second-hand devices, in particular those with storage capabilities, create security and privacy threats (e.g., malware or confidential data still stored on the device, aka remnant data). Previous work studied this issue from a technical point of view or only from the perspective of the sellers of the devices, but the perspective of the buyers has been largely overlooked. In this paper, we fill this gap and take a multi-disciplinary approach, focusing on the case of Switzerland. First, we conduct a brief legal analysis of the rights and obligations related to second-hand storage devices. Second, in order to understand the buyers' practices related to these devices and their beliefs about their legal rights and obligations, we deploy a survey in collaboration with a major online platform for transactions of second-hand goods. We demonstrate that the risks highlighted in prior research might not materialize, as many buyers do not inspect the content of the bought devices (e.g., they format it directly). We also found that none of the buyers uses forensic techniques. We identified that the buyers' decisions about remnant data depend on the type of data. For instance, for data with illegal content, they would keep the data to report it to the authorities, whereas for sensitive personal data they would either delete the data or contact the sellers. We identified several discrepancies between the actual legal rights/obligations and users' beliefs.

## KEYWORDS

second-hand storage device, privacy, security, law, user survey

## 1 INTRODUCTION

The online second-hand market is flourishing [41]; for second-hand electronics (e.g., smartphones, computer hardware, USB sticks), in particular, it is estimated that the global market value will be worth

\$66 billion in 2026 [35]. The second-hand market constitutes a key pillar of the circular economy [56], a sustainable model that encourages the reuse of products. As such, it is increasingly attractive to consumers who care about their environmental impact, in addition to the original opportunity to purchase goods for less money.

Besides its benefits, transactions of second-hand products can create new *security* and *privacy* threats—if not conducted properly. For example, the previous owner of a used smart-home device might still have remote access to control it after they sold it (similarly to the case of electronic devices in Airbnbs [37, 47]). Such incidents can cause trouble for the buyers of these devices, for example, their homes might get burgled. The consequences can be particularly severe if the second-hand product has *storage capabilities*, such as external hard drives and USB sticks.<sup>1</sup> Such devices could include remnant data<sup>2</sup> such as personal data or malware. While the former can cause privacy risks for the device sellers, the latter can cause security risks for the buyers [8].

The threat is real and serious. As demonstrated by earlier investigations [27, 29–32], more than half of the second-hand storage devices include remnant data—in the clear or recoverable through specific tools (i.e., forensic tools for carving<sup>3</sup>; see Appendix B)—such as confidential documents, private keys associated with crypto-assets, and sensitive personal information such as intimate photos. Beyond the extensive forensic investigations, a few existing works [8, 21, 53] investigate this issue from the perspective of the *users'* perception and practices. The main focus of these studies is on the users who *sell* second-hand storage devices. However, to the best of our knowledge, the understanding of the perspective of the users who *buy* such devices is quite limited.

Studying the buyers' perspective is quite important. First, it helps understand the extent to which the *security of buyers* is put at risk by using second-hand storage devices that may include malware. Second, given that the aforementioned studies [27, 29–32] exploited and proved the existence of *privacy risks for sellers*, it is yet unclear

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit <https://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

*Proceedings on Privacy Enhancing Technologies* 2024(2), 412–433

© 2024 Copyright held by the owner/author(s).

<https://doi.org/10.56553/popets-2024-0057>



<sup>1</sup>We define second-hand storage devices as drives (HDD or SSD), USB sticks, and memory cards that were *used* by someone and then used by someone else. In this study, we did not include devices with storage capabilities such as smartphones or computers.

<sup>2</sup>We define remnant data as any data left on a device by one of its former users and that can be found in the clear or recovered by one of its new users.

<sup>3</sup>Carving is a forensic technique used to analyze unallocated space on storage device in search of known file signatures. It is used to recover fragments of deleted files.

if such risks for the sellers would *materialize* in practice. For this, it is likely that sellers might not be aware of the data they forgot in the device they sold. Thus, it is necessary to collect information about such privacy violations from the buyers.

In this paper, we take a multidisciplinary approach and focus on two different aspects. First, we study buyers' beliefs regarding their legal rights and obligations concerning online transactions for second-hand storage devices. To establish ground truth for these beliefs, we conduct a brief legal analysis to understand the legal aspects of the privacy and security risks associated with the transactions of second-hand storage devices. Second, we investigate the buyers' perspective, with respect to these transactions, including their perception and practices (i.e., routines, behaviors, or precautions). Specifically, we ask the following research questions:

- **RQ1. Data Handling Behavior of Buyers.** What do buyers do with data (or what would they do if they found any)?
- **RQ2. Security Awareness and Precautions of Buyers.** Are buyers aware of security risks? Do they take any precautions? Are these security risks likely to materialize?
- **RQ3. Privacy Risks for Sellers.** Are privacy risks for sellers likely to materialize in practice? In other words, is remnant data accessed/retrieved by the buyers? And if so, what kind of data?
- **RQ4. Legal Perspectives of Buyers and Sellers.** What do buyers believe their legal rights and obligations and those of the sellers are, vis-a-vis second-hand storage devices and the data they contain?

To provide the ground truth—necessary for designing survey questionnaires and data analysis—we conduct a brief, non-exhaustive, legal analysis, under Swiss law, for a diverse set of interesting situations. Note that the analysis is relevant for countries other than Switzerland with similar legal systems (e.g., European countries). Note also that, for the sake of simplicity and conciseness, we make simplifying assumptions in our analysis, focusing on the general case; different conclusions could be reached with specific sub-types of individuals, data or contexts. Concretely, we provide answers to different questions about (1) buyers' legal rights and obligations (e.g., “can buyers make personal use of the remnant data they find?” and “must buyers notify authorities if they find illegal content?”) and (2) the liabilities of other entities (i.e., sellers, platforms, third-party victims) for possible incidents (e.g., “can sellers be held liable if they did not effectively remove sensitive data *about others* or dangerous data from the device?” and “are platforms liable for such incidents?”). With regard to the latter, while the focus of this paper is on buyers, understanding the liabilities of other entities is crucial to better understand the buyers' perspective as their actions might be driven by their perceptions of what these entities are entitled to do.

We deploy a small-scale—but with good ecological validity—survey (i.e., a survey with respondents who actually bought second-hand storage devices) in collaboration with the largest online platform for second-hand transactions in Switzerland ( $N = 46$ ). The survey probes the buyers' experience, attitude, and behavior with regard to remnant data found and beliefs regarding the associated legal aspects. It also assesses their awareness of the risks and their knowledge regarding the associated technical aspects (e.g., carving).

Our findings show that nearly one-third of the buyers did not at all check for data, 70% formatted their devices, and no one seems to use forensic tools. These findings are indeed surprising. Despite substantial literature on potential risks (e.g., [27]), we are the first to look at whether the risks materialize in practice. Our results seem to indicate (in our, relatively small, dataset at least) that the risks rarely materialize (e.g., because buyers format devices immediately)<sup>4</sup>, at least with buyers that are not ill-intentioned. Despite these findings, even incidents for a small number of users can cause severe consequences. This potential detrimental impact was later resonated by the fact that the respondents reported their tendency to keep sensitive data. For example, 15% stated that they would keep financial data. We discovered that the respondent's attitudes toward *notifying* various entities were greatly dependent on the type of data. The typical pattern was to not notify others about non-sensitive data, to notify sellers about sensitive data, and to notify competent authorities about illegal data. With regard to *illegal data* (e.g., child sexual abuse material), two thirds of the respondents reported that they would not delete such data. In fact, they wanted to keep such illegal data in order to report it to the authorities. They also believed there is a legal obligation to notify authorities, when in fact, there is none. About 40% could not anticipate that they could be held liable if such data was not deleted. These results indicate that well-intentioned buyers might experience severe problems if they come across such data. Finally, we found other *discrepancies* between legal facts and users' beliefs. For instance, several buyers believed they did not have to comply with the seller's request for deleting data, even though they should.

## 2 RELATED WORK

The presence of remnant data on discarded (trashed but also sold as “second hand”) hard drives and the possibility to recover them was discussed as early as 2003 by Garfinkel and Shelat [18]. In this section, we review related works on (1) remnant data on second-hand storage devices and (2) users' behavior with respect to second-hand storage devices and risk perception since then.

### 2.1 Presence of Remnant Data & Implications

The first line of related works is composed of studies that investigate the prevalence and type of remnant data on second-hand storage devices, as well as the associated security and privacy implications. These studies demonstrate the existence of risks; our work investigates whether these risks materialize. These studies are summarized in Table 1 (Appendix A) and categorized based on the type and number of devices analyzed, the country where the study took place, and the type of remnant data found.

A group of researchers studied the presence of remnant data on second-hand storage devices, since 2005, by buying second-hand devices on online marketplaces (e.g., eBay) and analyzing them by using forensic tools and methods [27, 29–32]. They performed, at first, a longitudinal study, covering multiple country markets, on hard disks and then extend their work to the investigation of other

<sup>4</sup>While this indicates a lack of data inspection and reduces the chances that the risk materializes immediately, it should be noted that formatting might not ensure data removal and that the buyer, or a future user, might still be able to recover data later.

country markets [2, 26, 38] and other types of second-hand devices such as USB sticks [28] and memory cards [25]. For instance, Jones et al. [25] reported recovering business documents, medical case reports, financial information (credit-card PIN numbers), personally identifiable information (vehicle registration numbers, phone numbers), photos of an intimate nature, and pornographic images. Interestingly, 29% of the memory cards were formatted, but data could still be recovered. They also study repairing unusable second-hand hard disks [48] and focus on hard disks that originate from corporate servers [54]. They reveal that around 60% of these devices contained recoverable data with different degrees of sensitivity such as confidential documents, resumes, crypto-asset keys, and databases. These findings on storage devices align with forensic studies on portable devices (e.g., mobile phones and tablets) [1, 6, 20] and a recent study on wearables (e.g., Fitbit) [40]. For example, Angelopoulou et al. [1] showed that one fifth of second-hand portable devices with remnant data contain the sellers' identity.

In parallel, a different group conduct similar longitudinal studies that were more focused on *portable* second-hand devices, such as USB sticks [44, 45] and memory cards [49–52]. They conclude that users fail to sanitize properly their devices and that no improvement can be observed, regardless of the number of available tools and the increase of regulations and publicity for raising awareness of users. A number of assumptions are made regarding the possible reasons behind those alarming observations, such as the lack of awareness about data deletion mechanisms (see Section 2.2). These studies showed that sellers' privacy could be at serious risk. However, this risk only would materialize if buyers actively seek remnant data (e.g., if they do not wipe the device and use carving methods). Therefore, we focus on collecting buyers' perspectives and experiences. Also, besides these studies, some real-life incidents are reported in the media. For example, in 2014, BBC News reported a forensic investigation that could recover nude pictures from 'factory reset' phones<sup>5</sup> or the Guardian reported an individual who was a victim of identity theft after selling his laptop on eBay.<sup>6</sup> Roberts et al. [43] conducted a similar analysis for cellphones seized by police departments and subsequently sold at auctions. The study uncovered alarming cases of personal information being exposed, including sensitive information not only about the owners, but also about their personal contacts and victims (i.e., in the case of criminals). Finally, our work aligns with a recent study in the electronics repair industry [9], revealing pervasive privacy violations by technicians, including unauthorized access to users' data folders, sensitive pictures, and financial information.

Other researchers studied the effectiveness of deletion methods on storage devices. BenRhouma et al. [4] analyze the data left on Android smartphones, after removing applications or doing a factory reset, and show that these operations did not effectively delete user data. Schneider et al. [46] find that remnant data could be recovered from 'new' USB sticks due to memory-chip recycling.

## 2.2 Users' Perspective

The second line of related works is composed of studies on users' perceptions—mainly sellers—regarding remnant data, in particular their awareness and use of data-deletion mechanisms for sanitizing storage devices they sell on second-hand marketplaces.

*Misleading User Interface and Mental Models.* Gutmann and Warner [21] test the different operations of data deletion (e.g., formatting, wiping) that are available to users on Windows and macOS. They reveal the confusion users face, caused by an unclear interface of the operating systems, when performing data-deletion operations [21]. They show that the terms 'erase' and 'delete' are used interchangeably—although they do not describe the same mechanism (as explained in Appendix B)—and that operating systems are not sufficiently transparent to users about what really occurs when the users performing such operations. Such design flaws lead users to fail sanitizing their devices effectively. Ramokapane et al. [42] surveyed cloud users and found that users fail to delete data in the personal cloud-storage space due to incorrect mental models or unclear cloud interfaces for data deletion. Interestingly, users develop coping strategies to overcome this problem (e.g., by not storing sensitive data in the cloud). To conclude, unclear user interfaces and users' incorrect mental models are two important reasons why sellers may leave remnant data on their old devices.

*Security Practices.* Conacher et al. [11] bought a number of USB sticks on eBay, analyzed them, and then deployed a survey to investigate users' awareness and actions taken to prevent the presence/recovery of remnant data. Most participants (94%) mentioned they would plug in a USB stick if they found one. Surprisingly, only a few participants mentioned they would format the device. In a different context, Tischer et al. [53] intentionally left a large number of USB sticks on their university campus. They found that 98% of them were picked up and in almost half of the cases (45%), the individual who found the device opened the files on it. The study showed that the main motivation for these individuals was altruistic (i.e., to return the device to its owner) and that the majority did not take any precautions when plugging in the device into their computers [53]. While such research provides a general indication of perceived security risks and informs our work, it still needs to be determined how *buyers* perceive the risks and take protective.

*Sanitizing Practices.* Ceci et al. [8] investigate why users fail to effectively remove data from their devices. The majority of the respondents reported using less secure methods (e.g., manual deletion) or the 'factory reset' function, for sanitizing their devices. Even though the majority of the respondents thought data can be easily recovered, they reported not using any secure sanitizing methods with broken devices, thinking that putting files in the recycle bin would be enough to remove data. Also, the participants were more inclined to keep their devices, or give them away to an acquaintance, than to sell them. But only one-third mentioned privacy reasons. Frik et al. [17] show similar findings for older adults who have a misconception about data deletion and might be less aware of potential privacy-related risks. On a different study, Frik et al. [16] indicated that a large number of smartphone users are uninformed about the presence of data-erasing methods. Dieburg et al. [12] survey participants who were willing to trade their

<sup>5</sup>See <https://www.bbc.com/news/technology-28264446>.

