stellar

RESIDUAL DATA STUDY ON SECOND HAND DEVICES

a study on the risk implication for people, businesses and economies

A STUDY CONDUCTED BY STELLAR

Index

Introduction

STELLAR's second hand device study report 2019 provides insights on the threat landscape, ranging from privacy & security breaches at the time of disposing off old devices, for individuals & businesses.

The goal of the study is to ascertain the awareness levels amongst device owners regarding usage of secure data wiping methods at the time of selling old storage devices.

About Stellar

Stellar Data Recovery is a leading data care solution provider headquartered in India, with presence in the US and Europe. We are an ISO 9001 & ISO 27001 certified organization specializing in Data Recovery, Data Erasure, Mailbox Conversion, and File Repair software & services. Our data care software products are known for their incredible ease of use and yet powerful in their use to fulfill needs of both consumers and enterprises. For more than 25 years we have been consistently developing innovative, future-ready solutions that are trusted by more than 3 million individuals & Fortune 500 companies globally.

FOREWORD

by Sunil Chandna, CEO STELLAR

In 2018, 5 billion people on this planet created 33 ZB (1 trillion GB) and this data is expected to grow explosively to 175 ZB in 2025. Since 2016, each year 2.3 billion computing & mobile devices were shipped to help people manage this data. The rapid technological evolution and aspirational needs have led to shortened device lifespan. As a result there is a huge amount of devices that are traded in the second hand market.

Unsecure device disposal increases data privacy breach risks leading to identity thefts, financial frauds and criminal acts against individuals. Businesses, governments and organizations face risk of paying fines, penalties, lawsuits and reputation loss on failing to meet obligatory compliances with various privacy and data protection regulations like GDPR, HIPAA, GLB, SOX.

Stellar, as a responsible global organization, has taken the initiative to conduct the study of second hand devices that were sold by individuals and businesses. This systematic study presents empirical findings on the risk of data breach associated with disposing of used devices.

While the findings are alarming, I hope this study finds its purpose to build awareness about the potential risk amongst all stakeholders including law enforcement agencies, regulators, consumers, data protection officers and professional information destruction providers.

Sunil Chandna

FOREWORD

by Robert Johnson, CEO NAID

NAID commends Stellar Information Technology for continuing to shed light on the problem of data security breaches caused by personal information that too often remains on second hand electronic devices. As the largest such investigation to date, and first conducted in India, this study establishes the problem of improper data erasure as a global issue, and that data protection problems in one region of the world poses challenges for data security everywhere.

NAID also commends Stellar for being the first organization to conduct such a study using the NAID Second-Hand Device Study Principles, developed to assure the evaluation and the results are honest, fair and compliant with relevant regulations.

ABOUT NAID

NAID® is one of the divisions of the International Secure Information Governance and Management Association™ (i-SIGMA™). It was originally formed as its own association in 1994 and became a part of i-SIGMA in 2018 when it merged with PRISM International. NAID continues to be the international watchdog for the secure data destruction industry, advocating for a standard of best practices across governments and by service providers as well as suppliers of products, equipment, and services to destruction companies.

EXECUTIVE SUMMARY

Background

Stellar released a report in 2017 that revealed widespread residual data in the storage devices procured from second hand market. The purpose of 2019 study is to re-validate the findings using NAID approved principles on a very large sample size of second hand storage devices procured from multiple locations.

Study Findings

The study revealed that over 71% of the 311 devices analyzed contained PII [Personally Identifiable Information], personal data and business information. 222 of the devices studied were disposed off in secondary market without using proper data erasure tools.

World's Largest Study

Stellar conducted world's largest study of old devices in India to ascertain awareness level amongst individuals & businesses about data leakage and use of secure data wiping methods at the time of disposing off old storage devices. 311 storage devices were procured comprising hard disk drives, memory cards & mobile phones.

Risk

7 out of every 10 individuals are vulnerable to data breach & privacy RISK while disposing off second hand devices. Misuse of individuals' data can lead to identity theft, financial frauds and criminal acts amongst others. Organizations could face penalization, legal suits for claims, loss of reputation and business.

