Report: Personally Identifiable Information Found on 40 Percent of Used Devices in Largest Study To-Date

The National Association for Information Destruction® (NAID®) has conducted the largest second-hand device study in the world to date. It was conducted in the first quarter of 2017 by NAID using CPR Tools Inc. data recovery services and revealed that 40 percent of devices resold in regular commerce channels contained personally identifiable information (PII) without taking heroic efforts to acquire it.

The current state of electronic storage has made it possible for nearly every adult to carry a form of data storage device (i.e. smart phones, tablets, laptop computers, etc.). “As data storage is included in nearly every aspect of technology today, so is the likelihood of unauthorized or unintended access to that data” states CPR Tools CEO, John Benkert. He goes on to say, “Auction, resell, and recycling sites have created a convenient revenue stream in used devices; however, the real value is in the data that the public unintentionally leaves behind.”

In this study, the devices inspected were intended to be a representative view of what typical users own and thus discard: smart phones, tablets, and hard drives. All devices were subjected to a basic recovery attempts using commercially available software tools. As Benkert puts it, “A five-year-old with some free software off of the web could have done it…” No specialized hardware or physical repairs were made to any of the over 250 devices.

PII recovered included credit card information, contact information, usernames and passwords, company and personal data, tax details, and more. While mobile phones had less recoverable PPI at 13%, tablets were disturbingly found with the highest amount at 50%. PII was found also found on 44% of hard drives. In total, 40% of the devices yielded PII.

Over the past 20 years there have been periodic studies of used hard drives purchased on the second-hand market. Robert Johnson, NAID CEO, points out that while this study’s results show a decrease in data found compared to past studies, “NAID employed only basic measures to extract data – imagine if we had asked our forensics agency to actually dig!” He goes on to surmise that “40 percent is horrifying when you consider the millions of devices that are out there.”

The conclusion is that individuals, organizations and even third party contractors are responsible for ensuring their data is not available to make it into the wrong hands when disposing of used devices, and many are not succeeding. This is one of the reasons that NAID exists, to provide a certification process so that organizations and individuals alike can trust that their data is being handled and disposed of properly.

SCOPE & PROCESS

CPR Tools was tasked to inspect and report the data contained on the storage media received for this project. The task was to perform basic data forensic transfer from working storage devices specifically using commercially available tools.

We were looking for the presence of any data and then identifying any PII that the devices may contain. (The steps listed below are a quick synopsis of how the process worked and are strictly to help the reader understand the steps taken but do not contain all the steps in the process.)
As each device was received at CPR Tools it was inventoried, assigned a unique number and the device model and serial number were logged into a database. The drives were given different color stickers to represent the different stages of their journey through the process.

Once the 'check-in' process was complete the devices were sent to a special storage area set aside in a separate lab for this project. There the data recovery engineers assigned to this project began the task of analyzing the media using commercially available tools (including our own data recovery tool, BitStorm) to copy data from the devices.

Once data was recovered we used commercially available tools to search or 'carve' the data for PII. All data was preserved forensically.

DEVICES

The devices received were a more representative view of what typical users own and thus discard: smart phones, tablets, and hard drives.

We received a total of 258 devices. Table 1 displays the device types and associated numbers that were tested for data in this project.

Device Type	Number of Devices Provided
Hard Disk Drives	214
Smart Phones	32
Tablet Computers	12
Total Devices	**258**

Table 1 - Device Types

The devices received were from different manufacturers, had different Operating Systems (OS) and interfaces. Table 2 shows the breakdown of the different types of interfaces and OS's we received.

Device	Interface/OS
Hard Disk Drives	SCSI, Fibre Channel, SATA, PATA
Smart Phones	Android and Apple
Tablet Computers	Android and Apple

Table 2 – Device Interfaces and OS

The significance of the different hard drive interfaces is that each interface is typically purchased for a specific type of task. As an example, SCSI and Fibre Channel hard drives are typically used in enterprise environments (servers).

METHOD(S)

All devices were subjected to what we consider a basic recovery attempt. We did not use specialized hardware or make any physical repairs to any devices. We did receive 4 devices that were 'Dead on Arrival' (DOA) or less than 1% which is consistent with our experience in purchasing devices from auction websites.

We used commercially available software tools for cloning and performing File System level analysis including deleted file space. Once completed all collected data was examined for Personally Identifiable Information (PII) again using commercially available tools. Personally Identifiable Information for this study is defined as two pieces of information that when together could be used to identify an individual.

RESULTS

Two of the hard drives and two of the smart phones were 'DOA' and thus were not tested. These devices were not included in the final percentages calculated.

We recovered PII data from 44% of the total working hard drives received. The data found on hard drives included the following information:

- Credit card information
- Names
- Addresses
- Photographs
- Videos
- Emails
- Usernames (files named users.doc etc)
- Passwords (files named passwords.txt etc)
- Company and Personal financial information
- Physical navigation history
- Internet navigation history
- Social media credentials
- Tax information

We recovered PII data from 13% of the total working smart phones received. The data found on smart phones included the following information:

- Names
- Phone numbers
- Addresses

We recovered PII data from 50% of the tablet computers we received. The data found on the tablets included the following information:

- Credit card information
- Names
- Addresses
- Photographs
- Emails
- Usernames (files named users.doc etc)
- Passwords (files named passwords.txt etc)
- Physical navigation history
- Internet navigation history
- Social media credentials

Table 3 provides an overview of the data discovered on the provided devices:

Device	PII Data	No Data	DOA	Total	Percentage
Hard Disk	92	120	2	214	44%
Phone	4	26	2	32	13%
Tablet	6	6	0	12	50%

Table 3 – Analysis of Data Recovered from Provided Devices

In sum, PII recovered included credit card information, contact information, usernames and passwords, company and personal data, tax details, and more. While mobile phones had less recoverable PPI at 13%, tablets were disturbingly found with the highest amount at 50%. PII was found also found on 44% of hard drives. In total, 40% of the devices yielded PII.

Johnson cautions that the results are in no way an indictment of reputable commercial services providing secure data erasure. “We know by the ongoing audits we conduct of NAID Certified service providers that when overwriting is properly done, it is a trustworthy and effect process. The problem lies with service providers who are not qualified and, too often, with businesses and individuals who feel they can do it themselves.”

ABOUT CPR TOOLS

CPR Tools Inc. performs basic through advanced data recovery services for individuals and organizations around the world. For more information visit https://www.cprtools.com/.

ABOUT NAID

The National Association for Information Destruction (NAID) is the international watchdog trade and non-profit trade association of the secure destruction industry, which currently represents more than 1,900 member locations globally. NAID advocates for a standard of best practices across governments and by service providers as well as suppliers of products, equipment and services to destruction companies. The mission of NAID is to promote the proper destruction of discarded information through education and to encourage the outsourcing of destruction needs to qualified contractors. For more information visit http://www.naidonline.org/, or follow us on Twitter and Facebook at @NAIDonline.

Contact:
Kelly Martínez
kmartinez@NAIDonline.org
+1 602-788-6243, ext. 2008