Hey, Can We Go Thrift Shopping? Understanding the Privacy Practices of Secondhand Device Sellers through Digital Forensics

Cora Rowena Ruiz
City College of New York
cruiz1@ccny.cuny.edu

Tushar M. Jois
City College of New York
tjois@ccny.cuny.edu

***Abstract*—Secondhand shopping has grown increasingly popular, particularly through consumer-to-consumer (C2C) platforms such as Facebook Marketplace, eBay, and OfferUp. Devices sold in such marketplaces must be properly digitally sanitized to ensure the security and privacy of the previous owner; however, prior work has repeatedly shown that secondhand devices often retain recoverable, sensitive data, and that consumers of such devices frequently lack a complete understanding of effective device sanitation. These studies are generally conducted independent of each other, such that they typically focus on either the persistence of remnant data, or user perceptions of deletion, but not both. To address this research gap, we propose a holistic study which traces a secondhand device seller's initial perception of device sanitization and their actual actions on the device before sale, to the actual data left on device and the seller's reaction to it. Clarifying this underexplored relationship is critical to protecting consumers in the rapidly expanding secondhand market.**

***Index Terms*—Secondhand Devices, Digital Sanitation, Device Privacy, Forensic Recovery, Consumer Perception**

1. Introduction & Motivation

Secondhand shopping, or thrifting, is the practice of buying previously owned goods, at a discounted price [1]. What was once highly stigmatized has evolved into a mainstream form of purchasing, practiced regardless of an individual's financial means [2], [3]. OfferUp's 2025 Recommerce Report found that 93% of surveyed participants had made at least one secondhand purchase in 2025, and 22% had sold an item secondhand for the first time that year [4]. Consumer-to-consumer (C2C) online marketplaces such as Ebay, Facebook Marketplace, Craigslist, Mercari, and OfferUp have seen a significant increase in utilization [5].

Activity in the secondhand market is notably responsive to the public's perception of the economy, particularly during periods of economic uncertainty. Prior works found secondhand purchases satisfy the need to obtain necessities at an affordable price, and act as a way to quickly earn money when necessary, engaging both buyers and sellers [6], [7]. Indeed, U.S consumer confidence, as measured by the University of Michigan Consumer Sentiment Index (MCSI), has fallen to multi-year lows amid compounding economic forces [8], [9]. Under these conditions, secondhand shopping is increasingly popular [10], [11].

The popularity of C2C marketplaces extends to consumer electronics, such as laptops, smartphones, and home IoT devices, as well as peripherals, such as flash drives and memory cards. Given the sensitivity of data on these devices, the importance of *sanitizing* digital goods is essential for privacy. A number of C2C marketplaces recommend conducting a factory reset before sale as their primary, or in some cases, sole preparation for sale [12]–[14]. But, work in the digital forensics literature has found that factory resets are insufficient, with experiments recovering both significant quantities and varieties of sensitive user data across various device manufacturers and models [15]–[18].

2. Related Work

There is a substantial body of prior work concerning remnant data on secondhand devices, which largely falls into two categories: *device-centric* and *user-centric*. Device-centric work primarily identifies and classifies remnant data on secondhand devices, and is rooted in digital forensics (e.g., [19]–[27]). User-centric focus on the human experience, exploring the users experience experience selling, donating, or purchasing secondhand devices, and is rooted in human-computer interaction (e.g., [28]–[31]). Below, we summarize some of this literature as relevant to our work.

Device-centric. Garfinkel and Shelat's seminal work on secondhand hard drives found that a mere 9% had been properly sanitized, describing the rest as "awash in information that is both sensitive and confidential" [27]. Subsequent studies by Jones et al. significantly furthered this research area, conducting a series of annual examinations on a variety of secondhand storage devices from 2005 and 2019. Across these studies, the authors consistently recovered sensitive user data ranging from medical documentation, credit card numbers, vehicle registration information, to pornographic material. Their examination of decommissioned corporate storage media found that approximately 60% of the examined devices contained confidential data, including databases, resumes, and cryptographic keys [24]–[26].

User-centric. Ceci et. al authored one of the earliest works in the user-centric space, focusing on individuals who had

recently "disposed-of" devices, defined as devices intended to be sold, donated, thrown away, or recycled [30]. This work found widespread misunderstanding of data sanitation best practice, and yet a fear of unauthorized data access post-disposal. More recent work from Niksirat et. al examined perception among Swiss *buyers* of secondhand external storage devices, raising the importance of understanding both the buyer and seller experience, as they are both subject to harm through improperly sanitized devices [31].

Research gaps. In the literature, device-centric works look at data pulled off devices *after a sale*, and do not have a view into the perceptions and beliefs of the seller. On the other hand, user-centric works *do* have this view, but they do not involve *validating* the seller's perceptions with their actions. As prior work notes [32], *users cannot always be trusted to self-report security behaviors*, and seller may be incorrectly reporting their sanitization practices. Understanding seller practices with regards to device sanitation requires therefore studying *the entire sale*, mapping the user to the device.