<sup>6</sup>See <https://www.theguardian.com/money/2013/sep/28/identity-theft-fears-faulty-laptop-resold>.

old USB sticks for new ones. But they do not find a statistically significant correlation between user perception of deletion/data recovery and the method they effectively used before trading the devices. Finally, Krumay [34] interviews company managers about the handling of electronic devices at their end of life (EoL) and showed that regulations are not always in place and that privacy awareness influences how data is handled at EoL.

*Research Gaps.* Earlier studies mainly considered the perceptions and behaviors of sellers—not the perspectives of *buyers*. Buyers can both exploit remnant data and be victimized by it. Thus, investigating the case of remnant data from their perspective is paramount. Moreover, previous research did not study the *legal* aspects of buying/selling. In particular, regarding buyers’ perception of their *responsibility* toward remnant data, our knowledge is limited. The only relevant study is from Glisson et al. [19] who explored the legal and ethical implications behind the use of second-hand devices for *researchers* (but not for the *lay users* who sell and buy such devices).

### 3 LEGAL ANALYSIS

To establish the ground truth for putting in perspective users’ beliefs about the legal aspects of the remnant data on storage devices (see RQ4), we provide insights about users’ legal rights and obligations concerning online transactions for second-hand storage devices. The objective of the legal analysis is to identify key points for discussion and inform the survey design and analysis. While the legal analysis is not exhaustive, serving more as an issue spotter, it strategically highlights *diverse* and *pertinent* legal aspects. This approach allows us to gain rich and valuable insights on different facets of the problem within the constraints of space and scope of our study. This brief legal analysis is conducted by two of the authors who are legal scholars—experts in the considered legal aspects. One of them is also a practicing attorney. We based this analysis on Swiss law where the study was conducted. Since there is no specific legislation in Switzerland regarding the second-hand market, we rely on a variety of relevant laws, including criminal law and certain provisions of data protection law (which is very similar to that of the EU, but different from that of the US). An introduction to Swiss law is provided in Appendix C.

Here, we first define *data ownership*. Individuals do not *own* data. They have rights on data, mainly intellectual property rights on protected content and, to protect themselves, personality rights. The data subject (i.e., the identified or identifiable individual to whom the data relates) has rights, and the data controller (i.e., the entity who processes data) has obligations. This means that when the buyer acquires the second-hand device, they legally own the device and the transferred rights on the data. For remnant data, there is generally a lack of knowledge/willingness to validly transfer any right on this data, unless specified in the ad posted on the platform.

#### 3.1 Legal Analysis Limitations

Our legal analysis has several limitations. First and foremost, it is important to note that our analysis is primarily rooted in Swiss law. Given the significant variations in criminal offenses across jurisdictions, the conditions of application may differ, requiring careful verification in each case. Consequently, the applicability of our legal analysis should be approached with caution outside the

Swiss context. Nevertheless, with respect to data protection laws, it is noteworthy that Swiss law closely aligns with GDPR,<sup>7</sup> making our analysis potentially more relevant for EU jurisdictions. While the shared principles discussed in our analysis may have relevance in various countries, it is crucial to exercise greater caution in applying our findings to jurisdictions with distinct legal frameworks, particularly in the US, where the absence of comprehensive privacy legislation necessitates careful consideration.

Moreover, our analysis reveals specific distinctions between Swiss and US law in critical areas. For instance, differences exist in the treatment of child sexual abuse material reporting obligations, where explicit requirements for service providers in Switzerland may not align with those in the US, especially for individual users. Additionally, our findings indicate variations in the legality of using inadvertently remnant data. US law generally permits such use in certain contexts, considering factors such as trade secrets, and privacy, but not copyright.

Lastly, our analysis, constrained by space limitations and the need to establish a “definitive” ground truth, incorporates simplifying assumptions and introducing a level of abstraction that may lack nuances in certain aspects. This is a deliberate choice for the sake of interdisciplinary clarity. It is crucial to acknowledge that *the answer to many legal questions posed in our analysis often depends on the specific context, with potential exceptions*. To address this inherent limitation and the complexity of legal interpretation, we recognize the role of prosecutorial discretion and potential defenses arising from unevenly enforced laws. While our analysis offers general insights, the application of specific legal principles may vary based on judicial and prosecutorial discretion, adding a layer of complexity that extends beyond the scope of this study. We have explicitly marked these simplifying assumptions in the following sections (labeled as **▲** at the beginning of the statement), indicating that the marked conclusion holds in the general case but might vary in specific instances, depending on factors such as individuals, data types, context, or judicial and prosecutorial discretion.

#### 3.2 The Buyers’ Perspective

*Potential Liability for “Intrinsically Illegal” Content.* One shall distinguish between content that is illegal per se and other content. Intrinsically illegal content is any content that the legislature has deemed so harmful that the mere fact of knowingly possessing it is likely to be held liable, for instance child sexual abuse material. Concretely, it means **the mere possession of child sexual abuse material is a criminal offense, even if the buyer did not seek or want to acquire such content.**<sup>8</sup> The fact that the buyer willingly chooses to keep this content after knowing its nature is punishable (except in specific cases, e.g., if the buyer is instructed to do so by the authorities when reporting the offense to them).<sup>9</sup> To be liable, it is *not* necessarily required to recover them through carving. Although it might differ in other jurisdictions, in Switzerland, there is no clear obligation to **notify the criminal justice**

<sup>7</sup>Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; GDPR).

<sup>8</sup>Art. 197 n. 5 SCC

<sup>9</sup>CR CP II-Cambi Favre-Bulle, Art.197 N 63.

**authorities** if the buyer finds, on a storage device, in the clear or through carving, for example, evidence of drug trafficking. Nevertheless, it is **preferable** to do so because if they do not and it is known afterward that they kept such evidence away from the authorities, they *might* be held liable for concealing evidence of an offense and for assisting offenders.<sup>10</sup>

*Potential Liability for “Illegal Uses” of the Data.* Here, we review finding other types of data that are *not* intrinsically illegal but whose *usage* can be punishable by law (i.e., some usage is illegal). For instance, if a buyer discovers nudes (i.e., intimate personal photos featuring naked people) or family pictures, of which possession is not *per se* illegal, they could decide to use these to blackmail the seller.<sup>11</sup> The Swiss law limits buyers from freely using such data.<sup>12</sup> This follows both from the *principle of good faith*<sup>13</sup> and specific legal provisions, such as the rules on the protection of personality and intellectual property rights.<sup>14</sup> Therefore, **if the seller forgets documents that hold corporate secrets, it is difficult to accept that the seller had any intent to share it with the buyer. The buyer would then be acting in bad faith if they sell the data.**<sup>15</sup> ▲ Similarly, if they find a draft of a book written by the seller, they would be acting illegally and in bad faith if they publish it under their own name.<sup>16</sup> However, this depends on the interpretation and specific criteria for the intellectual property status of the document. ▲ The same logic applies when a buyer finds credentials or redeemable financial data (e.g., vouchers) and uses them. Again, it also depends on the type of voucher/service and possibly, for the punishment, on the amount.

*Potential Liability for Recovering Data through “Carving”.* By recovering data through carving, the buyer could commit an additional offense (i.e., concurrent sentencing).<sup>17</sup> This raises the question of *whether the recovery of data is in itself unlawful*.

Two criminal norms are relevant in Switzerland: Art. 179novies SCC (i.e., obtaining personal data without authorization) and Art. 143 SCC (i.e., unauthorized obtainment of data). While the former makes it an offense to obtain without authorization sensitive personal data “which is not freely accessible,” the latter punishes the obtainment of data “that is not intended for them and has been specially secured (e.g., by a password, deletion) to prevent their access.” This question is addressed neither in the literature nor in the case law. In our opinion, it could be assumed that recovering data, through carving, fulfills Art. 179novies SCC and Art. 143 SCC.

<sup>10</sup>Art. 305 SCC

<sup>11</sup>This behavior could be punished for extortion (Art. 156 SCC), threatening behavior (Art. 180 SCC), or coercion (Art. 181 SCC).

<sup>12</sup>This is especially true when the owner forgets data, because it means they did not explicitly consent to give it.

<sup>13</sup>This principle is codified in Art. 2 and 3 of the Swiss Civil Code.

<sup>14</sup>The assignment of the ownership of a copy of a work does not include the right to exploit the copyright, even in the case of an original work (Art. 16 al. 3 of the Federal Act on Copyright and Related Rights of 9 October 1992, Copyright Act, CopA; RS231.1).

<sup>15</sup>They risk violating a norm that protects the economic interests tied to a secret, such as the Art. 5 and 23 of the Federal Act on Unfair Competition of 19 December 1986 (FAUC; RS 241) or the Art. 162 SCC. However, this assumption might differ under US law as the treatment of trade secrets or commercial proprietary data obtained without deception would generally be legal.

<sup>16</sup>Art. 67 CopA

<sup>17</sup>“Concurrent sentencing” means in concrete terms that it is an aggravating circumstance that the judge will take into account (negatively) when setting the sentence (Art. 49 SCC). In other words, it can contribute to increasing the sentence.

The act of deleting data from the device is a strong signal of closure that indicates that the seller did not want the buyer to discover, keep and/or use the data. However, it could also be considered that, if data can be recovered through carving, the buyer insufficiently protected the data and could therefore be held liable.

*Potential Liability for “Personal Uses of Non-intrinsically Illegal” Data.* For content protected by intellectual property rights (e.g., music, films), acquired by the seller either legally or illegally, and either available in the clear or recovered through carving, the general principle is that the buyer *cannot* freely use such data. A case-by-case analysis is necessary to establish if and to what extent the seller can share or transmit these rights, and if this was the common intent of the seller and the buyer. However, Art. 19 CopA provides that “any personal use of a work or use within a circle of persons closely connected to each other, such as relatives or friends” is permitted. For instance, if the buyer finds movies, they can legally watch them.<sup>18</sup> However, if they opt for sharing it on social media or for publicly sharing even a nature landscape picture of the seller’s holidays, they could be held liable because this is forbidden by intellectual property laws.<sup>19</sup> Overall, **it can assumed that if the buyer finds data that is not intrinsically illegal and either keeps it for themselves or uses it in a strictly personal way, they cannot be held liable, as long as they neither communicate nor sell the data.** For example, if they find personal nude photos (e.g., of the seller or of their contacts), they can legally keep them and make personal use of them (e.g., look at them).<sup>20</sup>

*Summary. In order to avoid liability, buyers should destroy intrinsically illegal contents when they discover them, preferably after having communicated them to the competent authorities (optional).*<sup>21</sup> Although it might differ in other jurisdictions, if a buyer keeps non-personal data (such as natural landscape photos) for themselves, there is *no legal basis* for obliging the buyer to inform anyone, apart from common sense and the general principle of good faith. However, it is safe to assume that if they find and keep personal data (such as pictures of the seller’s family on holiday), they might be subject to the FADP. According to this law (that generally does not apply to a mere domestic use, e.g., without communication), the mere act of keeping data is considered processing, so the buyer becomes the controller of the data, with all the obligations it implies.<sup>22</sup> Hence, **the buyer (controller) must inform the data subjects that they have collected their data,**<sup>23</sup> unless the provision of contact information is not possible or if it is possible only with disproportionate inconvenience or expense.<sup>24</sup>

<sup>18</sup>Barrelet Denis/Egloff Willi, dans: Le nouveau droit d’auteur, Commentaire de la loi fédérale sur le droit d’auteur et les droits voisins, 4e éd., Berne 2021, Art. 19 N 11 ss.

<sup>19</sup>Art. 2 al. 3bis, 10 al. 1 and 61ss CopA: The author of the picture has the exclusive right to decide how their work can be used.

<sup>20</sup>Salvadé Vincent, Le droit d’auteur dans le nuage ou dans le brouillard?, sic! 2012 p. 161 ss, p. 163.

<sup>21</sup>As there is no obligation to report, deleting the data without reporting it would not be considered an obstruction of justice.

<sup>22</sup>Art. 2 al. 1 let. a FADP and Art. 5 let. a, d, and j FADP.

<sup>23</sup>According to Art. 19 FADP, the data controller must communicate to the data subjects the information that they need in order to assert their rights, such as the name and coordinates of the data controller.

<sup>24</sup>This is an exception under Art. 20 al. 2 FADP.

▲ In accordance with Swiss law, if a buyer finds content that indicates a criminal offense, they can report it to prosecution authorities such as the police—but they do not have a legal duty to do so. Notwithstanding the lack of obligation to report, **they should report it to the authorities if they do not want to take the risk of being held liable for assisting offenders<sup>25</sup> (and for moral reasons)**. If the buyer is harmed, for instance, because the storage device they bought contains, in the clear, ransomware, they can lodge a criminal complaint<sup>26</sup> and claim for (civil) damages.<sup>27</sup> Finally, **if the seller asks the buyer to delete the data found on the device, it is preferable to comply**. If the buyer refuses to do so, the seller can sue them (e.g., based on intellectual property law, privacy law, or data protection law). After which, the authority can order the buyer to return/delete the data.

### 3.3 The Sellers' Perspective

We consider that the seller is the owner of the device (in our study, we excluded professional sellers).

*Potential Liability.* It is important to keep in mind that the seller can be convicted if and only if they act intentionally.<sup>28</sup> Criminal offenses include, for example, the breach of secrecy,<sup>29</sup> confidentiality,<sup>30</sup> and security measures,<sup>31</sup> but also the damage to data,<sup>32</sup> computer fraud,<sup>33</sup> the sharing of illegal content, etc. ▲ Notwithstanding the specifics of the case, **the seller can be criminally liable if, they willingly leave on the device, in the clear, confidential, or dangerous data (e.g., malware)**. The same applies when they know there is malware on the device.

If the seller acts through negligence, they can be criminally convicted only if the legal provision specifically stipulates so.<sup>34</sup> In this context, the seller's profession or technical skills can be taken into consideration when the judge assesses their guilt. For instance, if a seller with limited computer knowledge deletes sensitive data related to another individual (e.g., photos of their partner naked) but this data is recovered through carving (which they did not know was possible) and shared by the buyer, it is unlikely that the seller can be held liable from a criminal perspective. A computer scientist, however, is likely to be held liable. Note, however, that civil liability (for suffered damages) is independent from a criminal conviction, under Swiss law.

