International Journal of Information Security and Privacy
Volume 12 • Issue 4 • October-December 2018

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.

KEYWORDS

Computer Forensics, Data Disposal, Data Recovery, Memory Card Forensics, Privacy, Remnant Data

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).

DOI: 10.4018/IJISP.2018100106

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).

For novice end-users, permanently wiping data from flash storage media may not be as straightforward as wiping data from a mechanical hard disk drive. Non-technical end-users may face challenges with selecting effective data erasure tools, and using them correctly. Further, previous research has demonstrated that hard drive-centric sanitization methods may not correctly erase data from flash-based storage devices (Goodin, 2011; Wei, Grupp, Spada, & Swanson, 2011). Consequently, whilst data erasure software may notify the end-user that the sanitization process has completed successfully, remnant data may still be readily accessible.

This paper reviews the first three years of the study into remnant data (2011-2013) and then presents the new data from 2014 and 2015. A comparison of the total study period is provided to identify the trends in data disposal. The factors attributed to this ongoing issue are examined and mitigation measures proposed. The research also provides an insight into the more worrying issue of breaches of privacy and the potentially detrimental impact thereof.

RESEARCH STUDIES 2011 - 2013

Research into remnant data on memory cards began in 2011 following the published outcomes of successful investigations into hard disk and USB flash drives (Chaerani, Clarke, & Bolan, 2011; Jones, Valli, & Dabibi, 2009). The focus on memory cards presents a new set of challenges, in that consumer electronic devices, such as cameras, smartphones and tablet computers, typically include proprietary data erasure mechanisms. For example, digital cameras have the ability to erase data on a memory card through a “quick erase” function or via a lengthy “low-level format”, and a consumer could reasonably assume that one of these functions would ensure a complete erasure of data from the memory card (Meyer, 2012).

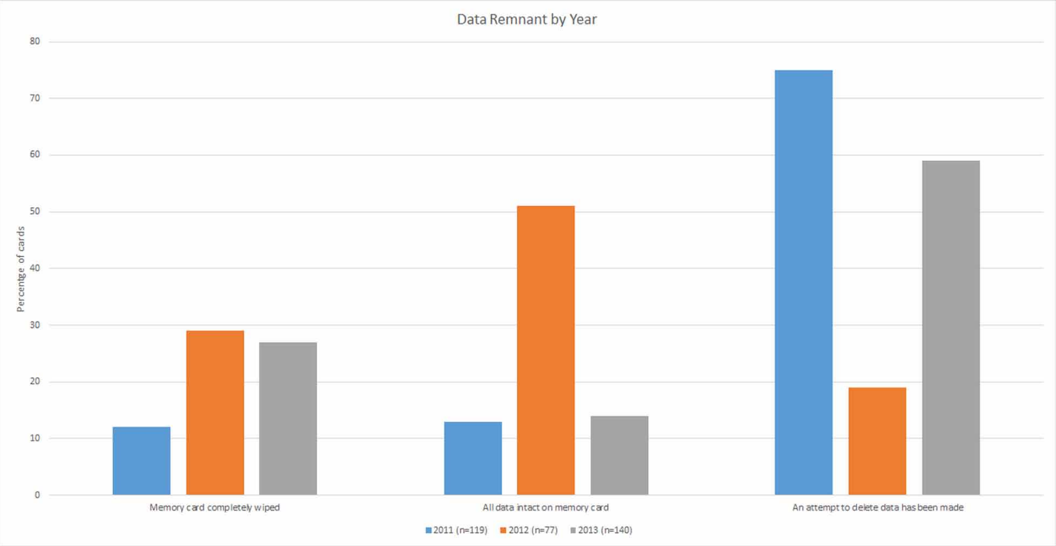
The 2011 research (Szewczyk & Sansurooah, 2012) demonstrated that a significant quantity of data was recoverable from memory cards. Of the 119 memory cards obtained in 2011, 88% contained recoverable data. It was also discernible that attempts had been made to remove data, with 75% of memory cards showing attempts at data erasure. Amongst the memory cards examined, 13% showed no sign of erasure procedure attempts and, as a result, data was readily accessible by directly connecting the card to an investigative workstation.

The results from the 2012 (Szewczyk & Sansurooah, 2012) and 2013 (Szewczyk, Robins, & Sansurooah, 2013) investigations were similar to those of the 2011 study. A decrease in the availability of memory cards on the second hand eBay market was identified in 2012, which resulted in only 78 memory cards being procured; this figure substantially increased to 140 cards in 2013. Figure 1 shows the breakdown of accessible data between 2011 and 2013.

Over the three years of research, the quantity and type of data recovered varied substantially. In 2011, a notable case was discovered in which detailed (high transaction) bank statements were recovered, an addition to employee pay slips, and legal firm and company documentation with letterhead. In 2012, a memory card was procured which contained a vast quantity of personal data. Amongst the files were personal resumes, job applications, utility bills, multimedia files, personal photos, and personal expense data stored in a spreadsheet (Szewczyk & Sansurooah, 2012). In 2013, sellers continued to disclose personal information. In one case a memory card contained numerous family holiday photos, photos of valid Australian passports, travel itineraries, and airline boarding passes (Szewczyk, Robins, & Sansurooah, 2013).

The outcome of the study in 2013 demonstrated an increase in the volume of confidential data recovered when compared to the preceding two studies (Szewczyk, Robins, & Sansurooah, 2013). The news and media attention, both in Australia and internationally, surrounding the investigation of storage media further demonstrated the severity of the security issues in relation to inappropriate disposal of persistent storage (Clarke, 2013; Gribbin, 2013; Munson, 2013; Orr, 2013). The presence of government and corporate data on a number of memory cards further demonstrated that appropriate persistent storage disposal practices and strategies were not being utilized (The Australian Business

Figure 1. Comparison of data remnants by year



Review, 2013). The subsequent 2014 and 2015 results are compared and contrasted with the results from the preceding years' research investigations.

METHODOLOGY

The procurement process targeted memory cards located on eBay Australia in the "mobile phone" and "camera" categories. Only memory cards which were listed by the seller as being used or refurbished were purchased. Multiple aliases were used on the auction site eBay Australia to avoid raising the suspicions and concerns of sellers. Each memory card was assigned a case number and was forensically acquired (*.dd) using the freely available software Access Data Forensic Toolkit Imager 3.1.2 (FTK Imager, 2015). Once a bit by bit forensic image was created, the physical memory cards were stored securely, together with all details pertaining to the sale. This process preserves the physical media and creates a chain of custody should criminal activity be discovered and the memory card required to be handed over to law enforcement. Analysis of each dd image was undertaken using X-Ways WinHex Specialist 17.5 (Reischmann, 2015), The Sleuth Kit Autopsy 3.0.9/4.0 (Carrier, 2016), Scalpel (Scalpel, 2016) and Bulk Extractor 1.5.5 (Bulk Extractor, 2016). The analysis and examination of each dd image focused on the type and quantity of recoverable data. The minor variations to this general approach used in the 2014 and 2015 studies were the updating of existing software and the introduction of additional digital forensic applications to validate results.