Analysis

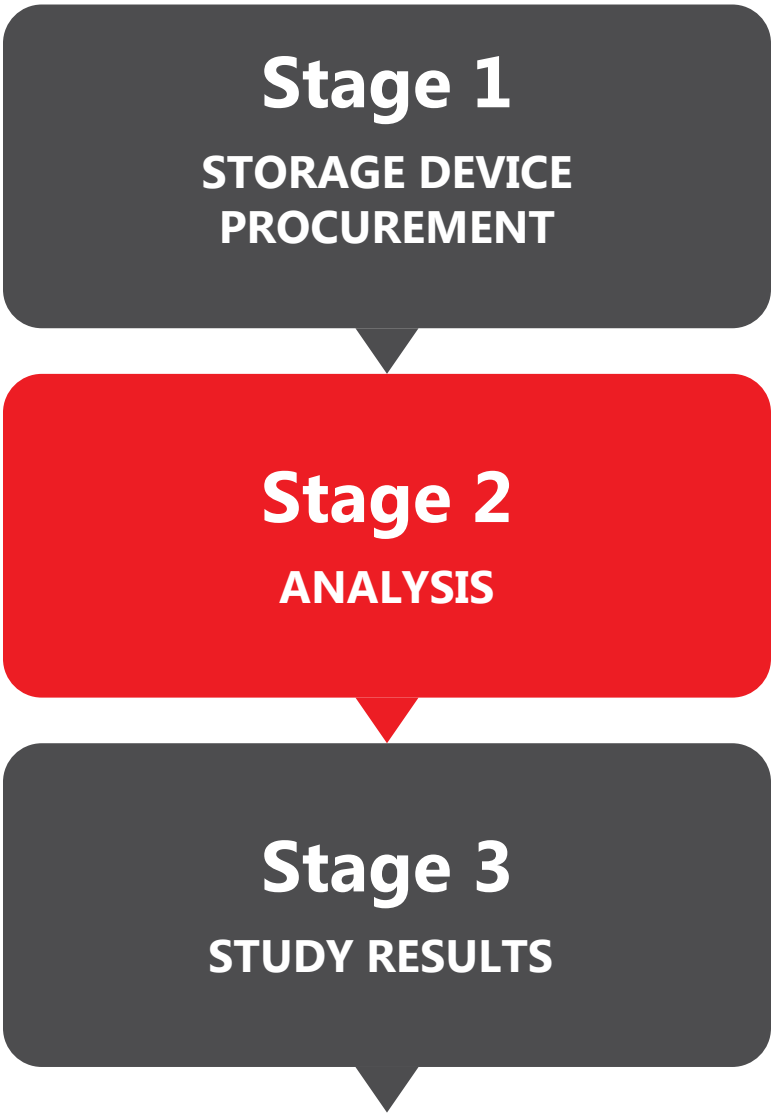
The analysis process for the study was methodical and transparent. All devices were cataloged. The hard drives & memory cards were analyzed using 'Stellar Data Recovery' software that is freely available for consumers. The purpose of using a standard DIY tool was to establish the relative ease with which any individual with no technical know-how could retrieve sensitive, private or business data. The mobile phones were scanned with a forensic analysis tool. The findings were recorded in a secure manner while ensuring no PII disclosure of the subjects.

Conclusion

1. Individuals & Organizations in India have very POOR AWARENESS of data breach related risks when selling old data storage devices.
2. It's likely in coming years that India would witness EXPONENTIAL INCREASE in acts of cybercrime.
3. The Personal Data Bill, 2018 when approved as a LAW, could trigger development of an ecosystem leading to HIGH AWARENESS and RISK MITIGATION ACTIONS by consumers and organizations.

STUDY METHODOLOGY

SYSTEMATIC MULTI-STAGE APPROACH



STAGE 1 STORAGE DEVICE PROCUREMENT

A - Procurement & Device Acquisition Management

A total of 311 storage devices (hard drives, memory cards & mobile phones) were procured from multiple locations in India. These were purchased from businesses & individuals directly via online portals or through resellers. All memory cards and mobile phones were purchased through resellers. Hard drives were purchased from both resellers and online portals. Stellar has record of purchase of each device for which study was conducted. These devices were obtained from publicly available outlets, with no knowledge of, or involvement in, the study. Though such sources have not been named in the study, their general nature in aggregate has been reported in the result.