*Summary.* Ideally, sellers should use secure data-deletion techniques before handing over the device to the buyer. If the seller deletes the data without knowing it could still be retrieved, for instance through carving, it could reasonably be assumed that the seller has no intention to commit an infraction hence should not be liable. Nevertheless, if the seller is a data controller (e.g., a company selling servers on which it stored data of its clients), they must take

<sup>25</sup> Art. 305 SCC

<sup>26</sup> Art. 30 SCC

<sup>27</sup> e.g., Art. 41 of the Federal Act on the Amendment of the Swiss Civil Code of 30 March 1911 (RS220).

<sup>28</sup> Art. 12 al. 1 SCC.

<sup>29</sup> Breach of manufacturing or trade secrecy (Art. 162 SCC).

<sup>30</sup> Breach of professional confidentiality (Art. 321 SCC, Art. 62 al. 1 FADP, Art. 47 Federal Act on Bank of 8 November 1934, FAB; RS 952.0).

<sup>31</sup> Art. 61 let. c FADP.

<sup>32</sup> Art. 144bis al. 1 SCC.

<sup>33</sup> Art. 147 SCC.

<sup>34</sup> Art. 12 al. 1 and 3 SCC.

technical and organizational measures appropriate to the risk (e.g., hire a professional to effectively erase the data).<sup>35</sup> The seller should report such a data breach to the data-protection authorities.<sup>36</sup>

### 3.4 The Platforms' Perspective

There is no general monitoring or active obligation to find criminal sellers, preventively.<sup>37</sup> In Switzerland, there are no laws dealing specifically with the obligations of digital platforms. Although there is no precedent, we should consider that **there is a general obligation to act to avoid complicity, at least when the platform has been informed by a criminal justice authority**. For example, if a court orders the platform to shut down the account of a seller who sold devices containing malware, but the platform does not react, it might be held liable for complicity.

### 3.5 The Third-Party Victims' Perspective

We study third parties—besides the buyers and sellers—that can be the victim of such incidents. A victim can be, for instance, a person whose data is processed or a person who appears in a nude photo found on the second-hand storage device of the seller is blackmailed by the buyer. This is a typical interdependent privacy situation [5, 24]. In this situation, we identify three main legal remedies, in accordance with Swiss law. First, under criminal law, the victim can lodge a criminal complaint (in this case, for blackmail)<sup>38</sup> with the authorities (mainly the police and the public prosecutor).<sup>39</sup> Second, if the victim's personality is harmed (e.g., the buyer publishes the nudes on a social network, the buyer simply refuses to delete the nudes), they can act on the basis of Art. 28ss of the Swiss Civil Code and claim civil damages. Third, the victim can demand that, based on the data protection law, the buyer stops processing and/or deletes their personal data.<sup>40</sup>

## 4 METHODOLOGY

To study the behaviors/attitudes and beliefs (w.r.t. the associated legal aspects) of buyers of second-hand storage devices, we deployed an online survey to users with real experience ( $N = 46$  answers).

### 4.1 Recruitment

To increase the ecological validity of our survey and the quality of the collected data, we recruited our respondents among users of Ricardo, as the respondents actually bought a storage device on the platform. Ricardo is the most popular online classified ads platform for transactions of second-hand products in Switzerland, with more than 4 million members and more than 1.9 million active ads. Compared to its competitor, eBay, Ricardo had five times more sales in Switzerland in 2010.<sup>41</sup> We conducted the study in the Fall of

<sup>35</sup> Art. 8 al. 1 FADP. If the data processor knows that they must ensure a higher standard of protection but willingly do not do so, they could be liable in accordance with Art. 61 let. c FADP.

<sup>36</sup> Art. 24 FADP.

<sup>37</sup> In Switzerland, this principle was laid down in case law (6B\_1360/2021, 6B\_645/2007).

<sup>38</sup> Art. 156 SCC.

<sup>39</sup> Art. 304 al. 1 CrimPC.

<sup>40</sup> Art. 32 al. 2 FADP.

<sup>41</sup> <https://fr.wikipedia.org/wiki/Ricardo.ch>. More recent statistics about Ricardo's market share can be found here: <https://swissmarketplace.group/what-switzerland-costs-2/general-marketplaces/which-online-marketplace-did-people-in-switzerland-use-to-make-second-hand-purchases-in-2021/>.

2022, in partnership with Ricardo that forwarded our questionnaire to their users who fulfilled our recruitment criteria:

- (1) **Being a non-professional user of Ricardo** (to focus on lay users, not on those who use the platform for their businesses);
- (2) **Having bought a used second-hand storage device (e.g., drives, memory card, USB stick) on Ricardo<sup>42</sup> in the last 12 months** (to support a better recollection of the transaction);
- (3) **Having chosen German as their preferred language on Ricardo** (to avoid differences in interpretation caused by the use of multiple translations of the questionnaire; German is the most spoken language in Switzerland);
- (4) **Having subscribed to Ricardo's newsletter** (to exclude users who prefer to not receive additional information).

From the initial set of transactions over a period of 12 months, Ricardo retained 1,184 eligible transactions. They filtered this set by excluding buyers who had opted out from receiving information from the platform, buyers who had registered as professional users, buyers who selected a language other than German for their communications with the platform, and transactions with brand new (i.e., unused) or broken devices. We further excluded, after closer inspection, transactions that had been misclassified by sellers (e.g., empty NAS units, RAM). Some buyers were involved in more than one transaction. We kept only the most recent transaction for each buyer, to optimize their recollection of the transaction. We identified 472 unique eligible buyers. The breakdown of the transactions, in terms of device type, was as follows: 368 drives (incl. 167 SSDs), 62 memory cards, and 42 USB sticks.

## 4.2 Design of the Online Survey Questionnaire

We designed a questionnaire with seven sections to collect information about respondents' real experiences, their attitudes toward security practices for specific types of data, their beliefs about legal rights and obligations of the buyers and sellers, and about their general knowledge about technology and security. The questionnaire included a total of 20 questions with 150 items (e.g., statements in grid questions). However, each respondent received at most 137 items based on their specific answers and experiences. The verbatim version of the questionnaire is available in Appendix D. The full version is available in [Supplementary 1](#).<sup>43</sup> Next, we describe each section in the order they were presented to the respondents.

*Sec. A: Security Knowledge.* To assess the security knowledge of the respondents, we presented them with eight statements (four true and four false)—split in two blocks (see Q1–Q2)—about data-deletion and -recovery techniques, and malware. The knowledge questions were asked using a seven-point Likert scale from *strongly disagree* to *strongly agree*. We presented this section first, as the following questions could have biased respondents.

*Sec. B: Experience (w.r.t device and data).* To collect direct observations of buyers' behavior, we used the critical incident technique [14], where we asked them to remember their experiences of buying a second-hand device (i.e., related to the most recent

purchase on the platform). This technique has been used in many security & privacy studies to collect users' experiences (e.g., [10]).

The section began with questions about if the respondents found any data after plugging in the device they purchased (see Q3). The respondents can select 'Yes,' 'No,' 'I do not remember,' or 'I did not check.' The respondents who answered 'Yes,' were further asked about the type of data they found (see Q4). Before designing the questionnaire, we identified different types of data based on the literature review, summarized in Appendix A. We included a wide variety of data types including regular or sensitive photos of the seller, confidential data that disclosed information about the seller, passwords, financial data, data about illegal activities, illegal content, data related to an identified organization, and any data related to identified third-party individuals other than the seller. We also included an "Other" option; respondents could use it to mention that they did not check the data types or did not remember. We also asked the respondents whether the data was accessible "in the clear" on the device or if they used a specific file-recovery technique (e.g., carving) (see Q5). Next, we focused on specific data-types found by the respondents. For each checked data-type, we asked three customized questions on whether they deleted the file (see Q6), if they used it, e.g., opening, copying, printing, sharing (see Q7), and if they contacted any entity to notify them about the data they found (see Q8). The entities included the seller (to be contacted via the Ricardo platform), a third-party individual or organization that owned the data, the authorities, or a contact person from the Ricardo platform. The last three questions were repeated if respondents found data types *other* than those we listed.

Finally, we asked all the respondents about the precautionary actions they took (predefined list plus an "other, please specify" text box, see Q9). We asked if they formatted the device, scanned it using anti-virus software, or if they first plugged the device into a device other than their main device. We also asked if their device was infected by malware from the purchased equipment and, if so, what kind of malware, e.g., spyware, ransomware (see Q10–Q11).

*Sec. C: Attitudes (w.r.t. data).* To investigate respondents' attitudes toward different actions, we used hypothetical scenarios. For any type of data that was reported as *not found*, in Sec. B, we asked a question with seven statements. We asked the respondents to *imagine* they had found a particular type of data on the device they purchased. Then we asked them how likely they would be to delete the data or to use it in any way, and whether they would notify the device owner, data subject (individual or organization), authorities, or the platform (see Q12). We used a seven-point Likert scale.

*Sec. D: Legal Beliefs.* To capture the respondents' beliefs about the legal rights and obligations of a seller and of a buyer upon selling or buying a second-hand storage device, we presented them with 21 statements and asked them to what extent they agree or disagree with the statements using the seven-point Likert scale, from *strongly disagree* to *strongly agree* (see Q13).<sup>44</sup>

Twelve statements were relevant to specific data-types on what users think is their right to do or what they should avoid doing with specific data found on their device, such as having the right to

<sup>42</sup>We relied on Ricardo's predefined product categories by which users label ads. We manually checked the validity of the user-declared type of storage devices sold.

<sup>43</sup>All supplementary materials are available in the Open Science Framework (OSF) repository. See <https://osf.io/esyvf/>.

<sup>44</sup>Our goal was not to establish the respondents' knowledge but to assess their intuitions about legal aspects. The middle point could be used by respondents who are unsure or judge the item context-dependent.

make personal use of the data, sharing the data on social media, not deleting the data, etc.. For instance, “If I find redeemable financial data (e.g., crypto-assets, vouchers) I can legally cash them in”. Nine statements focused on users’ general perceptions of rights and obligations. The respondents were asked if they have the right to use carving or forensic tools to access data deleted by the previous owner, if they are obliged to notify anyone about the data they found, or if the seller or the platform are liable for such incidents. For instance, “if a used device I bought contains malware in the clear, the second-hand shopping platform can be held liable.”

*Sec. E: Background.* To further characterize the respondents, we asked them about their age and gender (see Q14–Q15). We also assessed their privacy concerns using three-item Internet Users’ Information Privacy Concerns (IUIPC) [36] (see Q16).

*Sec. F: Security Practices.* To measure the respondents’ general security practices and skills in everyday life, we adopted the questions from the Security Behavior Intentions Scale (SeBIS) [13] (see Q17). We added two statements on security practices (see Q17), inspired by a previous research [53]. We used a five-point Likert scale, from *never* to *always*. The question about security skills (see Q18) asked whether they know how to use anti-viruses, how to empty the trash bin of their device, to format or to wipe their device, etc. We used a seven-point Likert scale, from *very untrue of me* to *very true of me*.

*Sec. G: Expectations.* To assess users’ expectations from online second-hand shopping platforms, we asked if they would have liked to receive more information from the platform when they bought a second-hand storage device (see Q19) and, if so, if such information should be about technical aspects (i.e., security & privacy risks) and/or legal aspects (i.e., rights, obligations, and liability). Using an open-ended question, we also asked them if they would change anything in the buying process (see Q20). Finally, we debriefed respondents by providing them information on the security & privacy risks, and on their legal rights and obligations.

### 4.3 Procedure

We had the questionnaire proofread by a professional German teacher and by two Ricardo employees. Also, we conducted a cognitive pretest with a native (Swiss) German-speaking colleague (not involved in this research), familiar with Ricardo. The cognitive pretest was conducted in person with two co-authors accompanying the participant. We asked him to read the questions aloud and to explain what the questions meant to him. We also asked the participant to notify us when the question was not clear. From this practice, we modified several questions. For example, we made some of the text entry questions non-compulsory, when they were part of attitude statements deemed unlikely by respondents (e.g., Q12) and we added emphasis to some of the statements on security practices to facilitate reading (e.g., Q17). The invitation e-mails were sent to eligible candidate respondents (see Section 4.1) through Ricardo’s newsletter service. The e-mail invited candidate respondents to participate in an online survey on security & privacy when buying used electronic storage devices. We mentioned the aim of our research and how eligible candidate respondents were selected. The respondents were offered a CHF 15 voucher for filling out a 20-minute-long survey (median completion time  $\approx$  26 minutes).

### 4.4 Data Analysis

We used descriptive analysis to report the outcome of the survey. For consistency, we define determiners-to-percentage mapping based on the frequency: *a few* for  $n = 2-5$  respondents, *several* for  $n = 6-10$  respondents, *some* for  $n = 11-15$  respondents, *about half* for  $n = 16-23$  respondents, *most* for  $n = 24-35$  respondents, *almost all* for  $n = 36-45$  respondents, and *all* for  $n = 46$  respondents.

### 4.5 Ethics

We debriefed our respondents at the end of the survey, to inform them about the security & privacy risks associated with second-hand storage devices (i.e., technical debriefing) and about their legal rights and obligations with regard to remnant data (i.e., legal debriefing). The debriefing content was simplified for conciseness. In particular, we offered general information about legal rights and obligations rather than individual legal recommendation. Because some of the legal conclusions were not necessarily moral or aligned with community norms (e.g., according to the law, buyers are allowed to keep the personal data of the sellers), we later contacted our respondents and clarified that: (1) the technical recommendation was provided by computer scientists, experts in security, and the legal recommendation provided by legal scholars experts in Swiss law, (2) the debriefing was kept simple for conciseness, the legal recommendation applies within Swiss jurisdictions and may not be valid in other jurisdictions, and that they can contact us for more complex cases, (3) some legal findings might not be in line with moral values and we encourage them to adopt a moral behavior even if they are not obliged to do so by law (e.g., to delete personal data left unintentionally). The debriefing and our message are available in [Supplementary 2](#) and [Supplementary 3](#), respectively.

