E4S Brief

Security and Privacy with Second-Hand Electronic Devices

Date: May 1st, 2024 – April 30th 2025

Authors: Kévin Huguenin and Öykü Işik

Keywords: second-hand storage device, privacy, security, user survey

Disclaimers /acknowledgements /embargo: N/A

In a Nutshell

As the second-hand electronics market grows, it plays a vital role in the circular economy by extending the life of devices and reducing e-waste. Yet, storage-equipped devices, from laptops and smartphones to USB sticks and memory cards, often contain *remnant* data: leftover files from previous users (personal or professional) that may reveal sensitive information. This creates *privacy* risks for *former users* and *security* risks for *new users*, threatening trust in the second-hand market ecosystem.

Our project examines these risks from multiple angles: *consumer* transactions on online marketplaces, *corporate* device lifecycle management, and the *research* practices used to study remnant data. We combine online surveys, in-depth interviews, and a systematic review of decades of technical and human-centred studies.

Early results show that, while prior forensic studies often report that remnant data can be recovered from many second-hand devices, our own user-focused study found that typical buyers on second-hand transaction platforms rarely find—or even attempt to access—such data. However, even isolated incidents can lead to severe consequences, especially when sensitive or illegal material is involved. We also found gaps in user awareness. In corporate contexts, employee training and policy communication are inconsistent, and risk perceptions vary widely.

To strengthen the circular economy, we call on organizations and policymakers to adopt verifiable data-wiping standards, improve user awareness, and support open guidance for safe reuse. Our forthcoming tutorial will equip researchers and practitioners with concrete, legally and ethically grounded, and methodologically rigorous recommendations for studying remnant data, ensuring results that are both reliable and socially responsible.

What we do and why is matters

The transition to a circular economy is critical for reducing environmental impact and conserving resources. Reuse of electronic devices is central to this transition, but it must be safe and trustworthy. Storage-equipped devices, such as smartphones, laptops, and USB sticks, often retain remnant data from previous users. This data can include personal (and sensitive) photos, business documents, login credentials, or even malicious software, creating privacy risks for sellers and security risks for buyers. If these risks remain unaddressed, they can undermine public trust in the second-hand market and slow the adoption of sustainable reuse practices.

Our project investigates these risks across three contexts: (1) consumer transactions on online platforms dedicated to the trade of second-hand goods, (2) corporate device management and redistribution, and (3) the research practices themselves in studying remnant data. By combining large-scale surveys, qualitative interviews, and a systematic literature review, we aim to generate practical, evidence-based recommendations.

Our target audiences are:

- **Consumers and corporate employees** who use storage-equipped devices that will or have been recycled.
- **Managers and IT/security professionals** in organizations who oversee device lifecycle management.
- **Online marketplaces** that enable the second-hand (electronics) trade.
- **Policy-makers and regulators** shaping data protection and sustainability frameworks.
- **Researchers** in security, privacy, and human-computer interaction who are studying this domain.

By raising awareness, standardizing safe device disposal practices, and promoting verifiable data sanitization, our work supports E4S's mission to foster an economy that is sustainable, inclusive, and digitally resilient.

How we do it and main findings

We adopt a user-centred, mixed-method approach to understand and address the privacy and security risks of remnant data in second-hand storage devices. Our work covers three complementary streams:

1. **Consumer context:** We surveyed users of a major Swiss second-hand marketplace (Ricardo.ch) to explore their awareness, behaviours, and experiences with remnant data when buying devices, and their attitudes if they sell devices.
2. **Organizational (corporate) context:** We developed an interview protocol and conducted an in-depth pilot with corporate IT management to understand policies, practices, and challenges in managing device lifecycles.
3. **Research community context:** We are conducting a systematic literature review (SLR) to identify the main findings regarding remnant data and the current research practices for studying remnant data, focusing on legal, ethical and scientific considerations.

Methodology in brief

- **Surveys:** Large-scale, online questionnaires targeting buyers of storage-equipped devices.
- **Interviews:** Semi-structured interviews with corporate IT leaders and C-suite executives.
- **Systematic literature review:** Comprehensive screening and coding of past technical and human-centred studies.