The 2011-2013 research identified that microSD and standard SD memory cards were the prominent media for containing digital content beyond graphics files. As a result, the purchasing procedure in 2014 and 2015 was altered to focus predominantly on purchasing SD and microSD cards, as these are the types of storage media one would expect to be used in smartphones, tablet computers and contemporary consumer electronic devices. Compact Flash cards are typically associated with Digital SLR cameras and are being slowly phased out. Legacy storage media such as miniSD, Memory Sticks and M2 memory cards are no longer used in contemporary electronic devices and hence were omitted from the research as of 2014.

Limitations of the Research

The potential inclusion of second hand memory cards from countries beyond Australia was considered. However, the cost of sellers shipping the items to Australia was deemed non-viable, as the postage cost was often 4 to 5 times greater than that of the memory card itself. In addition, Australian second-hand websites, including Gumtree and Quicksales, were also considered; however, neither of these online services included listings for used memory cards.

RESULTS

2014 Remnant Data Results

Figure 2 provides a breakdown of the one hundred and one (101) memory cards obtained during the 2014 study regarding their readability and erasure status.

Figure 3 shows the type of data recovered from the memory cards in 2014: as might be expected, some cards contained multiple file types. Photographic images were the prominent form of data recovered, which might be expected given that consumers now use mobile devices for photography rather than traditional cameras. For the purpose of this research, personal data stored as a photographic image was still classified as a photographic image, and was not considered in the overall scope of other types of documents recovered.

There were four notable cases in the 2014 study that included evidence of data that might be considered personal or sensitive:

Figure 2. 2014 memory card status - readability and erasure

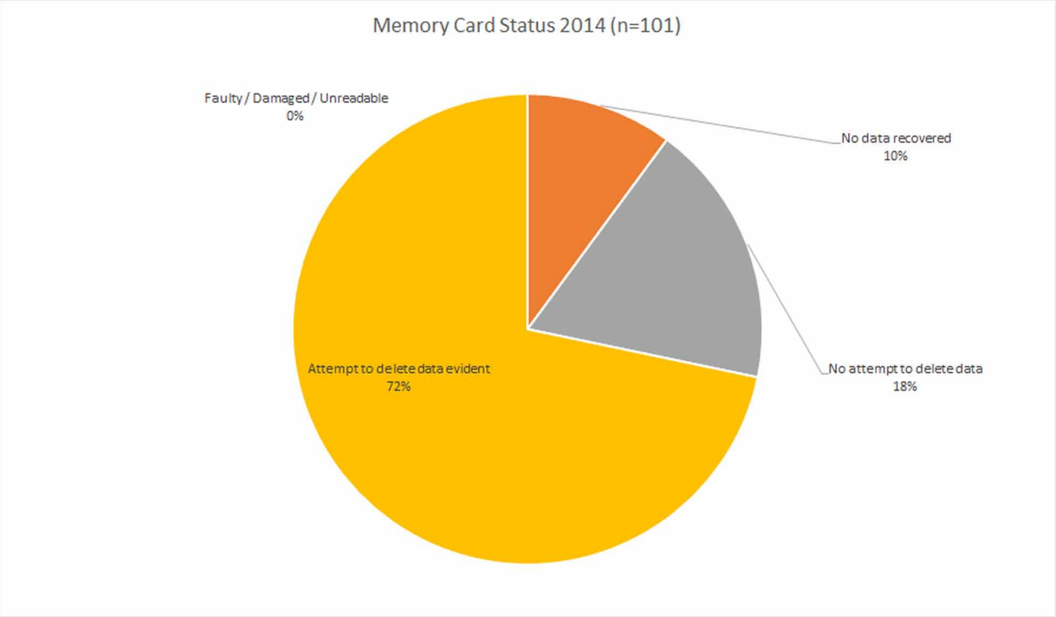
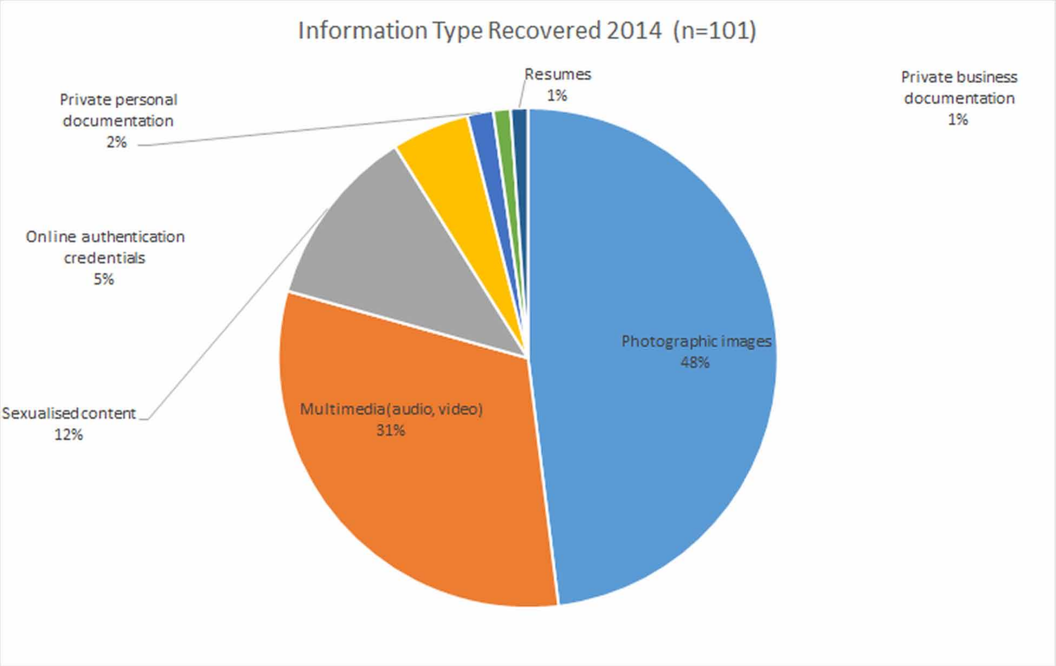


Figure 3. Types of information recovered in 2014



- Case 14 appeared to have been erased through a delete or format procedure. Despite this, many private and confidential documents were easily recoverable. Ninety-one documents were successfully recovered including a scanned birth certificate, legal affidavits, university qualifications, a comprehensive resume, immigration documents, a scanned passport, tax documents, telecommunication invoices, a bank statement, and various medical documents;
- Case 33 included a combination of both deleted and non-deleted files. The files which were intact and readily accessible without the use of data recovery or forensic tools had little sensitivity or interest to this study. Further recovery and examination of the deleted files identified a large quantity (approximately 1800) of photographic images. An analysis of each photographic image identified photos that had been taken of personal documents, screenshots of an Australian bank account, and, amongst alternative files of interest, a picture of a hand written document encompassing a significant quantity of authentication credentials to online social networking sites and online services utilized in Australia;
- Case 39 appeared to have been erased through a delete or format procedure. Given the large quantity of medical documents found on the memory card, it appeared to have belonged to a medical practitioner. Numerous referral letters were recovered with the name and signature of the medical practitioner consistently present. The memory card also contained employment pay slips, childcare documentation, mobile phone utility invoices, and numerous signed confidentiality agreements;
- Case 60 appeared to have been erased through a delete or format procedure. The data appeared to have belonged to a student at an Australian university. The memory card included a transcript of results pertaining to the student's degree and a series of assignment files and notes relating to their course. Numerous photographic images had been recovered from the memory cards, with a small quantity of these images being of a personal sexualized aspect. Personally identifiable details of the individual were consistent amongst all the data recovered.