Some questions in our survey asked the respondents to confess illegal activities (e.g., declaring activities related to data carving or having unlawfully processed data found on their storage device) they had done, if any. While collecting self-incriminating data is a common approach in some research topics (see, for example, intimate partner violence [15], cyberbullying [23], and coercive sexting [33]) it can subject research participants to risk. To protect our participants, we ensured not to be subject to any obligation to report a criminal offense and anonymized the data in order to not be able to re-identify the respondents. We also used forgiving and familiar wording in the survey to normalize the behaviors that might not be socially desirable. However, we did not learn of any illegal activity after data collection. Having said that, we should note that researchers in Switzerland are *generally* not required to report illegal activities to the authorities. We used some personal information such as the title of the transactions/advertisements (e.g., “USB2.0-Stick32GB, rot”) to personalize the questionnaire, but we deleted them together with the unique survey link after data collection. The study was approved by our IRB.

### 4.6 Survey Limitations

Our sample size was relatively small compared with typical online surveys. Nonetheless, we believe our survey findings are valuable, as they were collected from the users who were *recent, actual* buyers of second-hand storage devices. As such, they have a higher ecological validity than the information we could have obtained

with generic respondents from crowdsourcing platforms. To mitigate the potential issues related to over-representation, we reported the actual number of responses alongside the percentages. Furthermore, the population of our respondents consisted mostly of males over the age of 50. In terms of gender, our sample is roughly representative of the Ricardo’s customers for the considered products, however, we cannot assess it for age, as we do not have age information. Also, while Ricardo was an appropriate case study in Switzerland, future studies in different countries should take into account the platforms most used in those countries.

Given we used a survey for data collection, our methodology has a typical limitation of the self-report bias (see, e.g., self-report bias in security research [55]), where some respondents may not give truthful answers, particularly for some of the sensitive questions (e.g., those related to RQ1 and RQ3). To alleviate this problem, first, we ensured our respondents that their data would be kept private and anonymized (see Section 4.5). Second, we combined different approaches for screening respondents [39], before data analysis. We checked the response quality to ensure we did not have *speeders* or *straightliners* among the respondents. We also checked the quality of open-ended answers to ensure that all respondents provided *meaningful* responses. However, our results should be taken cautiously as some respondents may not disclose all information about their experiences with remnant data. Also, we used hypothetical scenarios to collect the respondents’ attitudes toward remnant data in part of the survey (see Section 5.3).

Finally, we have focused on the latest purchase of each respondent and studied average buyers who mostly purchased once or twice. The respondents might have found data on the other devices they purchased and that we did not investigate those events. Future work should also study (frequent) buyers who might be curiously or maliciously inspecting remnant data.

## 4.7 General Statistics

A total of 46 respondents completed the survey, corresponding to a 9.7% response rate. Respondents were predominantly men (91.3%,  $n = 42$ ). Only 4.3% ( $n = 2$ ) were women and 4.3% ( $n = 2$ ) preferred not to specify their gender. Male buyers make up a similarly high proportion in the set of eligible transactions (85%), as well as in the entire set of relevant transactions recorded over the reference period (86%). More than half of the respondents were aged 50 or older. The following summarizes the age distribution: 18–20 (4.3%,  $n = 2$ ), 21–29 (4.3%,  $n = 2$ ), 30–39 (15.2%,  $n = 7$ ), 40–49 (23.9%,  $n = 11$ ), 50–59 (26.1%,  $n = 12$ ), and 60+ (26.1%,  $n = 12$ ).<sup>45</sup>

Respondents’ level of privacy concerns (measured by UIIPC) was 5.0 (SD=1.6), thus indicating that our respondents’ general level of privacy concerns was relatively high. Regarding security practices (see Section 4.2-Sec. F), our respondents’ scores on security behavior intentions was better than the average for SeBIS [13].

Only 6.5% ( $n = 3$ ) of the respondents answered that they would *often* or *always* plug USB sticks that they find into their electronic devices (Q17-S5) and 10.8% ( $n = 5$ ) mentioned ‘sometimes.’ These *self-reported* attitudes seem to be at odds with the *observed* behavior of Tischer et al. [53], where a much larger number plugged in the

USB sticks they found. This discrepancy could be explained by the privacy paradox [3], in which users state being worried about their privacy but take relatively little action to preserve it.<sup>46</sup> However, when we asked the respondents if they would plug USB sticks given by their family, friends, or colleagues (Q17-S6), a relatively higher number answered positively: 36.9% ( $n = 17$ ) *often* or *always* and 39.1% ( $n = 18$ ) *sometimes*.

## 5 FINDINGS

### 5.1 Security Knowledge

We assessed the respondents’ awareness and knowledge of security & privacy risks related to second-hand storage devices, and of techniques for mitigating such risks (see 4.2-Sec. A). Figures 1a and 1b depict the respondents’ responses to the true (top) and false (bottom) statements, respectively. Correctly, almost all respondents agreed that plugging a USB stick into a computer can enable malware (84.8%,  $n = 39$ ). However, about half of the respondents agreed that it could also *physically damage* the computer (e.g., USB Killer)<sup>47</sup>. Also almost all correctly understood that data can be recovered from a device even after the trash bin has been emptied (84.8%,  $n = 39$ ) or most of the respondents understood that data can be recovered even if the device has been formatted (71.7%,  $n = 33$ ), that antivirus programs can scan both internal and external drives (82.6%,  $n = 38$ ), and that fully erasing all data from a storage device is still technically possible (78.2%,  $n = 36$ ). Mistakenly, about half of the respondents (45.6%,  $n = 21$ ) thought that pressing a powerful magnet on a USB stick could erase it; this shows that a considerable proportion of respondents are not aware of—or do not understand—the technology used in USB sticks (i.e., flash memory, not magnetic disk). In summary, our respondents had a good level of awareness.

### 5.2 Experience

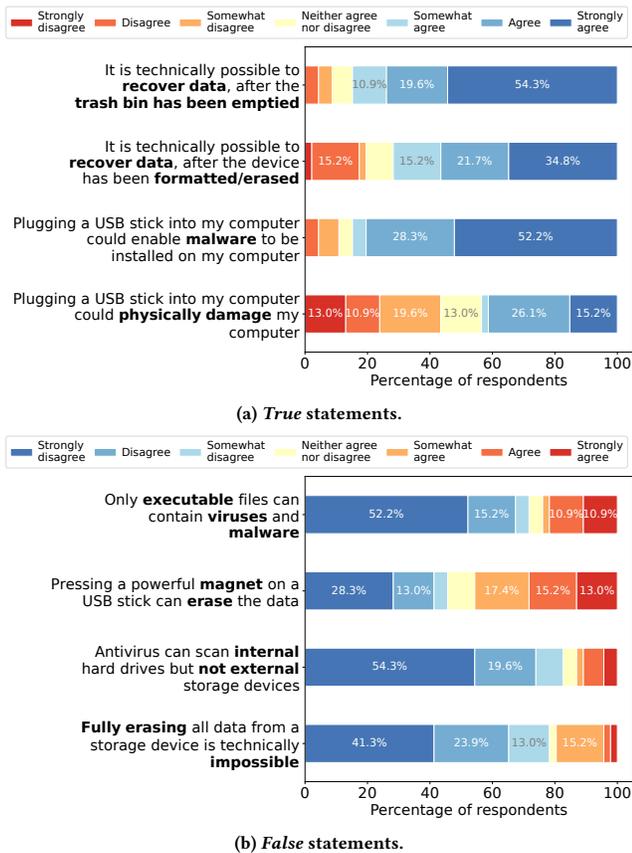
Our respondents reported scant actual experiences with data found after buying second-hand storage devices (see 4.2-Sec. B).<sup>48</sup> Indeed, 58.7% ( $n = 27$ ) indicated they did not find any data, 34.8% ( $n = 16$ ) that they did not check whether the device contained data (e.g., they formatted it right away without checking), and 4.3% ( $n = 2$ ) did not recollect whether they found any data. This shows that **although the privacy risks associated with remnant data is real, as demonstrated by previous work, it does not seem to materialize, in our setup at least (self-reported data about last purchase for a small sample in Switzerland)**. Note that our results focus more on “accidental” materialization (i.e., buyers finding data by accident) rather than on “intentional” materialization (buyers purchasing devices with the goal of finding and exploiting remnant data). Note also that users who bought devices intending to search for remnant data would opt out of responding. Only one respondent (2.2%,  $n = 1$ ) reported finding data, described as “*typical files one would find even on a new storage device.*” (e.g., device documentation in PDF). This respondent reported keeping the data, not using it, and not notifying anyone about it. Almost all respondents

<sup>45</sup>We do not have the age information of the customers for eligible (and ineligible) transactions who did not take our survey.

<sup>46</sup>Note that this is an hypothesis, it is not supported by the findings of this study, and it would require to be tested by future studies.

<sup>47</sup>[https://en.wikipedia.org/wiki/USB\\_Killer](https://en.wikipedia.org/wiki/USB_Killer).

<sup>48</sup>Note that the questions were asked about their *most recent purchase*; thus, they might have found data in previous purchases.



**Figure 1: Respondents' knowledge regarding data-deletion and data-security risks.**

(87.0%,  $n = 40$ ) indicated that their computer was not infected by any malware from the device they bought. The remaining were unsure or did not remember. It is important to note that detecting malware is challenging and buyers might fail to detect one (false negative).

These findings might be due to the precautionary measures adopted by the respondents, where formatting or erasing was by far the most favorite option, as shown in Figure 4 (see Appendix E). Yet, as only 13.0% ( $n = 6$ ) of the respondents scanned the purchased storage device with anti-virus software, those who did not use the anti-virus could have been infected by a malware contained on the device after they plugged it in and before they formatted it. Interestingly, some respondents also reported plugging the purchased device into a secondary computer with no or little sensitive data or that they would not be missed if damaged. Others mentioned they believed the device they had purchased was new or unused.

### 5.3 Attitudes Regarding Remnant Data

We present our findings about the respondents' attitudes to hypothetical scenarios involving remnant data (see 4.2-Sec. C). Figure 2 shows seven courses of action for the nine data types.

We first focus on two actions: deleting data and using data. When considering the option of deleting the remnant data, despite the lack of legal obligations, almost all respondents indicated they would more likely delete banal data, such as regular photos of nature landscapes (93.5% or  $n = 43$ , moderately or extremely likely). In the case of sensitive-data types, including private photos (e.g., depicting people being naked), confidential data (e.g., bank statements, work contracts, pay slips), credentials, passwords, and personal information related to other identified individuals, most respondents (at least 69.6% or  $n = 32$ ) would be extremely likely to delete the data. This is indeed a safer strategy as Swiss law limits the use of data that is not intrinsically illegal but whose usage can be punishable by law. However, a few respondents (10.9% or  $n = 5$ ) also reported their intention to not delete such data. This minority population was even larger (15.2–26.1% or  $n = 7$ –12) in the scenarios where the remnant data was redeemable financial data or data related to an identified organization. Such users could be held liable if they sell or misuse the data. In the case of data providing evidence of illegal activities or illegal content, more than two-thirds of respondents indicated they would not delete data. We elaborate on this somewhat surprising result below.

As for using the remnant data, regardless of the data type, most respondents (at least 73.9% or  $n = 34$ ) indicated they would not use the data. The exceptions were for the most problematic data types: evidence of illegal activities and illegal content, where more respondents reported they would use the data. Presumably, these respondents intended to use such data (i.e., open it or watch it to understand the content) to report it to competent authorities. The following findings shed more light on this.

We analyzed the respondents' attitudes toward notifying five types of entities for five data types. The respondents reported they would notify different entities based on data types: For data types such as redeemable financial data, credentials, passwords, and confidential data disclosing information about the seller, most respondents reported they would likely notify the seller ( $\approx 60$ –70%). There was slightly less agreement ( $\approx 46$ –54%) about notifying the seller about innocuous data such as regular photos, and even about more problematic data-types that could either be embarrassing (e.g., sensitive private photos) or could entail a certain liability (e.g., data related to an organization or to another individual). In contrast, for data representing illegal activities or illegal content, almost all respondents ( $\approx 93$ –98%) would not contact the seller, rather they would notify competent authorities—as encouraged by Swiss law.

When asked whether they would notify an identified (third-party) individual concerned by the data found, almost half of the respondents indicated that this would be extremely unlikely. Redeemable financial data elicited the highest likelihood of contacting a third-party individual (21.8% or  $n = 10$ , extremely likely). Similar attitudes were recorded when respondents were given the option to contact an identified organization concerned by the remnant data. Only several respondents were extremely likely to use this option. This is surprising as, according to Swiss law, the data controllers must inform the data subjects. Regarding the most common data types, when asked whether they would notify the platform, between half and two-thirds of the respondents were reticent to do so; with the exception of evidence of illegal activities and illegal content. 32.6% ( $n = 15$ ) and 39.1% ( $n = 18$ ) of the respondents mentioned