PROCUREMENT SOURCE
Individual
97
Reseller
214

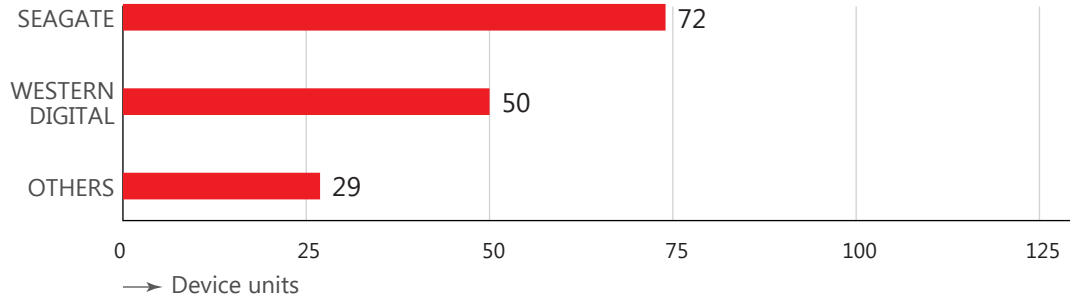
B - Research & Study Compliances Met

All personnel of Stellar that participated in the study signed a non-disclosure agreement confirming their understanding that any data and all PII / Personal data encountered during the study will be kept confidential and protected from unauthorized access. As a part of ISO compliance, each employee of Stellar signs a NDA with the company.

C - Storage Device Mix

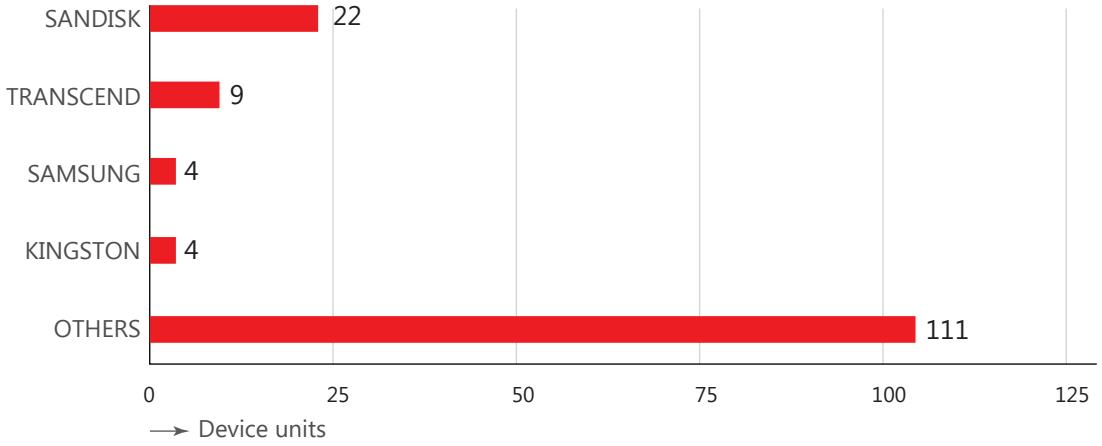
151
Hard Drives

151 hard drives (of 7 makes) were procured comprising desktop drives, laptop drives and external hard drives; with capacities ranging from 100GB to 1.5 TB. The desktop drives comprised of a majority – 100 units. Majority of the drives were of 500GB [65 units].



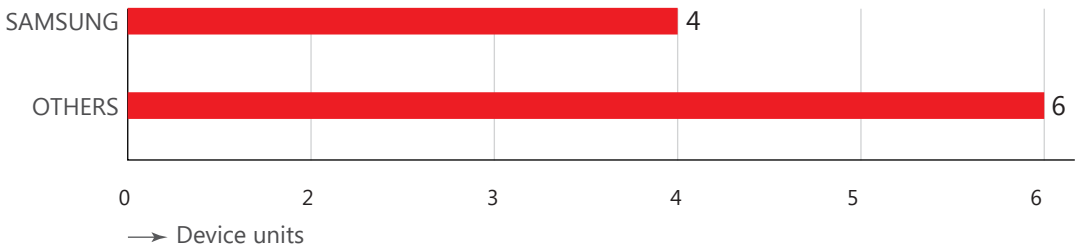
150
Memory Cards

150 memory cards (of 23 makes) were procured with capacities ranging from 128MB to 8GB. Majority of the cards were of 2GB capacity [71 units].



10
Mobile Phones

10 second hand mobile phones (of 7 makes) were procured ranging from 1GB to 8GB. Majority of the phones were of 8GB capacity [5 units].



D - Data Anonymization

Complete anonymization of extracted residual data was maintained, throughout the research. Potentially all sensitive data was anonymized or the information was put into broad categories and generalities throughout the study report.

E - Cataloging & Access Control

Each device was assigned a unique code and tagged to ensure traceability. The tagged details were recorded along with device specifications like media model, capacity, serial number, supplier details, location etc. A project administrator was appointed to catalog the devices and keep them in safe custody. All devices were kept in a secure place with restricted access control.