2015 Remnant Data Results

Figure 4 provides a breakdown of the 167 memory cards purchased in 2015 with regards to readability and erasure.

Figure 5 depicts the types of information that were recovered. Some cards contained multiple file types.

Whilst there were multiple files containing data of a confidential or sensitive nature, the 2015 analysis revealed three particularly concerning occurrences:

- Case 16 included four memory cards from the same seller. The memory cards, of varying capacities, included a combination of undeleted files (all of a non-confidential nature) and many easily recoverable files (of which many were confidential and private). This case included a combination of pornographic material, assignment files pertaining to an educational institute in Australia, personal photos, and a series of photos of a valid credit card (front and back), an Australian passport, and an Australian driver's license;
- Case 32 had some content deleted, but had not been securely wiped. Amongst the files of interest were a scanned contract for the sale of land or residential property, a Government application form for funding, and an engineer's report for the associated land. The document itself contained personal contact details and detailed financial information of the buyer;
- Case 71 had all of its contents deleted, but had not been securely wiped. The memory card contained photos of hundreds of random individuals in the vicinity of a limousine. One spreadsheet file confirmed suspicions that the memory card belonged to a limousine business. The spreadsheet contained booking dates and times, pick-up and drop-off locations, credit card numbers, expiry dates, and credit card security values.

Figure 4. 2015 memory card status - readability and erasure

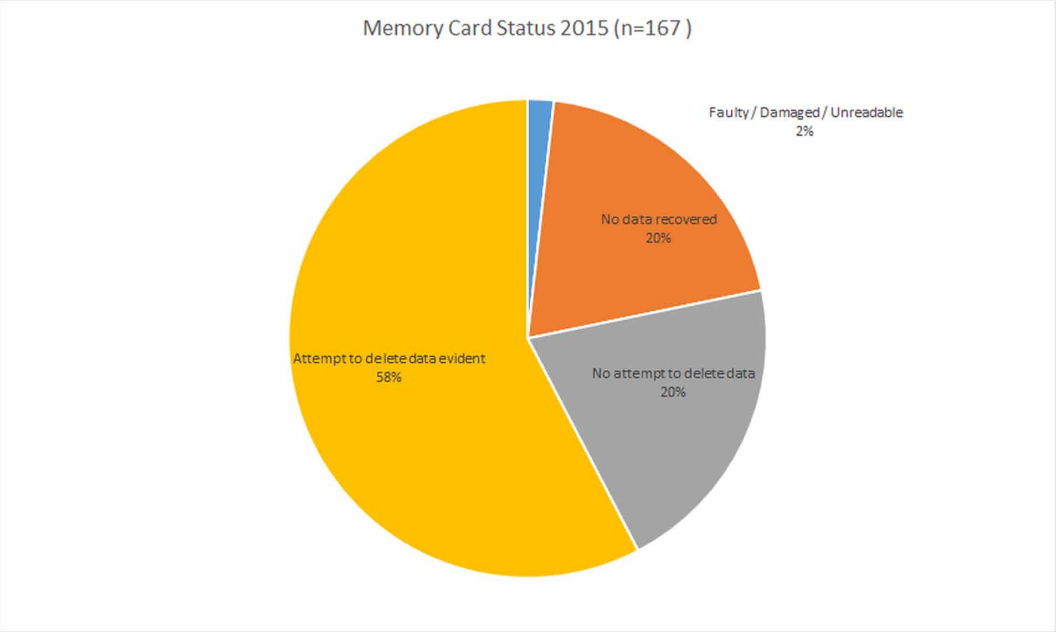
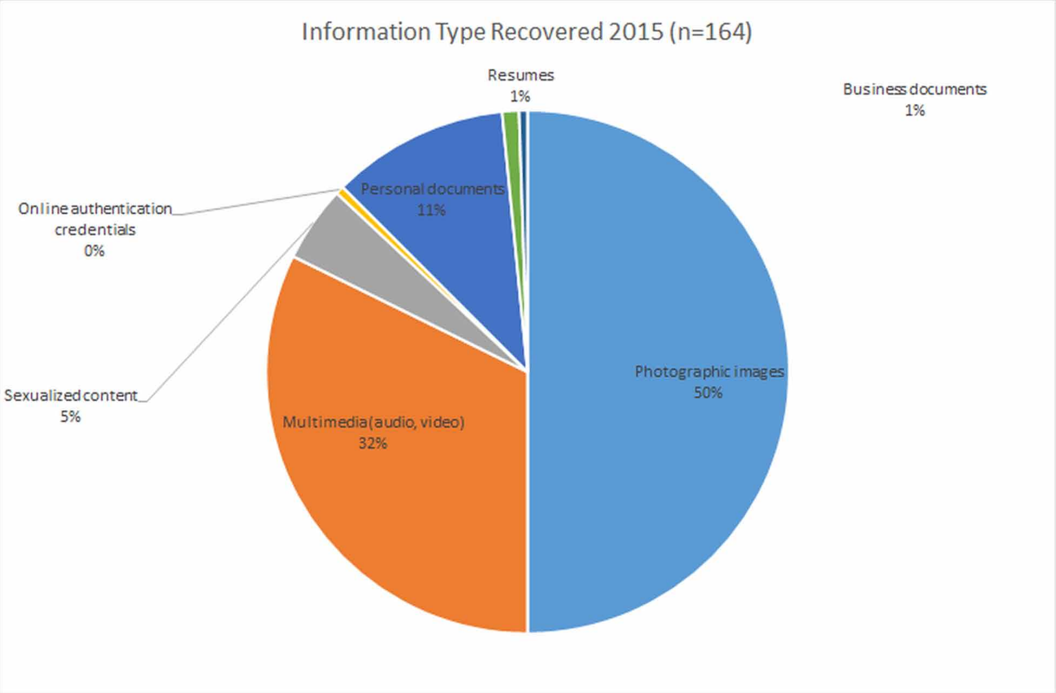


Figure 5. Types of information recovered in 2015



DISCUSSION

In order to understand the trends in the technology specification, recoverable data, and secure deletion attempts, the data from the 2011-2015 studies are compared. The availability of specific types of memory cards on eBay has evolved in line with changes in technology. At the commencement of this research in 2011, numerous types of memory cards were available on the second hand market and subsequently purchased consistent with the research criteria. As shown in Figure 6, microSD and standard SD cards were more commonly available throughout the duration of the five-year study. This may coincide with the increase in the number of personal electronic devices which use the microSD or standard SD memory card interface (Page, 2016). A technological evolution of persistent storage media was identified during the 2013 study. Consumers were predominantly selling microSD and standard SD memory cards. Alternative memory card types were occasionally listed and bid on during the 2014 and 2015 studies, but due to their scarcity, the researchers were often outbid in the procurement process.