Consider that each reseller has their own beliefs regarding device sanitation and deletion. Based on these beliefs, they will take certain presale actions drawing on their perception of potential risk, and overall understanding of deletion: this could be a factory reset, manually removing everything, or nothing at all. Notably, users are afraid of this potential risk [30]. But the risk to the secondhand seller only manifests once the device is actually resold: who spent effort sanitizing their devices at little risk, and those who did not facing a greater risk, due to remnant data on the device. Validating this risk therefore requires checking the device.

Thus, looking at the entire process end-to-end – perceptions generally, actions taken before the sale of a specific device, and data remaining after the sale – would give deeper insights than the literature current provides. As more consumers turn to the secondhand market, effectively mitigating the underlying factors that contribute to improper device sanitation becomes essential to prevent otherwise avoidable risks to consumer security and privacy.

3. Proposed Research

To develop a clear understanding of how a consumer's perception of deletion influences their sanitation practices while preparing a device for secondhand sale, we propose a study to answer the following research questions.

- **RQ1.** What specific sanitation actions do the sellers of secondhand devices take on an individual device before a sale?
- **RQ2.** How do these sellers perceive data sanitation and forensic recovery at the time of sale?
- **RQ3.** How do the specific presale sanitation actions correspond to data still available on the device after a forensic analysis?
- **RQ4.** How does awareness of the data still available on the sold device impact the future practices of secondhand device sellers?

4. Proposed Method

To answer our research questions, we propose a three-phase study to collect qualitative and quantitative data examining the participants understanding of device sanitation, their corresponding actions, and data remnants.

Phase I. We will recruit participants via their listings on C2C marketplaces for commonly purchased secondhand devices. Those who consent to participate will be asked semi-structured interview questions about the actions they performed *on the device they are selling*, as well as their general understanding of best practices in sanitizing secondhand devices for sale (which may be different).

Phase II. We will purchase the secondhand device from the seller at the asking price. The device will be forensically imaged and examined using standard forensic toolkits such as FTK Imager and Autopsy. Recovered data will be de-identified and documented, and compared against the participant's responses in Phase I the actions they performed.

Phase III. After the forensic exam, we will then contact the participant again and inform them about the data remaining on their device. They will then be asked semi-structured interview questions about how the exam results impacted their perceptions and their future secondhand device sale behavior. Once this interview is complete, we will destroy the the device image from the forensics tools, and the physical device will be properly cleared of remnant data using industry best practices and appropriately recycled.

5. Ethical Considerations

In presenting our proposal to the ConPro'26 community, we hope to get the community's feedback on all aspects of our work, but particularly in terms of ethical considerations. Given the use of forensic technologies – which have the potential to extract large amounts of sensitive user data [33] – against real consumer devices, we wish to design our study in accordance with the strongest safeguards.

First, we recognize actually *purchasing* devices may lead to unintentional pressure on the seller to participate in the study as a precondition for making the sale. We are interested in mitigating this possibility.

Next, reviewing forensically recovered content could be understandably uncomfortable for participants. We are interested in techniques to best handle this situation.[1]

Lastly, to reduce accidental disclosure, we plan to conduct the forensic examinations offline, in a dedicated virtual environment. We are interested in other suggestions to secure recovered participant data.

Acknowledgments

This work is supported by the National Science Foundation under award number 1955172, PSC-CUNY Research

1. We note that, in accordance with local laws and regulations, if we encounter illegal data, we will be obligated to report it instead.

Awards from the City University of New York, and the U.S. Department of Education under the TREAD program at the City College of New York. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily those of the sponsors.

References

[1] N. Angelica, F. Hasanah, S. Khumayah, and D. Erawati, "Thrifting: Consumer perceptions and decisions," *Asian Journal of Social and Humanities*, vol. 3, pp. 1810–1822, 07 2025.

[2] O. Waxman, "People have been reusing clothes forever but thrift shops are relatively new. here's why," https://time.com/5364170/thrift-store-history/, 2018.

[3] J. Cote, "Thrifting through the ages: How we've strayed from central values," https://www.statepress.com/article/2021/03/specho-thrifting-secondhand-clothing-through-the-ages, 2021.

[4] OfferUp, "Offerup recommerce report 2025," https://recommercereport.com/, 2025.

[5] Yahoo Finance, "C2c (consumer-to-consumer) e-commerce market size and share," https://finance.yahoo.com/news/c2c-consumer-consumer-e-commerce-142900980.html, 2024.

[6] T. N. A. of Resale & Thrift Shops, "What we know about secondhand goods and continued use," https://www.narts.org/i4a/pages/index.cfm?pageid=3290, 2015.

[7] H. Chu and S. Liao, "Exploring consumer resale behavior in c2c online auctions: Taxonomy and influences on consumer decisions," *Academy of Marketing Science Review*, vol. 11, no. 3, pp. 1–25, 2007.

[8] T. U. of Michigan, "The index of consumer sentiment," https://www.sca.isr.umich.edu/files/chicsh.pdf, 2025.

