NAID Conducts Largest Second-Hand Device Study in the World To-Date

Personally Identifiable Information Found on 40 Percent of Devices

NAID has long included research among the tools it uses to educate consumer and policy makers. In fact, over the years, research has contributed to the association's regulatory advocacy and standards development, and added significantly to the association's credibility. In continuation of that tradition, NAID recently conducted the largest known forensic examination of second hand memory devices.

According to NAID CEO Bob Johnson, this is the type of research that sets NAID apart. "There's no shortage of conferences, magazines, and certifications looking for support," says Johnson. "To my knowledge, however, NAID is the only one with a rich history of reinvesting that economic support back into research to advance and promote secure data destruction."

This study was commissioned by NAID but conducted by a third party, CPR Tools Inc., to ensure the reliability and integrity of the results. The study revealed that 40 percent of devices resold in regular commerce channels contained personally identifiable information (PII) without taking heroic efforts to acquire it.

Overview

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.

CPR Tools was 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 CPR Tools 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.

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

Table 1 - Device Types

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

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 of the devices from the study.

Table 2 – Device Interfaces and OS

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

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).

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

Table 3 – Analysis of Data Recovered from 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%

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."