The capacity of memory cards has increased significantly over the study period. Figure 7 shows the evolution of card capacity between 2011 and 2015. As larger capacity memory cards repeatedly emerged on the second-hand market, there has been a gradual decline in demand for lower capacity memory cards.

The presence of large quantities of photographic images and multimedia files on the memory cards throughout the study period is unsurprising. As illustrated in Figure 8, the volume of these files has fluctuated over the past five years. However, with the media continually exposing the issues of incorrect data disposal in Australia, there has been a progressive decline in the number of memory cards containing confidential data. This does not necessarily indicate that consumers are following best practices with regards to erasing data from memory cards.

There was a decline in the quantity of files containing data that would be considered private or of a confidential nature in 2014, which is a positive aspect. Analysis of the 2014 memory cards

Figure 6. Quantity and types of memory cards purchased during 2011-2015 period

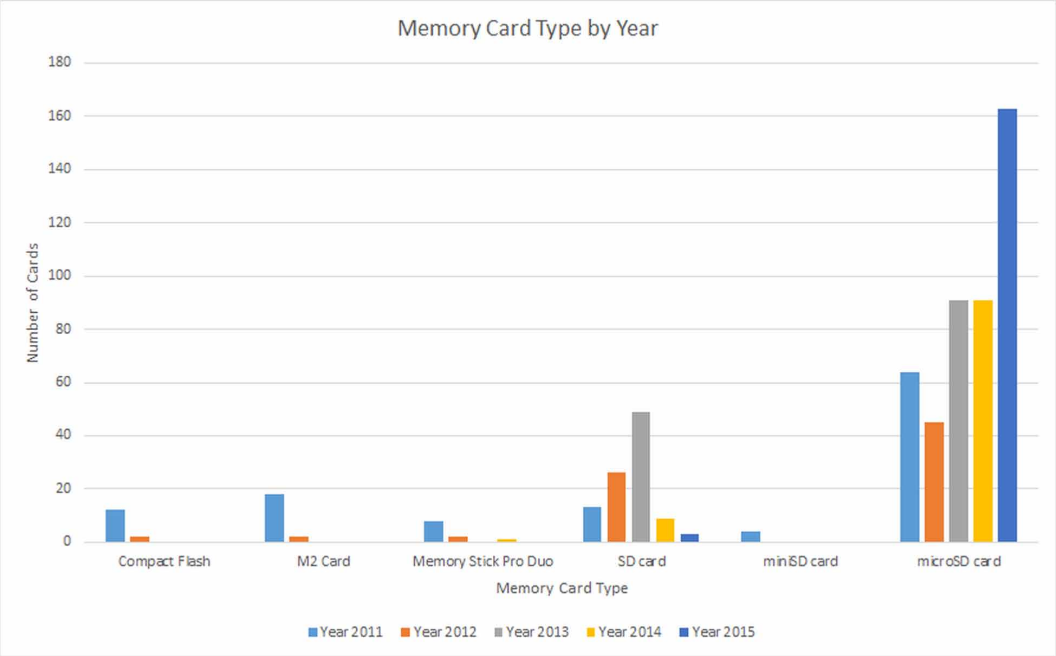


Figure 7. Capacity of memory cards purchased 2011-2015

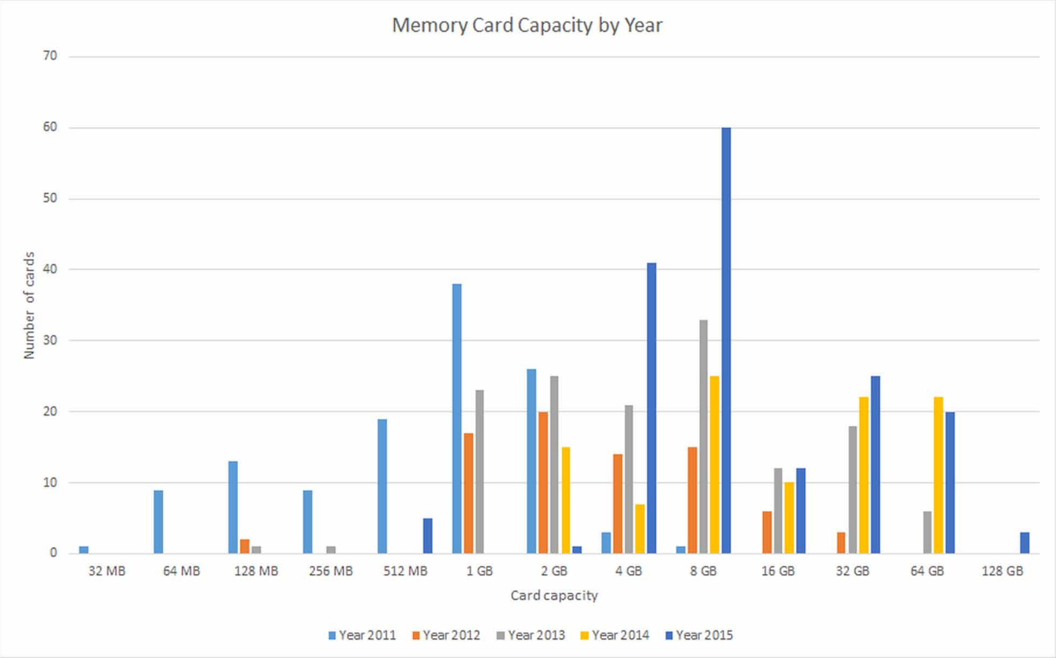
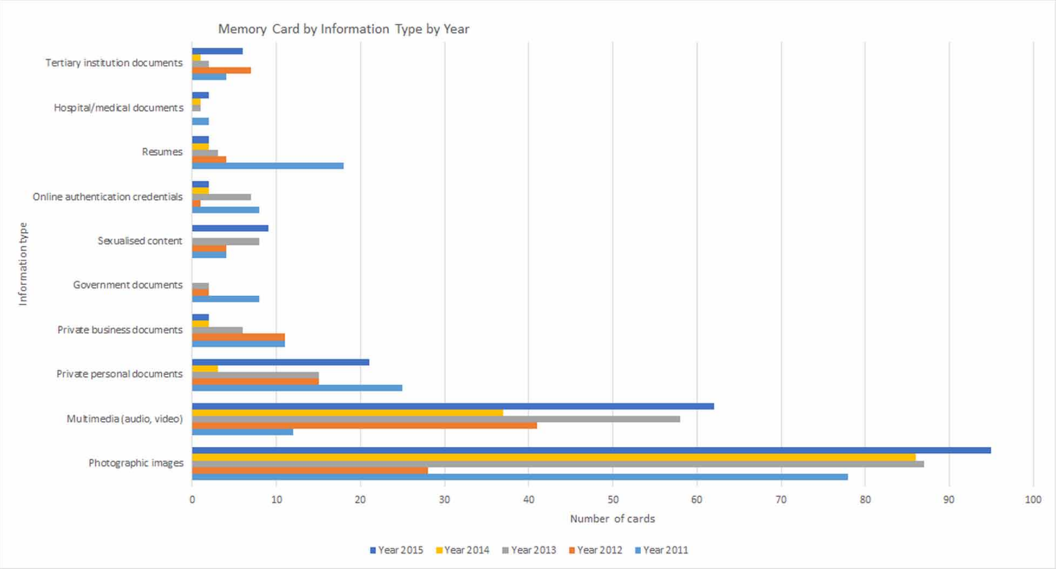


