Chapter 35
An Australian Longitudinal Study Into Remnant Data Recovered From Second-Hand Memory Cards

Patryk Szewczyk
Edith Cowan University, Joondalup, Australia

Krishnun Sansurooah
Edith Cowan University, Joondalup, Australia

Patricia A. H. Williams
Flinders University, Adelaide, Australia

ABSTRACT

Consumers demand fast, high capacity, upgradeable memory cards for portable electronic devices, with secure digital (SD) and microSD the most popular. Despite this demand, secure erasure of data is still not a composite part of disposure practices. To investigate the extent of this problem, second-hand memory cards were procured from the Australian eBay site between 2011 and 2015. Digital forensic tools were used to acquire and analyze each memory card to determine the type and quantity of remnant data. This paper presents the results of the 2014 and 2015 studies and compares these findings to the 2011–2013 research studies. The longitudinal comparison indicates resold memory cards are disposed insecurely, with personal, confidential and business data undeleted or easily recoverable. The impact of such discoveries, where information is placed in the public domain, has the potential to cause embarrassment and financial loss to individuals, business, and government organizations.

DOI: 10.4018/978-1-7998-3025-2.ch035

INTRODUCTION

The demand for Secure Digital (SD) memory cards is driven by "personal data ecosystems" coupled with "personal data empowerment" as reported by the Global Industry Analysts (GIA) in 2016, and it is estimated that the global market for SD memory cards will reach US$11.2 billion by 2020 (Global Industry Analysts, 2016). This demand can be attributed to end-user generation of large quantities of personal digital data, resulting in an increased need for digital storage. Memory cards are versatile and found in many consumer-based electronic devices such as smartphones, tablet computers, portable media players, personal navigation systems, digital cameras, smart watches, and wearable medical devices (Dolcourt, 2014; Zheng et al., 2013). At the same time, the increase in the storage capacity of memory cards has eliminated the restrictions associated with the quantity and types of data that end-users can store on their electronic devices. Despite the freedom associated with storing "anything and everything", concerns are growing regarding end-users' ability to adequately erase personal and business data from their electronic devices (Pultarova, 2016).

There is an abundance of inadequately erased persistent storage devices on second hand auction sites, and the breadth of the problem is supported through numerous studies: private and confidential data has been recovered from second hand USB flash drives (Chaerani, Clarke, & Bolan, 2011; Robins, Williams & Sansurooah, 2016), hard disk drives (Jones, Valli, & Dabibi, 2009), smartphones (McColgan, 2014), and memory cards (Szewczyk & Sansurooah, 2011). Researchers from different countries who have conducted similar studies have concluded that recovered data was associated with individuals, businesses and government organizations, indicating that poor security practices are not restricted to individual consumers. Personally identifiable information (PII) has also been extracted from digital camcorders (Ariffin, Choo, & Slay, 2013), smart televisions (Sutherland, Reada, & Xynos, 2014) and car navigation systems (Lim, Lee, Park, & Lee, 2014) and it can be extrapolated that data on the emerging Internet of Thing (IoT) based devices would also be recoverable.

Confidential personal and business information is a valuable commodity (Gompertz, 2012). Indeed, cyber criminals have sourced used computers from second hand auction sites for the purpose of extracting and using the confidential data for financial gain (Arthur, 2009). This method may be regarded as less precarious than compromising a computer network; however, hobbyists have also acknowledged engaging in the procurement of second hand persistent storage devices to identify the types of data left by sellers (Frauenfelder, 2004). The process of recovering and extracting information has been made simpler due to an abundance of free digital forensic tools. Such tools are typically associated with the recovery of data from persistent storage for use in a court of law; however, the same tools can be used to extract data for malicious purposes.

The issues of securing stored confidential organizational information are compounded by the 'Bring Your Own Device" (BYOD) model, which permits end-users to utilize their electronic devices to complete work related tasks (Wang, Wei, & Vangury, 2014). Employees are also boycotting workplace technology in favor of using advanced mobile computing devices, obtained at their own expense (Donovan, 2014). Technological obsolescence motivates consumers to upgrade their electronic devices or persistent storage media in favor of the newest trend in technology (Obire, 2015). The storage of sensitive business information is particularly concerning in environments such as hospitals, where employees are often permitted to use personal devices to access and update patient records and medical databases (Fox & Felkey, 2015).