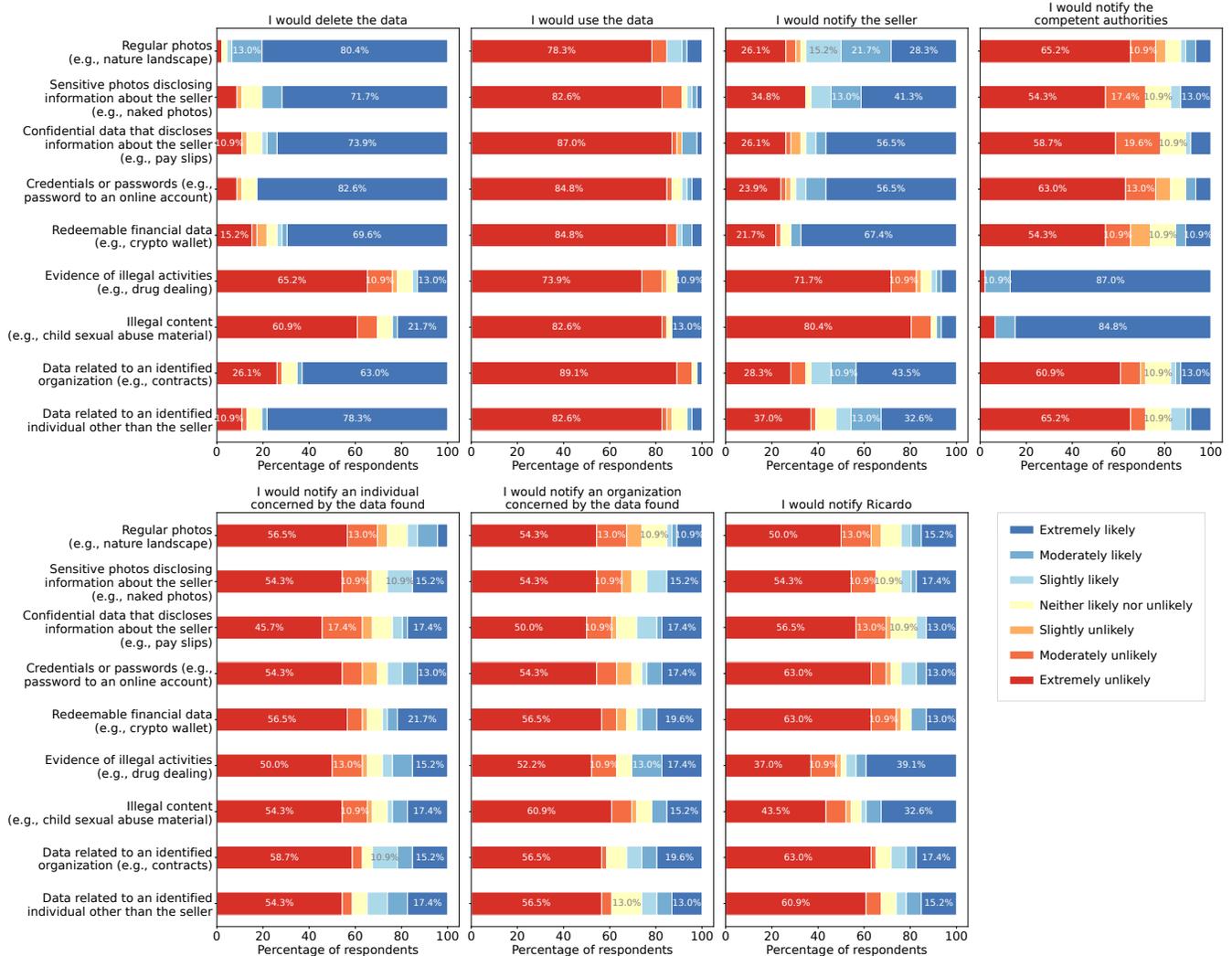


Figure 2: Respondents' general attitudes toward remnant data if they found it on the second-hand storage devices they purchased: use and deletion of the data and notification of relevant entities.

they would *extremely likely* contact the platform if they found illegal content or evidence of illegal activities. This highlights the potential interest in enabling such functionality (see Appendices F and G for potential associations between different attitudes).

#### 5.4 Beliefs about Legal Rights and Obligations

We present our findings with regard to the respondents' beliefs about their legal rights and obligations when they purchase second-hand storage devices. We split the "true" and "false" statements<sup>49</sup> and showed them in Figures 3a and 3b, respectively. For *true* statements, correct answers are colored in blue, corresponding to *somewhat agree*, *agree*, and *strongly agree*. For *false* statements, correct answers are colored in blue, corresponding to *somewhat disagree*, *disagree*, and *strongly disagree*. The statements are coded with numbers in the figures to be referred to in the following paragraphs and in Q13 in Appendix D (denoted with 'L').

<sup>49</sup>For some of the statements, the truth is in fact more nuanced and context dependent.

First, we discuss results related to users' *general* perceptions of rights and obligations. Almost all respondents (80.4%,  $n = 37$ ) ascertained correctly that if they found data from the seller on a used device they bought, they could not consider that the seller had left data willingly for them to use (L15). However, responses varied widely when asked if the buyer had a *legal obligation* to notify the seller (L17), an identified organization (L16), or an identified individual (L18). Only  $\approx 33\text{--}39\%$  ( $n = 15\text{--}18$ ) of the individuals knew for certain (i.e., strongly disagree and disagree) that they are not obliged to notify these entities. Most respondents (52%,  $n = 24$ ) knew that they are legally obliged to delete data if they are asked to do so by the seller (L7). In summary, **respondents hold the belief that remnant data is probably the result of forgetfulness. Some mistakenly think that they are obliged to inform sellers but that they do not need to comply with the seller's request to delete the data.**

Only several respondents (21.8%,  $n = 10$ ) knew that the seller can be held liable if the device contains malware (L4). About 21.8% ( $n = 10$ ) mistakenly thought that the platform can be held liable for malware (L21); this is false. **Therefore, in the malware infection case, it seems users do not have enough information about who can be held responsible.** Almost all respondents (78.3%,  $n = 36$ ) correctly believed that they do not have the right to use specialized software to gain access to data that has been encrypted or password-protected by the seller (L13). However, about half of the respondents (43.5%,  $n = 20$ ) knew that using forensic techniques to access previously deleted data is illegal (L14). Both of these statements are false if the intention is to recover data against the will of the seller. **Therefore, it seems necessary to remind buyers that they are not allowed to use carving or other forensic techniques on purchased devices.**

The rest of the legal questions targeted specific data types that we present below. In the event of finding **evidence of illegal activities** and/or **illegal content, such as child sexual abuse material**, almost all respondents ( $\approx 80\%$ ,  $n = 37-38$ ) were convinced they had the legal obligation to report it to the competent authorities (L19 & L20); whereas, in fact, they do not. Noticeably, about 43.5% ( $n = 20$ ) of them failed to anticipate that they could be held liable if they do not delete such data (L2). The relationship between the deletion of child sexual abuse material and its reporting is evident. As seen in Section 5.3, buyers might choose to keep such problematic data with the intention of reporting it to the competent authorities, which is not inherently illegal. If buyers believe reporting is mandatory and are willing to comply, authorities would likely provide guidance on whether to delete the material. This approach ensures that buyers ultimately align their actions with legal requirements, even if they were initially unaware of potential liabilities associated with mere possession.

Regarding personal use of the seller's **nude photos** (L1), most respondents (76.1%,  $n = 35$ ) mistakenly believed that such data could not be legally kept and used by the buyer. It could be interpreted that, in the absence of legal knowledge, respondents make use of their common sense and general appreciation of right and wrong (or empathy) to establish whether they are legally entitled to do something. For the same data-type (personal nude photos), most respondents (54.3%,  $n = 25$ ) truly believed that the seller could be held liable if the seller did not delete the data that **belonged to a third-party individual**, such as the seller's partner (L5). However, they disagreed that the seller could be held liable for the same event, in case if they did delete the data (L6). Thus, they believed the seller could be held liable **in one case but not in the other**. Most respondents (76%,  $n = 35$ ) correctly ascertained that **recovered data related to an identified organization** could not be sold legally (L9). There was no clear trend about whether **remnant purchased songs, movies, and software** could be kept and used personally (L3). However, most respondents (67.4%,  $n = 31$ ) correctly identified that they were not legally entitled to post on social media **any original nature landscape photos** found on the purchased device (L8). Almost all respondents also had similar correct beliefs with regard to not being entitled to use **credentials** (L10: 91.3%,  $n = 42$ ), to publish a **book** (L11: 89.1%,  $n = 41$ ), and to cash **redeemable financial data** (L12: 91.3%,  $n = 42$ ).

## 5.5 Expectations

30.4% ( $n = 14$ ) of the respondents indicated that, when they completed the specific transaction, they would have liked to receive from the platform more information on the *legal* aspects of transactions such as rights, obligations, and liabilities. 30.4% ( $n = 14$ ) would have liked to have more information on the *technical* aspects of transactions, such as security and privacy risks. The respondents (buyers) reported several takeaways from answering the questionnaire: avoid connecting the purchased storage device directly to their main computer, inform themselves about the related rights and obligations, and use an antivirus program. **Thus, providing buyers with a reminder of the security risks and solutions, as well as their legal rights and obligations, was deemed useful by the respondents.**

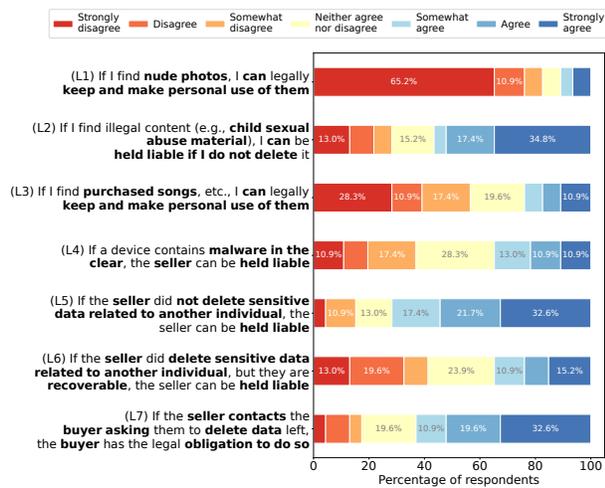
## 6 DISCUSSION

We found that, in general, buyers tend to delete remnant data; but, some keep sensitive data (see RQ1). The buyers believe they can notify others about the remnant data they find. In particular, if the data is sensitive, many users are inclined to notify the sellers and to notify authorities if the data contains any illegal content or evidence of illegal activities. Our respondents were well aware of security risks and solutions (see RQ2). They reported, taking some precautions such as formatting their device, plugging it into a secondary computer, and/or using antivirus software. As a plausible result of taking these precautions and/or not actively looking for data (or simply the absence of threat on the device), they reported very few incidents where they found any data (see RQ3). We collected insights into buyers' attitudes (i.e., how they would behave if they found any data).

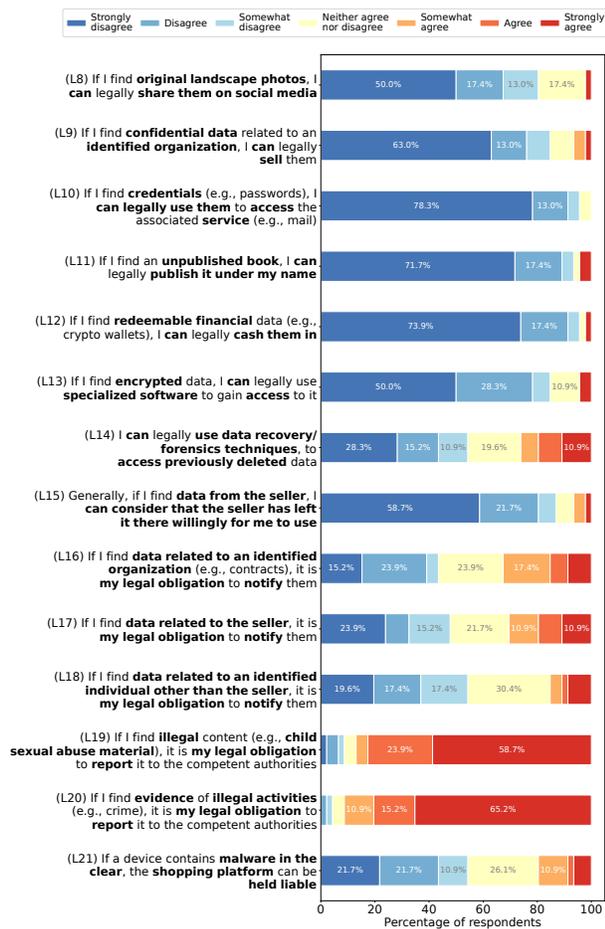
With regard to legal rights and obligations (see RQ4), we identified several regulations that are not well-known by buyers of second-hand storage devices and that could lead to misunderstandings. For instance, buyers do not have any legal obligation to report to other entities about the remnant data. Our respondents, however, thought otherwise. Although there is a mismatch between applicable regulations and users' beliefs, this could be helpful for both buyers and sellers, where most buyers, altruistically, can take more responsibility. Perhaps, the hazardous mismatch was related to data with illegal content, where buyers thought they could keep such data on their devices. Whereas, they could be held liable if they do not immediately delete it or report it to the competent authorities.

Some findings show users behave in common-sense ways. But they are still insightful. For instance, keeping illegal content (e.g., child sexual abuse material) to report to the authorities is common sense. But so is deleting it to avoid liability. Our results show that between these two approaches, the vast majority of users take the first. Our findings call for informing users about the risks and educating them about precautions and their legal rights and obligations.

Our findings revealed that the risks rarely materialize in practice (at least from what we could observe in our data): a finding that puts in perspective the results from the current forensic literature, which shows that privacy and security risks are widespread. Despite this scarcity, the problem of remnant data left in second-hand storage devices is still significant and should be addressed seriously. Even if buyers do not often find data (or even look for it), incidents



(a) True statements.



(b) False statements.

Figure 3: Buyers’ beliefs about the legal rights and obligations associated with transactions of second-hand devices.

involving a small number of users can have serious privacy and security consequences. The problem can be even more serious for businesses and government organizations, where a single storage device can include information about millions of users, and the remnant data can cause harm on a large scale. For example, a security researcher recently purchased a fingerprint and iris scanning device on eBay—originally owned by the U.S. military [22]. The device’s memory card contained information on more than 2000 wanted people, including their names, nationalities, photographs, fingerprints, and iris scans. Our study calls for future interventions, for the prevention and/or reduction of the frequency of incidents with regard to remnant data. In the future, we intend to collaborate closely with online platforms in order to develop practical solutions and to assess how well they mitigate potential security and privacy issues associated with the transactions of used products.

## 7 FUTURE WORK

We intend to conduct additional experiments to identify and poll buyers who *do* check storage devices for remnant data about their actual *behavior*. For this, we envision a methodology similar to that of Tischer et al. [53], that is, selling second-hand devices with remnant data and either detect automatically if they are accessed (e.g., HTML files embedding subresources located on servers we control, vouchers for which we are notified when they are cashed) or include a message in these files asking the buyer to contact us for a (paid) survey/interview. Future work should also consider other legal systems and study users who contemplate selling or buying storage devices but who do not do so due to security and/or privacy concerns. Understanding users’ concerns and their security mental models can help us develop a sustainable solution for users to recycle their unused devices, in a safe and secure manner. Moreover, to understand the discrepancies between sellers’ and buyers’ beliefs about their rights and obligations, future studies should investigate the legal beliefs of sellers of second-hand storage devices. This could inform designers of special advice or caution should be provided, depending on the user’s role in the transaction. Future studies should also design solutions for raising awareness among all users and for evaluating their effectiveness (e.g., using A/B testing).