Figure 8. Quantity of memory cards containing specific types of information recovered 2011-2015



indicated a shift towards consumers taking photographic images of confidential data. The entire five-year study revealed that it is commonplace for end-users to take photos of personal documents. Storing personal documents as photos may allow the owner of a mobile computing device to quickly and easily access the information when needed. This practice raises a privacy concern as third parties or malicious software could access the confidential information with relative ease.

Australian print, radio and television media warnings were made public between 2011 and 2013 highlighting the issues of consumers disposing of persistent storage media inappropriately (DeCeglie, 2011; Gribbin, 2013; White, 2013). Unfortunately, as depicted by Figure 9, neither the memory card disposal practices nor the behavior of end-users have seen a steady positive improvement over the years.

An incidental observation of the research was that sellers appeared to encourage buyers to erase the data on the memory card prior to use. The 2014-2015 study period saw a few instances in which the seller would either directly message the buyer through eBay or include a note within the envelope stating that the memory card should be erased prior to use. These actions may encourage a buyer to purposefully interrogate the memory to locate data of interest. In one instance, the seller had apologized and stated that they did not have sufficient time to properly erase the memory card prior to sending it.

It was noted that during both the 2011-2013 and 2014-2015 study periods, sellers started to advertise the fact that memory cards had not been erased and consequently may still contain data (Figure 10). By employing these tactics, sellers may have intended enticing buyers to competitively bid on memory cards containing potentially desirable data. This study identified this trend by observing specific eBay usernames which that bid on used memory cards. Sellers who advertise their products as containing confidential data may encourage the potential buyer to examine the memory card containing undeleted data, whilst at the same time maximizing the potential profit in selling their memory card.

A discussion of the limited impact made by media publicity in promoting positive change from an organizational or individual perspective in relation to incorrect hard disk drive disposal was raised by Jones et al. (2009). The issues identified included: organizational constraints in new process development, lack of education and awareness of the issue, and a lack of priority given to the problem by government and organizations. In contrast, this research study determined that counteracting the problem is reliant upon the individual and their ability to make appropriate security conscious decisions towards their data.

Figure 9. Comparison of data erasure patterns

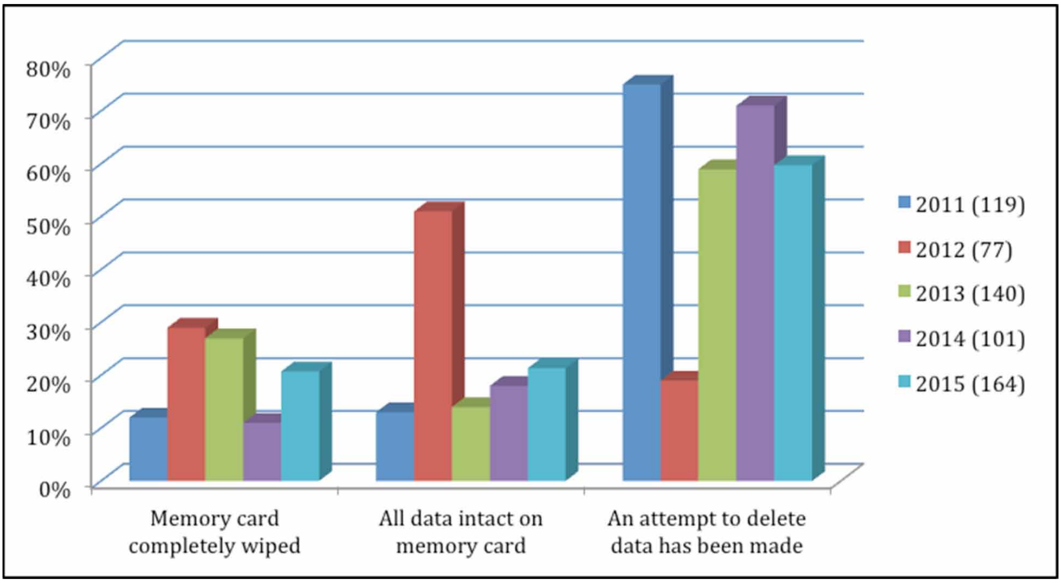
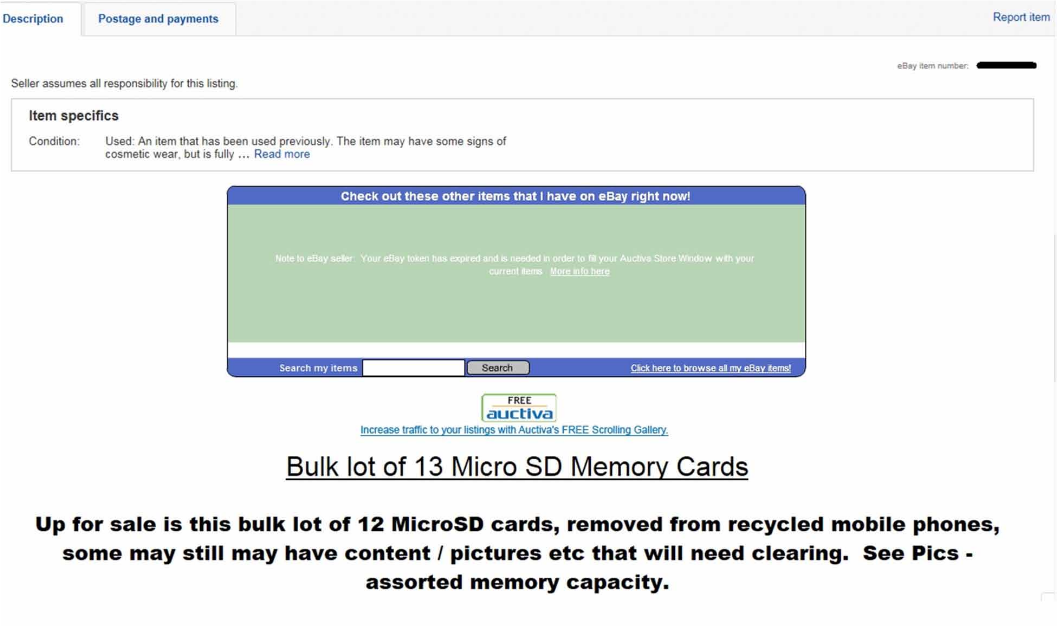


Figure 10. Advertising practices of sellers on eBay Australia



eBay item number: [redacted]

Seller assumes all responsibility for this listing.