STAGE 2 ANALYSIS

The devices were analyzed at Stellar's central laboratory in India by a team of 9 data recovery experts.

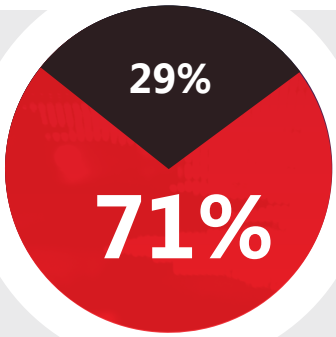
- As the first step we analyzed the devices and checked if they were recognized by the computer and if any files were accessible when connected to the computer.
- In the next step, a freely available DIY software – Stellar® Data Recovery was used to scan 301 devices (memory cards and hard drives) for recovering data. 10 Mobile phones were scanned using Cellebrite® forensic tool.
- All findings, including the analysis observations & tools used, were recorded for every tagged device that formed a part of the study in secure server. The recovered data was also stored in secure recovery server of Stellar that has restricted access.

STAGE 3 STUDY FINDINGS

RESIDUAL DATA FOUND : 71% - 222/311

71% Vulnerable to THREATS

- *Residual data found*
- *Were prone to risk with no or poor understanding of privacy risks*



29% Aware of RISKS

- *Residual data not found*
- *Were aware of risks and took measures to erase information before selling devices*

147 out of 150 memory cards had residual data like photos, videos, visa, passport copies, etc.

MEMORY CARDS

69 out of 151 hard drives had data like photos, videos, identification cards, business documentation, banking info, sales deeds, partnership agreements, invoice bills, etc.

HARD DISK DRIVES

6 out of 10 mobile phones had data such as contacts, photos, identification card, banking info, etc.

MOBILE PHONES

7 out of 10 devices were vulnerable to Personal Data / PII leakage risks.

TYPE OF DATA COMPROMISED

The data comprised of "Personal data & Sensitive information" such as the following :


PHOTO & VIDEO


PASSPORT & VISA


NATIONAL IDENTITY CARD
VOTER ID CARD


REAL-ESTATE PURCHASE RECORDS


INCOME TAX CARD


DRIVING LICENSE


RESUME


CONTACT LIST


CALL RECORDING

ADULT CONTENT

INCOME TAX FILING


BANK INFORMATION & CHEQUES


LOGIN CREDENTIAL & PASSWORDS

IP ADDRESSES


BUSINESS CONTRACTS & INVOICE

These are just some examples of the data left behind.

196	Devices had Photographs, Videos.
50	Devices had Personal Documentation (Passports, Visa, Identification Documents).
25	Devices had Business Documentation (Partnership Agreements, Sale Deeds, Invoice, Bills).
9	Devices had Banking Information (Cheques, Bank Details, Account Statement, Credit Card Details).

HIGH PRIVACY & SECURITY RISKS

For owners of digital devices when they dispose off old devices into secondary markets

INDIVIDUALS

User Identity Thefts

Residual data if it falls in wrong hands can lead to Identity thefts. Your personal data like biometric information, medical information, national identity card along with credit card numbers and online banking credentials etc. can be misused for fake online transactions such as opening bank accounts and filing tax returns, etc. The perpetrators may further exploit children's clean credit histories and PII such as social security number to make fraudulent transactions on their names.

User Privacy Issues

Sensitive personal data such as private pictures, contacts, text messages, emails, addresses, chat history, browsing history, and date of birth etc. is commonly stored on hard drives and mobile devices. This data is breached and misused if left behind on old device.

Personal Security Threats

Personal data such as private pictures, messages, and other sensitive information is stolen from a user's personal device. The perpetrator exploits this information to pose personal security threat which can be in the form of harassment, extortion, and other kinds of physical/emotional threats.

Consumers Vulnerable to Financial Frauds

Financial security could be compromised if account passwords or near field communication payment information is recovered from the device.

Risk to New Owners

The new buyer of an inadequately sanitized second hand storage media might unknowingly end up in possession of 'illegal information' that was owned by the previous device user. This information 'if discovered' can be mis-attributed to the current device owner and pose risks of litigation, reputation loss, and embarrassment.

BUSINESSES

In the business context, the ambit of data threats extends beyond Personal data or PII to include theft and misuse of business-critical information such as intellectual property, financial reports, business intelligence, and trade secrets, etc. These data breach scenarios put businesses at an immense risk of financial loss, legal proceedings, brand damage, and embarrassment. With arrival of tough regulations such as GDPR, the implications for non-compliant businesses have grown even more serious.