[9] D. B. Papadimitriou, G. T. Yajima, and G. Zezza, "The us economy amid rising global uncertainty, strategic analysis report, october 14, 2025," https://www.levyinstitute.org/publications/the-us-economy-amid-rising-global-uncertainty/, 2025.

[10] NPR, "Tariffs and the secondhand shopping boom," https://www.npr.org/2025/04/11/nx-s1-5357033/tariffs-secondhand-shopping, 2025.

[11] S. James, R. B. Brown, T. L. Goodsell, J. Stovall, and J. Flaherty, "Adapting to hard times: Family participation patterns in local thrift economies," *Family Relations*, vol. 59, no. 4, pp. 383–395, 2010. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1741-3729.2010.00610.x

[12] eBay, "Have a phone to sell?" https://pages.ebay.com/smartphone/custombox.html/, 2025.

[13] Mercari, "How to list a smartphone," https://www.mercari.com/us/help_center/article/376/, 2025.

[14] Facebook, "Selling on facebook marketplace," https://www.facebook.com/help/1252783238218358/, 2025.

[15] M. B. Blankesteijn, A. Fukami, and Z. J. M. H. Geradts, "Assessing data remnants in modern smartphones after factory reset," *Forensic Science International: Digital Investigation*, vol. 46, p. 301587, 2023.

[16] L. Simon and R. Anderson, "Security analysis of android factory resets," in *4th Mobile Security Technologies Workshop (MoST)*, 2015.

[17] R. Schwamm, "Effectiveness of the factory reset on a mobile device," Ph.D. dissertation, Monterey, California: Naval Postgraduate School, 2014.

[18] R. Schwamm and N. Rowe, "Effects of the factory reset on mobile devices," *Journal of Digital Forensics, Security and Law*, vol. 9, 01 2014.

[19] W. Glisson, T. Storer, and G. e. a. Mayall, "Electronic retention: what does your mobile phone reveal about you?" *Int. J. Inf. Secur. 10, 337–349*, 2011.

[20] R. Roberts, J. Poveda, R. Roberts, and D. Levin, "Blue is the new black (market): Privacy leaks and re-victimization from police-auctioned cellphones," *2023 IEEE Symposium on Security and Privacy (SP)*, 2023.

[21] P. S. Szewczyk, N. Robins, and K. Sansurooah, "Sellers continue to give away confidential information on second hand memory cards sold in australia," *Proceedings of the 11th Australian Digital Forensics Conference*, 10.4225/75/57b3dac1fb876.

[22] A. Martin, Thomas; Jones and M. Alzaabi, "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*, 2016.

[23] T. Ojo, H. Chi, J. Elliston, and K. Roy, "Secondhand smart iot devices data recovery and digital investigation," *SoutheastCon 2022*, 2022.

[24] A. Jones, V. Mee, C. Meyler, and J. Gooch, "Analysis of data recovered from computer disks released for resale by organisations," *Journal of Information Warfare*, vol. 4, no. 2, pp. 45–53, 2005. [Online]. Available: https://www.jstor.org/stable/26504063

[25] A. Jones, C. Valli, G. Dardick, and I. Sutherland, "The 2007 analysis of information remaining on disks offered for sale on the second hand market," *Journal of Digital Forensics, Security and Law*, vol. 3, no. 1, 2008.

[26] A. Jones, O. Angelopoulou, and L. Noriega, "Survey of data remaining on second hand memory cards in the uk," *Computers & Security*, vol. 84, 2019.

[27] S. Garfinkel and A. Shelat, "Remembrance of data passed: A study of disk sanitization practices," *IEEE Security & Privacy*, vol. 1, no. 1, pp. 17–27, 2003.

[28] Saeedi, Payam and Cade, Willie and Oh, Tae and Watson, Stacey and Williams, Eric, "Data wiping behaviors for end-of-first-use electronics: Insights from a survey of u.s. consumers," *Association for Computing Machinery*, 2025.

[29] A. Murillo, A. Kramm, S. Schnorf, and A. De Luca, "" if i press delete, it's gone"-user understanding of online data deletion and expiration," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018, pp. 329–339.

[30] J. Ceci, H. Khan, U. Hengartner, and D. Vogel, "Concerned but ineffective: User perceptions, methods, and challenges when sanitizing old devices for disposal," in *Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 2021, pp. 455–473.

[31] K. S. Niksirat, D. Korka, Q. Jacquemin, C. Vanini, M. Humbert, M. Cherubini, S. Métille, and K. Huguenin, "Security and privacy with second-hand storage devices: A user-centric perspective from switzerland," *Proceedings on Privacy Enhancing Technologies*, vol. 2024, no. 2, pp. 412–433, 2024.

[32] R. Wash, E. Rader, and C. Fennell, "Can people self-report security accurately? agreement between self-report and behavioral measures," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 2228–2232. [Online]. Available: https://doi.org/10.1145/3025453.3025911

[33] M. Zinkus, T. M. Jois, and M. Green, "Data security on mobile devices: Current state of the art, open problems, and proposed solutions," *arXiv preprint arXiv:2105.12613*, 2021.