Item specifics

Condition: Used: An item that has been used previously. The item may have some signs of cosmetic wear, but is fully … Read more

Check out these other items that I have on eBay right now!

Note to eBay seller: Your eBay token has expired and is needed in order to fill your Auctiva Store Window with your current items. More info here

Increase traffic to your listings with Auctiva's FREE Scrolling Gallery.

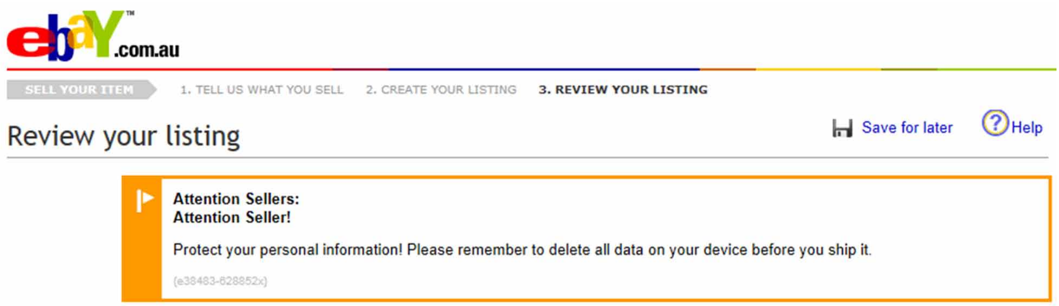
Bulk lot of 13 Micro SD Memory Cards

Up for sale is this bulk lot of 12 MicroSD cards, removed from recycled mobile phones, some may still may have content / pictures etc that will need clearing. See Pics - assorted memory capacity.

Proposed Solutions

Three solutions exist for ensuring that private data is not sold through second hand auction sites by consumers: user education, following secure data erasure practices, and policy enforcement by second hand auction sites. Toward the end of 2013, the issue of poor end-user data disposal practices received considerable coverage by the Australian media. At this time, sellers on eBay Australia were quick to remove their listings, and for a short period the quantity of used memory cards on eBay Australia decreased. Furthermore, following this media coverage the memory cards purchased as part of this project had been securely erased. Second hand auction sites began to promote positive security behavior to influence end-users who may be unaware of the potential issues. Unfortunately, however, the promotion of user education and awareness relating to poor data disposal practices has proved inconsistent. Figure 11 illustrates the warning provided to sellers upon listing a persistent storage item on eBay Australia during 2013. Unfortunately, as of 2014 this notification no longer appears; hence sellers receive no directive to ensure confidential data is securely erased prior to shipping the item to the buyer.

Figure 11. eBay Australia warning notification in 2013



Review your listing

Attention Sellers:
Attention Seller!

Protect your personal information! Please remember to delete all data on your device before you ship it.

(e38483-628852x)

Following secure data erasure practices is imperative in addressing the problem and ensuring that private data is not disclosed and exposed to malicious parties. It is impossible to stop consumers selling their surplus persistent storage devices, and thus it is important that secure procedural practices are followed to permanently remove data. There is a range of commercial and open source products available to securely wipe or erase persistent storage devices.

Availability notwithstanding, the effectiveness of these data erasure products is yet to be established. From an end-user's perspective, selecting an appropriate product can be overwhelming given the marketing hype and manufacturers' claims regarding the effectiveness of their tools. There is also the issue of operating system familiarity. For instance, Microsoft Windows does not provide a clear explanation and differentiation between "delete", "quick format" and "format" of persistent storage data. For example, when an end-user opts to quickly format a drive, a notification is generated stating, "WARNING: Formatting will erase ALL data on this disk". This misrepresentation of erasing all data may lead the novice end-user to believe that their data has been permanently erased from the target drive. Highlighting the lack of consistency with erasure tools, previous research examined the effectiveness of ten secure desktop based, data erasure tools (commercial and open source) (Sansurooah, et al., 2013).

From the ten tools investigated, only four proved to securely erase all data from the target drive examined. This is concerning given that end-users may trust the product used and form a belief that all data had been permanently erased. Furthermore, the commercial variants of the products tested resulted in the least permanently erased data, despite the vendors' positive claims regarding their products.

Unfortunately, data erasure software is not the only issue. Manufacturers of persistent storage are also known to give potentially misleading advice to consumers. For instance, SanDisk states that "Reformatting will clear file system corruption or quickly erase everything on the device" (SanDisk, 2015). SanDisk also provides the procedural instructions to be undertaken on Microsoft Windows to ensure this process is undertaken successfully. Unfortunately, formatting the target drive will not securely erase all data from the drive, thus leaving it vulnerable to data recovery.

Given the limited and misleading nature of information provided to consumers, it is not surprising that private data is continually emerging on second hand auction sites. Numerous researchers agree that additional precautions must be taken by end-users to sanitize their persistent storage devices prior to disposal (Jones, et al., 2009; Simao, et al., 2011; Grupp, Davis, & Swanson, 2012; Kessler, 2013). The need for easily accessible, reliable end-user education is paramount. The Australian government has a vested interest in protecting end-users and has accordingly funded two operational websites, namely the eSafety (eSafety, 2016) and Stay Smart Online (StaySmartOnline, 2016) information portals. Unfortunately, the information on these portals is limited, providing little support to a novice end-user. For instance, with regard to data on mobile computing devices, one website recommends that the end-user encrypts the contents of their device or avoids selling or disposing of the device; or properly delete the data on the drive (StaySmartOnline, 2015). The advice concludes there, with no additional procedural instructions given as to how to undertake these recommendations. Similarly, limited information is provided by Australia's largest telecommunication provider, Telstra, which encourages end-users to utilize dedicated file deletion programs or a third party service, yet gives no additional instructions should the end-user wish to pursue these actions (Telstra, 2015). Other telecommunication providers in Australia provide equally limited instructions on permanently erasing data.

CONCLUSION

This research provides a case study in remnant data from auctioned second hand memory cards in Australia. The results of the survey reveal that the problem is widespread and disposal of memory storage devices continues to pose a personal and corporate security and privacy threat.