Key findings (so far)

- **Prevalence & awareness:** While forensic studies show remnant data is often recoverable, our user-focused survey suggests that typical buyers rarely attempt advanced recovery; however, awareness of legal and privacy risks is inconsistent.
- **Buyer behaviour:** Nearly one-third of buyers did not check for data at all; 70% formatted devices, and none reported using forensic tools. Some buyers, however, indicated they would keep sensitive or illegal data to report it, despite lacking legal obligations.
- **Corporate practices:** Pilot interview revealed heavy reliance on vendor-issued “data wipe” certificates, with minimal independent verification.

- **Employee awareness:** Corporate staff generally understand devices must be returned, but often lack knowledge of how data is processed or destroyed.
- **Risk perception among employees:** Higher concern when devices come from senior staff; otherwise, risks are often perceived as low.
- **Research practices:** Existing remnant-data studies vary widely in applied methodologies, ethical safeguards, legal compliance, and handling of sensitive content, with no consensus on best practices.

Scientific contribution

- First integrated view of remnant data risks across consumer, organizational, and research contexts.
- New qualitative insights into corporate device management, including drivers, constraints, and gaps in verification.
- Ongoing development of a structured framework for the best methodological, legal, and ethical practices for studying remnant data, targeting publication in ACM Computing Surveys.

Stream	Methods	Preliminary Findings
Consumer	Survey	Most buyers format devices; few attempt recovery. Awareness of privacy/legal risks is mixed. Some keep sensitive/illegal data to report despite no legal obligation.
Corporate	Interviews; doc review	Heavy reliance on vendor "wipe" certificates with limited independent checks. Employees know devices must be returned, but often lack insight into data handling. Risks are seen as higher for senior staff devices.
Research	SLR	Remnant-data studies vary widely in ethics and legal compliance; no consensus on best practices.

These findings lay the groundwork for concrete interventions, such as buyer/seller awareness tools, verifiable data-wiping protocols, and standardized research guidelines, to make second-hand electronics reuse safer and more trusted.

Call for action

To sustain the growth of the circular economy, the reuse of electronic devices must be safe, secure, and trusted. Our findings show that while remnant data risks are well-documented, they rarely materialize in everyday consumer transactions, often because buyers format devices immediately, yet even isolated incidents can have severe consequences. In corporate settings, reliance on vendor-issued "wipe" certificates is common, but independent verification is rare. Buyers and employees education is inconsistent, and misconceptions about legal obligations persist. Research practices in this space remain inconsistent, with no consensus on ethical or legal standards, underscoring the need for clear, shared guidance.

We call on marketplaces, corporations, policymakers, and researchers to:

1. **Increase user awareness:** Integrate clear, actionable guidance for sellers, buyers, and employees at every stage of the device lifecycle.
2. **Strengthen corporate policies:** Ensure device management protocols address both security and sustainability, and are communicated effectively.
3. **Standardize research practices:** Establish shared ethical, legal, and methodological guidelines for studying remnant data.

These actions will reduce the risk of privacy breaches, protect organizational and personal data, and encourage wider participation in safe device reuse, ultimately extending product lifespans and reducing e-waste. Equally important, adopting clear ethical and legal safeguards, along with rigorous, replicable research methods, will protect both researchers and participants while ensuring that findings are trustworthy and actionable.

By bridging consumer, corporate, and research perspectives, our project delivers practical tools and evidence-based recommendations that can be implemented. We invite collaboration from industry, regulators, and the research community to turn these insights into lasting change.

> "While the risks associated with remnant data are high, they rarely materialize. However, a single incident is enough to undermine the trust in the second-hand market and the circular economy for electronic goods" Prof. Kévin Huguenin

Learn more

- Research article: Security and Privacy with Second-Hand Storage Devices: A User-centric Perspective. Proceedings on Privacy Enhancing Technologies (PoPETs), 2024 (2), pp. 412-433. https://dx.doi.org/10.56553/popets-2024-0057

- Conference presentation: https://youtu.be/h3pzneOEzHs?si=mdI4jM35ALwlvVC5

- Technical report: Remnant Data : A Survey of Results and a Tutorial on Good Research Practices. In preparation [to be submitted to ACM CSUR].

- Project overview (E4S website): https://e4s.center/resources/reports/security-and-privacy-with-second-hand-electronic-devices/

Contact us:

Prof. Kévin Huguenin, Department of Information Systems, University of Lausanne

Kevin.Huguenin@unil.ch