## 8 CONCLUSION

We have contributed to the research on the security and privacy of used or shared devices. By conducting an online survey with buyers of second-hand storage devices, we have gained valuable insights into the buyers’ knowledge, behaviors, attitudes, and beliefs about their legal rights and obligations. We have also provided a legal foundation to benefit buyers, sellers, platform operators, and third-party individuals and organizations. Furthermore, we shed light on different courses of action that buyers can take toward different data types and highlighted the discrepancies between users’ beliefs and legal requirements. These findings have implications for developing effective guidelines for the responsible use of second-hand storage devices and highlight the importance of raising awareness about the risks and responsibilities. Given the environmental benefits of second-hand transactions, it would be unfortunate if privacy and security issues impede the market’s growth.

## **ACKNOWLEDGMENTS**

We thank Holly Cogliati for her great editing job and Eoghan Casey and Thomas Souvignet for their insightful feedback in the early stages of the project. We express our thanks to Bente Lowin Kropf and Alain Mermoud for their kind assistance in proofreading the survey. We thank Valentin Mulder for participating in the cognitive pre-tests for the survey. We are very grateful to Aurelia Jaquier and Niccolo Piombanti from Ricardo for their tremendous help in collecting data. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

## REFERENCES

- [1] Olga Angelopoulou, Andy Jones, Graeme Horsman, and Seyedali Pourmoafi. 2022. A Study of the Data Remaining on Second-Hand Mobile Devices in the UK (2022).
- [2] Olga Angelopoulou, Andrew Jones, Vidalis Stilianos, and Helge Janicke. 2017. The 2016 Hard Disk Study on Information Available on the Second Hand Market in the UK. In *European Conference on Cyber Warfare and Security (ECCWS)*. Elsevier BV, Dublin, Ireland, 193–199.
- [3] Susanne Barth and Menno D. T. de Jong. 2017. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics* 34, 7 (Nov. 2017), 1038–1058. <https://doi.org/10.1016/j.tele.2017.04.013>
- [4] Oussama BenRhouma, Ali AlZahrani, Ahmad AlKhodre, Abdallah Namoun, and Wasim Ahmad Bhat. 2021. To sell, or not to sell: social media data-breach in second-hand Android devices. *Information & Computer Security* 30, 1 (Jan. 2021), 117–136. <https://doi.org/10.1108/ICS-03-2021-0038> Publisher: Emerald Publishing Limited.
- [5] Gergely Biczók and Pern Hui Chia. 2013. Interdependent Privacy: Let Me Share Your Data. In *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, Ahmad-Reza Sadeghi (Ed.). Springer, Berlin, Heidelberg, 338–353. [https://doi.org/10.1007/978-3-642-39884-1\\_29](https://doi.org/10.1007/978-3-642-39884-1_29)
- [6] Sirapat Boonkroong and Tongpool Heeptaisong. 2022. INVESTIGATION OF RESIDUAL DATA ON SECOND HAND SMART PHONES. 29, 4 (2022).
- [7] Brian Carrier. 2005. *File system forensic analysis*. Addison-Wesley, Boston, Mass.; London. OCLC: ocm57751590.
- [8] Jason Ceci, Hassan Khan, Urs Hengartner, and Daniel Vogel. 2021. Concerned but Ineffective: User Perceptions, Methods, and Challenges when Sanitizing Old Devices for Disposal. In *Proc. of the Symp. on Usable Privacy and Security (SOUPS)*, 455–474. <https://www.usenix.org/conference/soups2021/presentation/ceci> USENIX.
- [9] Jason Ceci, Jonah Stegman, and Hassan Khan. 2023. No Privacy in the Electronics Repair Industry. In *Proc. of the IEEE Symp. on Security and Privacy (S&P)*. IEEE, San Francisco, CA, USA, 3347–3364. <https://doi.org/10.1109/SP46215.2023.10179413>
- [10] Mauro Cherubini, Kavous Salehzadeh Niksirat, Marc-Olivier Boldi, Henri Keopraseuth, Jose M. Such, and Kévin Huguenin. 2021. When Forcing Collaboration is the Most Sensible Choice: Desirability of Precautionary and Dissuasive Mechanisms to Manage Multiparty Privacy Conflicts. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 53:1–53:36. <https://doi.org/10.1145/3449127>
- [11] James Conacher, Karen Renaud, and Jacques Ophoff. 2020. Caveat Venditor, Used USB Drive Owner. *SSRN Electronic Journal* (2020). <https://doi.org/10.2139/ssrn.3631441>
- [12] S. Diesburg, C. A. Feldhaus, M. Al Fardan, J. Schlicht, and N. Ploof. 2016. Is your data gone?: measuring user perceptions of deletion. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. ACM, Los Angeles California, 47–59. <https://doi.org/10.1145/3046055.3046057>
- [13] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. <https://doi.org/10.1145/2702123.2702249>
- [14] John C. Flanagan. 1954. The critical incident technique. *Psychological Bulletin* 51 (1954), 327–358. <https://doi.org/10.1037/h0061470> Place: US Publisher: American Psychological Association.
- [15] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. “A Stalker’s Paradise”: How Intimate Partner Abusers Exploit Technology. In *Proc. of the ACM Conf. on Human Factors in Computing Systems (CHI) (CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. <https://doi.org/10.1145/3173574.3174241>
- [16] Alisa Frik, Juliann Kim, Joshua Rafael Sanchez, and Joanne Ma. 2022. Users’ Expectations About and Use of Smartphone Privacy and Security Settings. In *Proc. of the ACM Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, New York, NY, USA, 1–24. <https://doi.org/10.1145/3491102.3517504>
- [17] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce S Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proc. of the USENIX Security Symposium (Sec)*. USENIX, Santa Clara, CA, 21.
- [18] S.L. Garfinkel and A. Shelat. 2003. Remembrance of data passed: a study of disk sanitization practices. *IEEE Security & Privacy* 1, 1 (Jan. 2003), 17–27. <https://doi.org/10.1109/MSECP.2003.1176992>
- [19] William Glisson, Tim Storer, Andrew Blyth, George Grispos, and Matt Campbell. 2016. In-The-Wild Residual Data Research and Privacy. *Journal of Digital Forensics, Security and Law* 11, 1 (2016), Article 1. <https://doi.org/10.15394/jdfsl.2016.1371>
- [20] William Bradley Glisson, Tim Storer, Gavin Mayall, Iain Moug, and George Grispos. 2011. Electronic retention: what does your mobile phone reveal about you? *International Journal of Information Security* 10, 6 (Nov. 2011), 337–349. <https://doi.org/10.1007/s10207-011-0144-3>
- [21] Andreas Gutmann and Mark Warner. 2019. Fight to Be Forgotten: Exploring the Efficacy of Data Erasure in Popular Operating Systems. In *Privacy Technologies and Policy : 7th Annual Privacy Forum (Lecture Notes in Computer Science)*, Maurizio Naldi, Giuseppe F. Italiano, Kai Rannenberg, Manel Medina, and Athena Bourka (Eds.). Springer International Publishing, Rome, 45–58. [https://doi.org/10.1007/978-3-030-21752-5\\_4](https://doi.org/10.1007/978-3-030-21752-5_4)
- [22] Kashmir Hill, John Ismay, Christopher F. Schuetz, and Aaron Krolik. 2022. For Sale on eBay: A Military Database of Fingerprints and Iris Scans. *The New York Times* (Dec. 2022). <https://www.nytimes.com/2022/12/27/technology/for-sale-on-ebay-a-military-database-of-fingerprints-and-iris-scans.html>
- [23] Sameer Hinduja and Justin W. Patchin. 2022. Bias-Based Cyberbullying Among Early Adolescents: Associations With Cognitive and Affective Empathy. *The Journal of Early Adolescence* 42, 9 (Nov. 2022), 1204–1235. <https://doi.org/10.1177/02724316221088757> Publisher: SAGE Publications Inc.
- [24] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A Survey on Interdependent Privacy. *Comput. Surveys* 52, 6 (2019), 40. <https://doi.org/10.1145/3360498>
- [25] Andy Jones, Olga Angelopoulou, and Len Noriega. 2019. Survey of data remaining on second hand memory cards in the UK. *Computers & Security* 84 (July 2019), 239–243. <https://doi.org/10.1016/j.cose.2019.03.006>
- [26] Andy Jones, Thomas Martin, and Mohammed Alzaabi. 2012. The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE. In *Proceedings of the 10th Australian Digital Forensics Conference*. Perth, Western Australia. <https://doi.org/10.4225/75/57b3b239fb863>
- [27] Andrew Jones, Vivienne Mee, Christopher Meyler, and Joanna Gooch. 2005. Analysis of Data Recovered from Computer Disks released for Resale by Organisations. *Journal of Information Warfare* 4, 2 (2005), 45–53. <https://www.jstor.org/stable/26504063> Publisher: Peregrine Technical Solutions.
- [28] Andy Jones, Craig Valli, and G. Dabibi. 2009. The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market. In *Proceedings of the 7th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University. <https://doi.org/10.4225/75/57B2836B40CCA>
- [29] Andy Jones, Craig Valli, Glenn Dardick, and Iain Sutherland. 2008. The 2007 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. *Journal of Digital Forensics, Security and Law* 3, 1 (2008), Article 1. <https://doi.org/10.15394/jdfsl.2008.1034>
- [30] Andy Jones, Craig Valli, Glenn S. Dardick, Iain Sutherland, G. Dabibi, and Gareth Davis. 2010. The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. In *Proceedings of the 8th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University. <https://doi.org/10.4225/75/57B2968040CDD>
- [31] Andy Jones, Craig Valli, Gareth Davies, Glenn Dardick, and Iain Sutherland. 2009. The 2008 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. *Journal of International Commercial Law and Technology* 4, 3 (July 2009), 162–175. [https://www.researchgate.net/publication/26627736\\_The\\_2008\\_Analysis\\_of\\_Information\\_Remaining\\_on\\_Disks\\_Offered\\_for\\_Sale\\_on\\_the\\_Second\\_Hand\\_Market](https://www.researchgate.net/publication/26627736_The_2008_Analysis_of_Information_Remaining_on_Disks_Offered_for_Sale_on_the_Second_Hand_Market)
- [32] Andy Jones, Craig Valli, Iain Sutherland, and Paula Thomas. 2006. The 2006 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market. *Journal of Digital Forensics, Security and Law* 1, 3 (2006), Article 2. <https://doi.org/10.15394/jdfsl.2006.1008>
- [33] Poco D. Kernsmith, Bryan G. Victor, and Joanne P. Smith-Darden. 2018. Online, Offline, and Over the Line: Coercive Sexting Among Adolescent Dating Partners. *Youth & Society* 50, 7 (Oct. 2018), 891–904. <https://doi.org/10.1177/0044118X18764040> Publisher: SAGE Publications Inc.
- [34] Barbara Krumay. 2016. The E-Waste-Privacy Challenge. In *Proc. of the Annual Privacy Forum (APF)*, Vol. 9857. Springer International Publishing, Cham, 48–68. [https://doi.org/10.1007/978-3-319-44760-5\\_4](https://doi.org/10.1007/978-3-319-44760-5_4)
- [35] Federica Laricchia. 2022. Recycling and reuse of consumer tech. <https://www.statista.com/topics/9540/recycling-and-reusage-of-consumer-tech/>
- [36] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15, 4 (Dec. 2004), 336–355. <https://doi.org/10.1287/isre.1040.0032> Publisher: INFORMS.
- [37] Shirang Mare, Franziska Roesner, and Tadayoshi Kohno. 2020. Smart Devices in Airbnbs: Considering Privacy and Security for both Guests and Hosts. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (April 2020), 436–458. <https://doi.org/10.2478/popets-2020-0035>
- [38] Thomas Martin, Andy Jones, and Mohammed Alzaabi. 2016. The 2016 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE. *Journal of Digital Forensics, Security and Law* 11, 4 (2016), Article 6. <https://doi.org/10.15394/jdfsl.2016.1428>
- [39] Tenga Matsuura, Ayako A. Hasegawa, Mitsuaki Akiyama, and Tatsuya Mori. 2021. Careless Participants Are Essential for Our Phishing Study: Understanding the Impact of Screening Methods. In *Proceedings of the European Symposium on Usable*