Technology has evolved considerably in recent decades and so has the proliferation of digital storage devices such as flash memory technology. Such technologies have gained popularity and are used by millions of people across the world, replacing previous portable media and, to some extent, the external hard disk.

The volume and range of information recovered in the research studies discussed (2011-2015) could have a potentially profitable and destructive impact, as well as posing a risk to the identity and privacy of the individuals involved. From a criminal intent perspective, the information recovered was more than sufficient to impersonate individuals and provide a means to commit identity theft, or to undertake other nefarious activities such as blackmail. With corporate espionage a mechanism in the landscape of information warfare and competitive advantage, such recoverable information from organizations is highly valuable.

This research highlights the need for more end-user education with easily accessible and reliable information designed for the novice end-user. The need to protect information appropriately and to erase it securely is well understood, yet the failure of individuals and organizations to ensure this occurs relates to a lack of knowledge, and a lack of business policies and procedures. There is an ongoing necessity for corporate awareness, education, and training of staff and the public to ensure that the uses of flash technology devices are managed appropriately and that the data they contain is effectively protected and securely disposed of. For the home user there is a need for education and understanding of the implications of insecure disposal of devices.

From a privacy perspective, there are multiple aspects raised by the research to be considered. Firstly, the issue of personal privacy is highlighted, regardless of whether any laws have been contravened. Such concerns can have a significant and long-lasting impact on an individual. Secondly, where information is entrusted to an organization and subsequently finds its way onto a public auction website, this action may contravene national legislation such as the Australian Privacy Principles. Organizations have an obligation to protect personal information, whether or not they come under the Australian Privacy Principles (2012).

The research into remnant data on memory cards will continue within an Australian context, and an attempt will be made to pursue similar investigation on an international level. Australia is perceived as a country that is highly susceptible to cyber-criminal activity due its reluctance to adopt appropriate and adequate cyber security technologies and practices. As a result, future research at an international level will allow the researchers to compare and contrast data disposal strategies of other countries and identify where Australia is placed. Clearly, there are significant improvements to be made to ensure that confidential and private data is not disposed of incorrectly.

REFERENCES

Ariffin, A., Choo, K. R., & Slay, J. (2013). Digital camcorder forensics. *Proceedings of the Eleventh Australasian Information Security Conference (AISC '13)*, *138,* 39-47.

Arthur, C. (2009, Jan 8). Before you sell your computer, smash the hard drive, says Which? *The Guardian*. Retrieved from http://www.theguardian.com/technology/2009/jan/08/hard-drive-security-which

Australian Privacy Principles. (2012). *Australian Privacy Principles.* Australian Government, Office of the Australian Information Commissioner. Retrieved from https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles

Bulk Extractor. (2014). *Bulk Extractor (version 1.5.5)* [Software]. Available from http://digitalcorpora.org/downloads/bulk_extractor/

Carrier, B. (2016). *The Sleuth Kit (Version 3.0.9/4.0)* [Software]. Available from http://www.sleuthkit.org/autopsy/download.php

Chaerani, W., Clarke, N., & Bolan, C. (2011). Information leakage through second hand USB flash drives within the United Kingdom. In *Proceedings of the 9th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Clarke, T. (2013). Government data found on old memory sticks. *The Australian*. Retrieved from http://www.theaustralian.com.au/news/latest-news/government-data-found-on-old-memory-sticks/story-fn3dxiwe-1226772717895

DeCeglie, A. (2011, December 10). WA study reveals private details exposed in sale of second-hand memory cards. *Sunday Times*. Retrieved from http://www.perthnow.com.au/news/your-secrets-exposed/story-e6frg12c-1226218988783

Dolcourt, J. (2014). *Cross Country watch ridiculously encapsulates all of Android (hands-on)*. Retrieved from http://www.cnet.com/products/cross-country-smartwatch/

Donovan, F. (2014). *Bad tech at work puts pressure on enterprises to go BYOD*. Retrieved from http://www.fiercemobileit.com/story/bad-tech-work-puts-pressure-enterprises-go-byod/2014-10-15

eSafety. (2016). *eSafety.* Australian Government, Office of the eSafety Commissioner. Retrieved from https://esafety.gov.au/

Fox, B. I., & Felkey, B. G. (2015). Tech Trends We Are Watching in 2015: Health Information Technology Developments. *Hospital Pharmacy*, *50*(1), 84–85. doi:10.1310/hpj5001-84 PMID:25684805

Frauenfelder, M. (2004). *Hobby: buying used hard drives on eBay and unerasing the data for fun*. Retrieved from http://boingboing.net/2004/03/23/hobby-buying-used-ha.html

Global Industry Analysts. (2016). *Secure Digital (SD) Memory Cards – A Global Strategic Business Report*. Retrieved from http://www.strategyr.com/PressMCP-7679.asp

Gompertz, S. (2012). Watchdog finds undeleted data on second-hand disk drives. *BBC News.* Retrieved from http://www.bbc.com/news/technology-17827562

Goodin, D. (2011). Flash drives dangerously hard to purge of sensitive data. *The Register*. Retrieved from http://www.theregister.co.uk/2011/02/21/flash_drive_erasing_peril/

Gribbin, C. (2013). Selling second-hand memory cards online could bring serious risk of identity fraud: experts. *ABC News*. Retrieved from http://www.abc.net.au/news/2013-12-02/selling-second-hand-memory-cards-bring-risk-of-identity-fraud/5129848

Grupp, L. M., Davis, J. D., & Swanson, S. (2012). The bleak future of NAND flash memory. In *Proceedings of the 10th USENIX conference on File and Storage Technologies*. USENIX Association.

Imager, F. T. K. (2015). *Forensic Toolkit Imager (Version3.12)* [Software]. Available from http://accessdata.com/support/adownloads#FTKImager

Jones, A., Valli, C., & Dabibi, G. (2009). The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market. In *Proceedings of the 7th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Kessler, G. (2013). *Cybersecurity and Your Computer: What's At Risk and What Can You Do.?* Retrieved from http://www.garykessler.net/presentations/201303_TBE.pdf

Lim, K., Lee, C., Park, J. H., & Lee, S. (2014). Test-driven forensic analysis of satellite automotive navigation systems. *Journal of Intelligent Manufacturing*, *25*(2), 329–338. doi:10.1007/s10845-012-0653-6

McColgan, J. (2014). *Tens of thousands of Americans sell themselves online every day*. Retrieved from https://blog.avast.com/2014/07/08/tens-of-thousands-of-americans-sell-themselves-online-every-day/

Meyer, J. (2012). 49 seriously good Canon DSLR tips, tricks, time savers and shortcuts. *Techradar*. Retrieved from http://www.digitalcameraworld.com/2012/07/12/49-seriously-good-canon-dslr-tips-tricks-time-savers-and-shortcuts/3/