INSIGHTS: AWARNESS & ROAD AHEAD

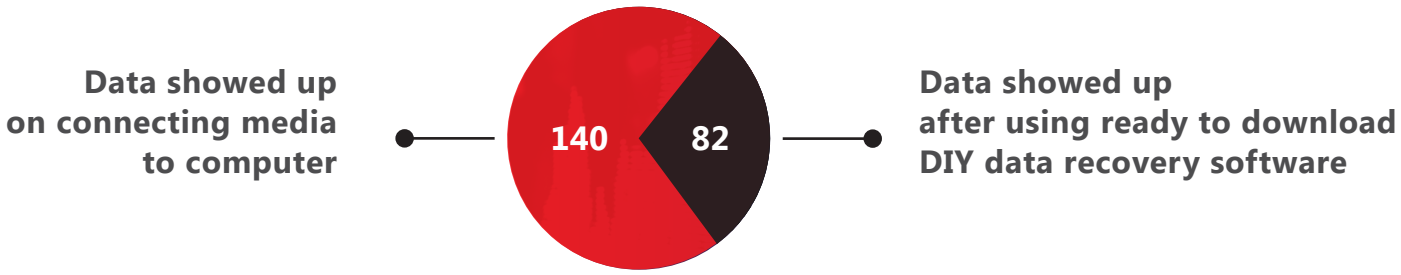
Ignorance is RISK!

A large 45% of the total [140] devices studied in this report were disposed off, with no action taken at all by the sellers. The data was just lying there on those devices, with the device owners being totally oblivious of the potential damages. This abject disregard for the data risks clearly highlights that the device owners were ignorant of the need to use secure methods to erase data by using data wiping software.

Data Erasure Myths ... Drive Formatting & File Deletion

1 in every 4-device studied was disposed off either after deleting the files or by formatting the storage media. File deletion tools are designed to free up storage space when files are no longer needed. They do not erase data. Similarly, the purpose of drive formatting utility software is to prepare a storage media for fresh use. Usually, the data is not wiped from the media after a formatting action. Over 25% of the device owners had wrong presumptions that the data is permanently removed by using these methods, and had thus put their private or business information at risk.

Findings of the 222 storage devices



Awareness Campaigns & Consistent Monitoring

Continuous Awareness campaigns should help reduce the instances of residual data left in the old devices at the time of disposal. Similar studies should be conducted at regular intervals to help drive and ascertain the change. Updated lab studies on evolving data threats can play an imperative role in driving widespread awareness & helping the users take on their data protection responsibilities with conviction.

Secure Disposal Procedures & Audits

Organizations should implement clearly defined policies & procedures for secure storage media sanitization, when decommissioning IT assets. While media sanitization procedures could be carried out internally or through a professional IT Asset disposition agency, it's important to conduct regular data security & privacy audits to meet the prevalent regulatory standards. Realizing the shortened lifecycle of personal devices with quick technological changes, media sanitization has gained primacy in the consumer segment as well. Individuals must proactively arm themselves with the necessary information to safely dispose off their outgoing storage media and devices.

REFERENCES

01 Recommended Citation: William Bradley 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), pp. 77-98

02 https://timesofindia.indiatimes.com/india/globally-80-of-e-waste-either-ends-up-in-landfills-or-being-informally-recycled-says-un-agencies/articleshow/67694429.cms

03 https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

04 https://www.gartner.com/en/newsroom/press-releases/2018-01-29-gartner-says-worldwide-device-shipments-will-increase-2-point-1-percent-in-2018

05 https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

ABBREVIATIONS

CAGR	Compound Annual Growth Rate
GB	Gigabyte
GDPR	General Data Protection Regulation
IANS	Indo-Asian News Service
ICT	Information and Communication Technologies
IT	Information Technology
ITAD	IT Asset Disposal
MB	Megabyte
NAID	National Association for Information Destruction
NCR	National Capital Region
PII	Personally Identifiable Information
TB	Terabyte
ZB	Zettabyte (1 trillion GB)
NDA	Non-Disclosure Agreement
ISO	International Organization for Standardization

RESIDUAL DATA STUDY ON SECOND HAND DEVICES

Release APRIL 2019

A Report by
STELLAR INFORMATION TECHNOLOGY PVT. LTD.

US | India | Europe

+1 877 778 6087
www.stellarinfo.com

Release : April, 2019