- Security (*EuroUSEC*) (*EuroUSEC '21*). Association for Computing Machinery, New York, NY, USA, 36–47. <https://doi.org/10.1145/3481357.3481515>
- [40] Taiwo Ojo, Hongmei Chi, Janei Elliston, and Kaushik Roy. 2022. Secondhand Smart IoT Devices Data Recovery and Digital Investigation. In *SoutheastCon 2022*. IEEE, Mobile, AL, USA, 640–648. <https://doi.org/10.1109/SoutheastCon48659.2022.9763996>
- [41] Chandrasekaran Padmavathy, Murali Swapana, and Justin Paul. 2019. Online second-hand shopping motivation – Conceptualization, scale development, and validation. *Journal of Retailing and Consumer Services* 51 (Nov. 2019), 19–32. <https://doi.org/10.1016/j.jretconser.2019.05.014>
- [42] Kopo Marvin Ramokapane, Awais Rashid, and Jose Miguel Such. 2017. "I feel stupid I can't delete." : A study of users' cloud deletion practices and coping strategies. In *Proc. of the Symp. on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA, 241–256. <https://www.usenix.org/legacy/events/fast05/tech/> OCLC: 931663505.
- [43] Richard Roberts, Julio Poveda, Raley Roberts, and Dave Levin. 2023. Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones. In *Proc. of the IEEE Symp. on Security and Privacy (S&P)*. IEEE, San Francisco, CA, USA, 3332–3336. <https://doi.org/10.1109/SP46215.2023.10179348>
- [44] Nikki Robins, Patricia A. H. Williams, and Krishnun Sansurooah. 2017. An investigation into remnant data on USB storage devices sold in Australia creating alarming concerns. *International Journal of Computers and Applications* 39, 2 (April 2017), 79–90. <https://doi.org/10.1080/1206212X.2017.1289689>
- [45] Krishnun Sansurooah. 2012. A study of remnant data found on usb storage devices offered for sale on the Australian second hand market in 2011. In *Proceedings of the 10th Australian Information Security Management Conference*. Edith Cowan University, Perth Western Australia, 83–91.
- [46] Janine Schneider, Immanuel Lautner, and Denise Moussa. 2021. In Search of Lost Data: A Study of Flash Sanitization Practices. In *Proceedings of the Digital Forensics Research Workshop Europe (DFRWS EU)*. Cyberspace, 11.
- [47] Rahul Anand Sharma, Elahe Soltanaghaei, Anthony Rowe, and Vyas Sekar. 2022. Lumos: Identifying and Localizing Diverse Hidden IoT Devices in an Unfamiliar Environment. In *Proc. of the USENIX Security Symposium (Sec)*. USENIX.
- [48] Iain Sutherland, Gareth Davies, Andy Jones, and Andrew J. C. Blyth. 2010. Zombie Hard disks - Data from the Living Dead. In *Proceedings of the 8th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University. <https://doi.org/10.4225/75/57B2B48D40CE3>
- [49] Patryk Szewczyk. 2011. Analysis of Data Remaining on Second Hand ADSL Routers. *Journal of Digital Forensics, Security and Law* (2011). <https://doi.org/10.15394/jdfsl.2011.1098>
- [50] Patryk Szewczyk, Nikki Robins, and Krishnun Sansurooah. 2013. Sellers Continue to Give Away Confidential Information on Second Hand Memory Cards Sold in Australia. In *Proceedings of the 11th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University. <https://doi.org/10.4225/75/57B3DAC1FB876>
- [51] Patryk Szewczyk and Krishnun Sansurooah. 2012. The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia. In *Proceedings of the 10th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University. <https://doi.org/10.4225/75/57B3D443FB870>
- [52] Patryk Szewczyk, Krishnun Sansurooah, and Patricia A. H. Williams. 2018. An Australian Longitudinal Study Into Remnant Data Recovered From Second-Hand Memory Cards. *International Journal of Information Security and Privacy* 12, 4 (Oct. 2018), 82–97. <https://doi.org/10.4018/IJISP.2018100106>
- [53] Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, and Michael Bailey. 2016. Users Really Do Plug in USB Drives They Find. In *Proc. of the IEEE Symp. on Security and Privacy (S&P)*. IEEE, San Jose, CA, 306–319. <https://doi.org/10.1109/SP.2016.26>
- [54] Craig Valli and Andrew Woodward. 2008. The 2008 Australian study of remnant data contained on 2nd hand hard disks: the saga continues. In *Proceedings of the 6th Australian Digital Forensics Conference*. Security Research Institute (SRI), Edith Cowan University, December 3rd 2008. <https://doi.org/10.4225/75/57B27F6840CC7>
- [55] Rick Wash, Emilee Rader, and Chris Fennell. 2017. Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. In *Proc. of the ACM Conf. on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery, New York, NY, USA, 2228–2232. <https://doi.org/10.1145/3025453.3025911>
- [56] Wikipedia. 2022. Circular economy. [https://en.wikipedia.org/w/index.php?title=Circular\\_economy&oldid=1122402696](https://en.wikipedia.org/w/index.php?title=Circular_economy&oldid=1122402696) Page Version ID: 1122402696.

## A RELATED WORK ON PRESENCE OF REMNANT DATA AND IMPLICATIONS

**Table 1: The list of works that investigated remnant data in second-hand devices. In the ‘device’ column, , , , and  indicate drives (HDD/SSD), USB sticks, memory cards, and portable devices (e.g., smartphone, tablet, laptop), respectively. To specify the types of remnant data, we used:  (‘data related to an identified organization’),  (‘data related to an identified individual’),  (‘regular photos’),  (‘sensitive photos’),  (‘credentials’),  (‘redeemable financial data’), and  (‘illegal content or evidence of illegal activities’). N refers to the number of devices/participants. n refers to the number of devices/participants with remnant data. The spreadsheet version of this table is available in [Supplementary 4](#).**

authors	year ▲	device	N	n	country							
Jones et al. [27]	2005		105	92	UK	✓	✓	-	-	✓	-	✓
Jones et al. [32]	2006		317	130	UK, US, AU, DE	✓	✓	✓	-	✓	✓	✓
Jones et al. [29]	2007		300	126	UK, US, AU, DE	✓	✓	-	✓	✓	✓	✓
Jones et al. [31]	2008		338	158	UK, US, AU, DE, FR	✓	✓	✓	✓	✓	✓	✓
Valli and Woodward [54]	2008		48	N/A	AU	✓	✓	-	-	✓	-	✓
Jones et al. [28]	2009		43	39	UK	✓	✓	✓	-	-	-	-
Jones et al. [30]	2009		346	163	UK, US, AU, DE, FR	✓	✓	-	-	✓	✓	✓
Sutherland et al. [48]	2010		32	5/7*	UK	✓	✓	-	-	✓	-	-
Glisson et al. [20]	2010		49	49	UK	✓	✓	✓	✓	-	✓	✓
Szewczyk [49]	2011		119	105	AU	✓	✓	✓	✓	✓	✓	✓
Sansurooah [45]	2011		80	64	AU	✓	✓	✓	-	✓	-	-
Jones et al. [26]	2012		45	30	UAE	✓	✓	✓	-	✓	-	-
Szewczyk and Sansurooah [51]	2012		78	55	AU	✓	✓	✓	✓	✓	✓	✓
Szewczyk et al. [50]	2013		140	102	AU	✓	✓	✓	✓	✓	-	✓
Szewczyk et al. [52]	2014-2015		268	255	AU	✓	✓	✓	✓	✓	✓	✓
Martin et al. [38]	2016		40	26	UAE	✓	✓	-	-	✓	✓	✓
Angelopoulou et al. [2]	2016		110	43	UK	✓	✓	✓	-	✓	-	-
Robins et al. [44]	2016		272	248	AU	✓	✓	✓	✓	✓	✓	✓
Angelopoulou et al. [1]	2018		100	70	UK	-	✓	✓	-	✓	✓	-
Jones et al. [25]	2019		100	71	UK	✓	✓	✓	✓	-	-	✓
Boonkroong and Heeptaisong [6]	2019		30	20	TH	-	✓	✓	✓	-	✓	✓
Conacher et al. [11]	2020		122	68	GB	✓	✓	✓	-	✓	-	-
Schneider et al. [46]	2021		614	75	CN	-	✓	✓	✓	-	-	-
Roberts et al. [43]	2023		228	61	US	✓	✓	✓	✓	✓	✓	✓
Ceci et al. [9]	2023		16	14	CA	-	✓	✓	✓	-	✓	-

\*Five out of seven repairable devices had remnant data.

## B BACKGROUND ON DATA RECOVERY

To explain how data could be recovered from second-hand storage devices, thus creating security and privacy issues, we provide some background about data deletion and recovery techniques. For consistency, we follow Gutmann and Warner’s definition of the terms ‘erase’ and ‘delete’, which defines ‘erase’ as “purposeful overwriting of data with other data – thus rendering it immediately irretrievable” and ‘delete’ as “data being *forgotten* by the operating system and being marked as available for overwrite”. In the case of ‘delete’, data can be retrieved, to a large extent, until it is overwritten. Data deletion includes different operations. The process behind these operations varies across systems. Yet, it generally consist in deleting only the *link* between a file’s metadata and its content stored in the allocation units of a storage device (e.g., when files are sent to the trash bin then emptied on a Windows operating system). Although this could be sufficient for the system to manage visible and deleted files, data might still be recoverable otherwise [7].

Easy-to-use and open-source forensic tools such as Autopsy<sup>50</sup> can restore the link between the content of a file and its metadata. Such tools also enable users (buyers) to perform advanced operations such as *carving*, that is the analysis of the unallocated space in search for known signatures to recover fragments of deleted files [7]. To reduce the chances of recovering files, *wiping* can be used. With this technique, every bit of the storage is zeroed-out, i.e., overwritten multiple times with zeroes. Wiping tools are largely available on modern operating systems, e.g., Windows, macOS.

## C BACKGROUND ON SWISS LAW

Switzerland is a federal state which follows the legal tradition known as “Civil Law” like the countries of the European Union, as opposed to the Anglo-Saxon conception of “Common Law.”<sup>51</sup> The latter is a system characterized by case law, that is law developed by judges through decisions of courts and similar tribunals.<sup>52</sup> In the “Civil Law” tradition, the jurisprudence is certainly important, but it is “only” an aid to interpretation.<sup>53</sup>

Civil law is defined by the fact that its core principles are codified into a referable system which serves as the primary source of law.<sup>54</sup> This is especially true in criminal law, which is the primary source of this legal analysis, since there can be no punishment without law.<sup>55</sup> Due to the special focus on the criminal implications, to determine the infractions, we use mainly the Swiss Criminal Code<sup>56</sup> and, to determine the legal proceedings, we use the Swiss Criminal Procedure Code.<sup>57</sup> We also refer to the legal literature and case

<sup>50</sup><https://www.autopsy.com/>

<sup>51</sup>Müller-Chen/Müller/Widmer Lüchinger, Comparative Private Law, Zurich/St.Gallen 2015, p. 149, 207.

<sup>52</sup>Müller-Chen/Müller/Widmer Lüchinger, Comparative Private Law, Zurich/St.Gallen 2015, p. 223 ss; Fallon-Kund, Zum Einfluss von Kultur- und Sozialnormen auf das Recht, Geneva - Zurich - Basel 2015, p. 78.

<sup>53</sup>Swiss Civil Code of 10 December 1907 (RS 210) states that “the court shall follow established doctrine and case law” (Art. 2).

<sup>54</sup>Müller-Chen/Müller/Widmer Lüchinger, Comparative Private Law, Zurich/St.Gallen 2015, p. 154 ss.

<sup>55</sup>Also known by the Latin adage “nulla poena sine legem” and which also appears in Art. 7 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950 (ECHR).

<sup>56</sup>Swiss Criminal Code of 21 December 1937 (SCC; RS 311.0).

<sup>57</sup>Swiss Criminal Procedure Code of 5 October 2007 (CrimPC; RS 312.0).

laws whenever relevant. Regarding data protection, the FADP<sup>58</sup> is the major piece of legislation in Switzerland.

## D SURVEY QUESTIONNAIRE

Below, we provide the full transcript of the survey questionnaire. In order to avoid leading questions, we (i) used skip logic/coding rules, (ii) used unbiased language and statements, and (iii) did not make any assumptions in the questions.

Note: Coding rules are marked in gray (not visible to respondents)

### Sec. A: Security Knowledge

The following questions relate to buying second-hand electronic storage devices in **general** (hard drives, USB sticks, or memory cards).

Some of these questions concern your knowledge of specific technologies; please **remember that remuneration IS NOT dependent on your knowledge**. So, please answer based on your **current** knowledge (e.g., do not look for the correct answer online).

- (1) [Grid question. Row order randomized.] To what extent do you **agree or disagree** with the following statements?

Row options:

- It is technically possible (by using simple software readily available on the Internet) to **recover data** from a storage device, after the data has been sent to the trash bin and the **trash bin has been emptied**
- It is technically possible (by using simple software readily available on the Internet) to **recover data** from a storage device, after the device has been **formatted/erased** with the standard procedure
- Only **executable** files (e.g., programs, scripts) can contain **viruses** and **malware**
- Pressing a powerful **magnet** on a USB stick can **erase** the data it contains

- (a) Strongly disagree
- (b) Disagree
- (c) Somewhat disagree
- (d) Neither agree nor disagree
- (e) Somewhat agree
- (f) Agree
- (g) Strongly agree

- (2) [Grid question. Row order randomized.] To what extent do you **agree or disagree** with the following statements?

Row options:

- Plugging a USB stick into my computer could enable **malware** (i.e., a malicious software designed to cause harm) to be automatically installed on my computer
- Plugging a USB stick into my computer could **physically damage** my computer
- Antivirus software can scan **internal** hard drives but **not external** storage devices (external hard drives, memory cards, and USB sticks)
- **Fully erasing** all data from an electronic storage device (i.e., without someone being able to recover them) is technically **impossible**

- (a) Strongly disagree
- (b) Disagree
- (c) Somewhat disagree
- (d) Neither agree nor disagree
- (e) Somewhat agree
- (f) Agree
- (g) Strongly agree

### Sec. B: Experience

The following questions relate **specifically** to your experience when you bought online the storage device \$DeviceName on Ricardo.ch, on \$TransactionDate.

- (3) When you plugged the device you bought, did you find any data on it?

<sup>58</sup>Federal Act on Data Protection of 25 September 2020 (FADP; RS 235.1).

- (a) Yes
- (b) No
- (c) I do not remember
- (d) I did not check

[Display Q4 and Q5 if Q3\$Yes]

- (4) [Multiple selection. Order randomized.] What types of data did you find? (select all that apply)
- (a) Regular photos (e.g., photos of nature landscape)
  - (b) Sensitive private photos that disclose information about the seller (e.g., photos picturing the seller or one of their contacts being naked)
  - (c) Confidential data that discloses information about the seller (e.g., bank statements, work contracts, pay slips, medical records)
  - (d) Credentials or passwords (e.g., password to an online account)
  - (e) Redeemable financial data (e.g., voucher, credit-card number, crypto wallet)
  - (f) Evidence of illegal activities (e.g., rape, drug dealing, arms trafficking, homicide)
  - (g) Illegal content (e.g., child pornography)
  - (h) Data related to an identified organization (e.g., client details, contracts)
  - (i) Data related, sensitive or not, to an identified individual other than the seller (e.g., photos, e-mail, personal information)
  - (j) Other types of data, please specify: [ ] (Text field)
- (5) Regarding the data/files that you found on the device, were they readily visible and accessible on the device or did you use specific file-recovery techniques such as carving (e.g. with the help of software such as Autopsy, DiskDrill, or Scalpel)?
- (a) I used file recovery techniques. I followed the following procedure: [ ] (Text field)
  - (b) I accessed the files without any specific technique (i.e., they were readily visible on the device)
  - (c) I do not remember

[Display Q6, Q7, Q8 and if Q4 is answered.]  
[Repeat Q6, Q7, Q8 for every Q4\$DataType.]

You answered that you found Q4\$DataType on the device you bought.

- (6) Did you delete them?
- (a) Yes, I deleted them
  - (b) No, I kept them
  - (c) I do not remember
- (7) Have you **used them** in any way (opened, copied, printed, shared, etc.)?
- (a) Yes, please specify: [ ] (Text field)
  - (b) No
  - (c) I do not remember
- (8) [Multiple selection.] Which of the **following entities (if any)** did you notify about the data you found? (select all that apply)
- (a) The seller from Ricardo.ch
  - (b) The competent authorities, please specify: [ ] (Text field)
  - (c) An identified individual, other than the seller, who is concerned by the data found
  - (d) An identified organization, who is concerned by the data found
  - (e) A contact person from Ricardo.ch
  - (f) No
  - (g) I do not remember

The following questions relate **specifically** to your experience when you bought online the storage device \$DeviceName on Ricardo.ch, on \$TransactionDate.