Munson, L. (2013). What Should We Do With Governments And IT Consultants Who Can't Look After Their Data? *BH Consulting*. Retrieved from http://bhconsulting.ie/securitywatch/?p=1858

Obire, T. (2015). Between technological obsolescence and consumer spending. *Vanguard*. Retrieved from http://www.vanguardngr.com/2015/01/technological-obsolescence-consumer-spending/

Orr, A. (2013). Homemade sex tapes and identity details sold on old digital devices. *WA Today, WA News*. Retrieved from http://www.watoday.com.au/wa-news/homemade-sex-tapes-and-identity-details-sold-on-old-digital-devices-20121202-2am5i.html

Page, C. (2016). Galaxy S8 release date, price, specs and features. *The Inquirer*. Retrieved from http://www.theinquirer.net/inquirer/news/2462247/galaxy-s8-release-date-price-specs-and-features

Pultarova, T. (2016). Improper disposal of electronic devices puts data at risk. *Engineering & Technology*. Retrieved from http://eandt.theiet.org/news/2016/mar/hard-drives-disposal.cfm

Reischmann, S. (2016). *X-Ways Software Technology (Version 17.5)* [Software]. Available from http://www.winhex.com/winhex/

Robins, N., Williams, T., & Sansurooah, K. (2016). I know what you did last summer... An Investigation into Remnant Data on USB Storage Devices Sold in Australia in 2015. *Proceedings of the Australasian Computer Science Week Multiconference (ACSW '16)*. doi:10.1145/2843043.2843356

SanDisk. (2015). Formatting a memory card, flash drive or device using a PC. *SanDisk*. Retrieved from http://kb.sandisk.com/app/answers/detail/a_id/312

Sansurooah, K., Hope, H., Almutairi, H., Alnazawi, F., & Jiang, Y. (2013). An Investigation in the efficiency of forensic data erasure tools for removable USB flash memory storage devices. In *Proceedings of the 11th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Scalpel. (2014). *Scalpel (Version 1.60)* [Software]. Available from https://github.com/sleuthkit/scalpel

Simao, A. M., Sicoli, F. C., Melo, L. P., & Sousa, R. T. (2011). Acquisition of digital evidence in android smartphones. In *Proceedings of the 9th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

StaySmartOnline. (2015). Android smartphones not securely deleting user data. *Australian Government*. Retrieved from https://www.communications.gov.au/what-we-do/internet/stay-smart-online/alert-service/android-phones-not-securely-deleting-user-data

StaySmartOnline. (2016). Stay Smart Online. *Australian Government*. Retrieved from https://www.communications.gov.au/what-we-do/internet/stay-smart-online

Sutherland, I., Reada, H., & Xynos, K. (2014). Forensic analysis of smart TV: A current issue and call to arms. Journal Digital Investigation. *The International Journal of Digital Forensics & Incident Response*, *11*(3), 175–178. doi:10.1016/j.diin.2014.05.019

Szewczyk, P., Robins, N., & Sansurooah, K. (2013). Sellers Continue to Give Away Confidential Information on Second Hand Memory Cards Sold in Australia In *Proceedings of the 11th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Szewczyk, P., & Sansurooah, K. (2011). A 2011 investigation into remnant data on second hand memory cards sold in Australia. In *Proceedings of the 9th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Szewczyk, P., & Sansurooah, K. (2012). The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia. In *Proceedings of the 10th Australian Digital Forensics Conference*. Perth, Australia: Academic Press.

Telstra. (2015). Safeguarding Your Devices: Cyber Safety Tips. *Telstra.* Retrieved from http://www.telstra.com.au/consumer-advice/download/document/cyber-safety-consumer-safe-guarding.pdf

The Australian Business Review. (2013, Dec 2). Government data found on memory sticks. *The Australian.* Retrieved from http://www.theaustralian.com.au/business/technology/government-data-found-on-memory-sticks/story-e6frgakx-1226773129880

Wang, Y., Wei, J., & Vangury, K. (2014). Bring Your Own Device Security Issues and Challenges. In *Proceedings of the 11th Annual IEEE Consumers Communications & Networking Conference*. Las Vegas, NV: IEEE.

Wei, M., Grupp, L. M., Spada, F. E., & Swanson, S. (2011). Reliably Erasing Data From Flash-Based Solid State Drives. In *Proceedings of the 9th USENIX Conference on File and Storage Technologies*. San Jose, CA: USENIX.

White, N. (2013). *Personal data recovered in USB swipes*. Retrieved from http://www.sciencewa.net.au/topics/technology-a-innovation/item/2417-personal-data-recovered-in-usb-swipes/2417-personal-data-recovered-in-usb-swipes

Zheng, J., Shen, Y., Zhang, Z., Wu, T., Zhang, G., & Lu, H. (2013). Emerging wearable medical devices towards personalized healthcare. *Proceedings of the 8th International Conference on Body Area Networks*. doi:10.4108/icst.bodynets.2013.253725

Patryk Szewczyk is a cyber security/digital forensics lecturer at Edith Cowan University (ECU), Perth, Western Australia. Patryk is also a researcher and committee member for the ECU Security Research Institute. He has served as a reviewer for numerous international journals and conferences. Patryk has attained national awards for his research and community service achievements towards addressing end-user cyber security challenges. His research focuses on the human factor issues emerging from the evolution of ICT coupled with the digital investigations of small-scale digital devices.

Krishnun Sansurooah is a cyber security lecturer at Edith Cowan University (ECU), Perth, Western Australia and a member of the ECU Security Research Institute (ECU-SRI). His doctorate focused on the development and creation of a validated forensic framework and method for the acquisition and extraction of data from NAND flash memory storage chips. Hence, generating new knowledge and perspectives on ways to acquire and extract raw data from NAND flash memory storage device. He has achieved a Masters of Internet Computing, and completed his Bachelor Honours in Computing and Information Science. His professional associations include the Australian Computer Society (ACS), the Australian Information Security Association (AISA), Health Level 7 Australia (HL7) and the Australian New Zealand Forensic Science Society. His areas of research include Digital Forensics, USB Forensics, Embedded System Forensic, Small Devices Forensic, E-Health, Information and Data Privacy.

Trish Williams is a leader in research and innovation in digital health and cyber security. Trish is Cisco Chair and Professor of Digital Health Systems at Flinders University in South Australia, and co-director of Flinders Digital Health Research Centre. Internationally recognized in her field, Trish applies 30 years' experience in healthcare computing to research and practical outcomes in cyber security, health IoT, mobile health, medical devices, governance, patient safety, and health software safety. A passionate contributor and advocate for digital health informatics standards, Trish is co-chair HL7 International Security Workgroup and nominated national expert on many ISO standards. She is co-editor of HISA's Privacy Guideline and the E-Safety Professional Practice Standard, was primary author of the RACGP Computer and Information Security Standards, and has over authored over 120 medical information security and safety publications.