- (9) [Multiple selection. Order randomized.] Which of the following **precautions** did you take with the device you bought?
- (a) I scanned it with an anti-virus software
  - (b) I plugged it to a computer that has little or no sensitive data and/or that would not be missed if the computer broke
  - (c) I plugged it to a personal electronic device other than a computer, such as a phone, camera, etc.
  - (d) I formatted/erased it

- (e) Other, please specify: [ ] (Text field)
- (f) I did not take any precaution

- (10) Was your computer or another device infected with a malware by the device you bought when you plugged it?
- (a) Yes
  - (b) No
  - (c) I am not sure
  - (d) I do not remember

[Display Q11 if Q10\$Yes]

- (11) What kind of malware was carried by the device you bought?
- (a) Trojan horse, worm, virus
  - (b) Ransomware
  - (c) Spyware
  - (d) I am not sure

### Sec. C: Attitudes

[Display Q12 for Q4\$DataType = 'false']

The following questions relate to **hypothetical** scenarios about the purchasing of used electronic storage devices **in general** (hard drives, USB sticks, memory cards) on Ricardo.ch.

- (12) [Grid question. Row order randomized.] **Imagine** that you found Q4\$DataType = 'false' on a second-hand storage device you bought, how likely would you do the following?

Row options:

- I would delete the data
- I would use the data (if likely please specify how): [ ] (Text field)
- I would notify the person who sold me the device (seller)
- I would notify the competent authorities (if likely please specify who): [ ] (Text field)
- I would notify an identified individual, other than the seller, who is concerned by the data found
- I would notify an identified organization who is concerned by the data found
- I would notify Ricardo.ch

- (a) Extremely unlikely
- (b) Moderately unlikely
- (c) Slightly unlikely
- (d) Neither likely nor unlikely
- (e) Slightly likely
- (f) Moderately likely
- (g) Extremely likely

### Sec. D: Legal Beliefs

The following questions relate to purchasing second-hand electronic storage devices **in general** (hard drives, USB sticks, memory cards).

Below you will be presented with **different statements related to legal rights and obligations in online transactions for second-hand electronic storage devices**. You will be asked to what extent **you agree or disagree** with these statements, under  **Swiss law**.

Please answer truthfully; your answers will be treated confidentially.

- (13) [Grid question. Row order randomized.] To what extent do you **agree or disagree** with the following statements?

Row options:

- (L1) If I find **personal nude photos** (e.g., of the sellers or of their contacts) on a used device I bought, I **can** legally **keep them and make personal use of them** (e.g., look at them).
- (L8) If I find **original nature landscape photos** on a used device I bought, I **can** legally **share them on social media**

- (L2) If I find illegal content, such as **child pornography**, on a used device I bought, I can be **held liable** if I **do not delete** it.
- (L9) If I find **confidential data** related to an **identified organization** on a used device I bought, I can legally **sell** them.
- (L10) If I find **credentials (passwords and identifiers)** on a used device I bought, I can legally **use them to access** the associated **service** (e.g., mail, Dropbox).
- (L3) If I find **purchased songs, movies, software**, etc. on a used device I bought, I can legally **keep and make personal use of them**.
- (L11) If I find an **unpublished book** (e.g., a novel written by the seller) on a used device I bought, I can legally **publish it under my name**.
- (L12) If I find **redeemable financial data** (e.g., **vouchers, credit card numbers, or crypto wallets**) on a used device I bought, I can legally **cash them in**.
- (L13) If I find **encrypted or password-protected** data on a used device I bought, I can legally use **specialized software** to gain **access** to it.
- (L14) After purchasing a used device, I can legally **use data recovery/forensics techniques**, (e.g., carving) to **access** data that was **previously deleted** from the device.
- (L15) **Generally speaking**, if I find **data from the seller** on a used device I bought, I can consider that the seller has left it there **willingly for me to use as I choose**.
- (L16) If I find **data related to an identified organization** (e.g., client details, contracts) on a used device I bought, it is **my legal obligation** to **notify** them.
- (L17) If I find **data related to the seller** on a used device I bought, it is **my legal obligation** to **notify** them.
- (L18) If I find **data related to an identified individual other than the seller** on a used device I bought, it is **my legal obligation** to **notify** them.
- (L19) If I find **illegal content** such as **child pornography** on a used device I bought, it is **my legal obligation** to **report** it to the competent authorities.
- (L20) If I find **evidence of illegal activities** (e.g., rape, drug dealing, arms trafficking, homicide) on a used device I bought, it is **my legal obligation** to **report** it to the competent authorities.
- (L4) If a used device I bought contains **malware** in the **clear** (i.e., without the need to recover it through specific software), the **seller** can be **held liable**.
- (L21) If a used device I bought contains **malware** in the **clear** (i.e., without the need to recover it through specific software), the **online second-hand shopping platform** can be **held liable**.
- (L5) If the **seller did not delete** possibly **sensitive data related to another individual** (e.g., nude photos of their partner), the seller can be **held liable**.
- (L6) If the **seller did delete** possibly **sensitive data related to another individual** (e.g., nude photos of their partner) but these data are **still recoverable** (e.g., through carving), the seller can be **held liable**.
- (L7) If the **seller contacts the buyer after the transaction asking them to delete** some **data** left on the device, the **buyer** has the legal **obligation to do so**.
- (a) Strongly disagree  
 (b) Disagree  
 (c) Somewhat disagree  
 (d) Neither agree nor disagree  
 (e) Somewhat agree  
 (f) Agree  
 (g) Strongly agree

#### Sec. E: Background

- (14) With which gender identity do you most identify?
- (a) Male  
 (b) Female  
 (c) Non-binary  
 (d) Prefer to self-describe: [ ] (Text field)  
 (e) Prefer not to say
- (15) What is your age group?
- (a) 18 to 20  
 (b) 21 to 29  
 (c) 30 to 39  
 (d) 40 to 49  
 (e) 50 to 59  
 (f) 60 or older

- (16) [Grid question. Row order randomized.] Please indicate to what extent you **agree or disagree** with the following statements.
- Row options:
- Compared to others, **I am more sensitive** about the way online companies **handle** my personal information.
  - To me, it is the most important thing to **keep my privacy intact** from online companies.
  - **I am concerned** about **threats to my personal privacy** today.
- (a) Strongly disagree  
 (b) Disagree  
 (c) Somewhat disagree  
 (d) Neither agree nor disagree  
 (e) Somewhat agree  
 (f) Agree  
 (g) Strongly agree

#### Sec. F: Security Practices

- (17) [Grid question. Row order randomized.] Please indicate how often you use the following technology-related practices.
- Row options:
- I use a **password/passcode to unlock** my electronic devices (computer, tablet, smartphone).
  - If I discover a security problem, **I continue what I was doing** because I assume someone else will fix it.
  - I try to make sure that the **programs** I use are **up-to-date**.
  - I verify that my **anti-virus** software has been **regularly updating** itself.
  - I **plug** USB sticks that I **find** into my electronic devices (computer, tablet, smartphone).
  - I **plug** USB sticks that **my contacts** (family, friends, colleagues) **give me** into my electronic devices (computer, tablet, smartphone).
- (a) Never  
 (b) Rarely  
 (c) Sometimes  
 (d) Often  
 (e) Always
- (18) [Grid question. Row order randomized.] To what extent do the following statements reflect what you are capable of doing?
- Row options:
- I know how to **manually delete some files** from a storage device (by sending them to the trash bin).
  - I know how to **manually delete all data** from a storage device (by sending them to the trash bin).
  - I know how to **empty the trash bin** of a storage device.
  - I know how to **format** a storage device.
  - I know how to **safely erase (wipe)** a storage device.
  - I know how to **scan** a storage device **with my antivirus software**.
- (a) Very untrue of me  
 (b) Untrue of me  
 (c) Somewhat untrue of me  
 (d) Neutral  
 (e) Somewhat true of me  
 (f) True of me  
 (g) Very true of me

#### Sec. G: Expectations

- (19) [Multiple selection. Order randomized.] When you bought the device \$DeviceName, would you have liked to receive more information from Ricardo.ch on any of the following? (select all that apply)
- (a) The technical aspects of transactions with storage devices (i.e., security and privacy risks)

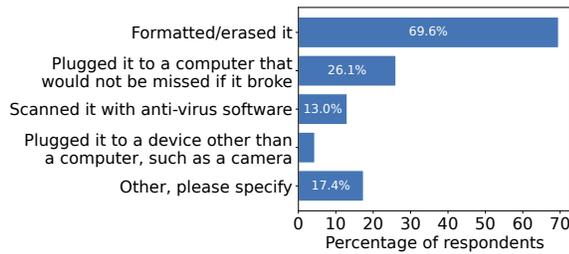
- (b) The legal aspects of transactions with storage devices (i.e., rights, obligations, liability)
  - (c) Other, please specify: [ ] (Text field)
  - (d) None
- (20) [Order randomized.] After reading this questionnaire, is there anything you would change when buying second hand storage devices on online platforms?
- (a) Yes, please specify: [ ] (Text field)
  - (b) No

**Table 2: Spearman rank correlation matrix for general attitudes toward remnant data.**

	D	U	NS	NCAs	NII	NIO
Delete (D)						
Use (U)	-0.11 *					
Notify Seller (NS)	0.11 *	0.03 *				
Notify Competent Authorities (NCAs)	-0.47 **	0.18 **	-0.05			
Notify Identified Individual (NII)	0.0	0.25 **	0.36 **	0.44 **		
Notify Identified Organization (NIO)	0.03	0.26 **	0.4 **	0.45 **	0.86 **	
Notify the Platform	-0.19 **	0.19 **	0.25 **	0.57 **	0.6 **	0.65 **

\* and \*\* refers to correlation coefficients with  $p < .05$  and  $p < .001$ , respectively.

## E PRECAUTIONARY ACTIONS



**Figure 4: Precautions taken by buyers to mitigate risks.**

## F ASSOCIATIONS BETWEEN ATTITUDES

Table 2 shows Spearman’s rank correlation coefficients between different courses of action for any type of data. The **likelihood to delete the remnant data is negatively correlated with the intention to notify the authorities** ( $r = -0.47, p < .001$ ) and **the platform** ( $r = -0.19, p < .001$ ). We found medium position correlations between *using* data and *notifying* other entities, including competent authorities ( $r = 0.18, p < .001$ ), individuals ( $r = 0.25, p < .001$ ), organizations ( $r = 0.26, p < .001$ ), and platforms ( $r = 0.19, p < .001$ ). This explains that, even before reporting remnant data, users need to first investigate the content. We found several strong positive correlations between notifying different entities. These findings were expected, as those who are open to notifying others built a similar understanding of the opportunity to notify these different entity types and do not differentiate between them.

Finally, to better understand the respondents’ attitudes with regard to illegal content, we looked at the associations between the likelihood of data usage and other attitudes, such as deleting data or notifying other entities. Particularly, we sought for understanding why some respondents (13%) reported they would use illegal data vs. legal data. Figures 5 and 6 in Appendix G depict these associations. The results show that out of the 13% who reported they would extremely likely use data, 11% responded that they would extremely likely notify the competent authorities. This again highlights the fact that, in order to report incidents, users would need to open and understand the content. One of the respondents, in an open-ended answer, reported that “[*deleting illegal content*] could be very problematic, as it could easily lead to potential evidence and information relevant to the investigation simply being destroyed.” **These findings highlight the possible difficulties even well-intentioned users could face in real life.**

## G ADDITIONAL DATA



Figure 5: Associations of the likelihood of data ‘usage’ and other attitudes towards Illegal content (e.g., child sexual abuse material)

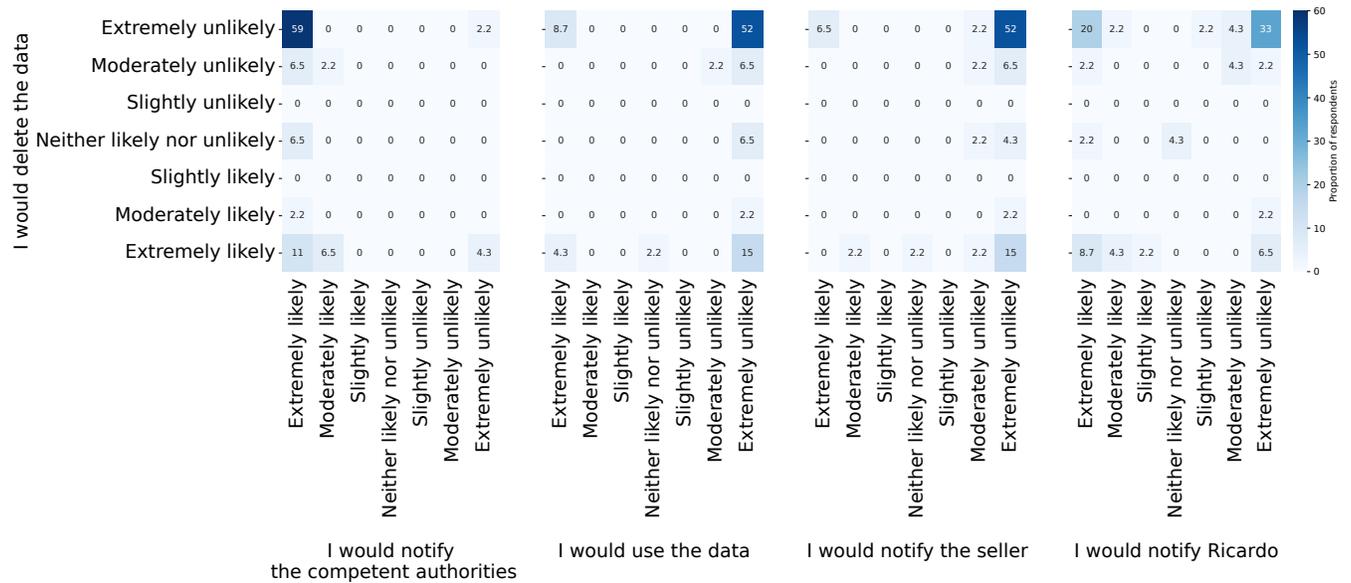


Figure 6: Associations of the likelihood of data ‘deletion’ and other attitudes towards Illegal content (e.g., child sexual abuse material).