ISSN: 2473-3857
v3 n4338

Digital Footprint on Mobile Devices: Donate Your Phone, Donate Your Life

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department, St. Vincent College
Latrobe, PA 15650

Elizabeth Loftus
ejoloftus@outlook.com
CIS Department, St. Vincent College
Latrobe, PA 15650

Abstract

The concept of the "digital footprint" – the trailing wake of data that everyday people leave behind in their modern online lives - has been around for as long as the World Wide Web has been public. With the spread of social media and increase in services for education and government agencies online, this footprint has expanded dramatically. 2017 marks a 10 year anniversary of practical smart phones. This past decade has seen rapid advancement of the capabilities in processing power and the capacity of the data streams that feed these devices. They have truly become the primary computing device for the majority of people today. With that use, these devices have also become the epicenter of the digital footprint repository. Through the force of carrier contracts and pace of market/technology development, many people are also cycling through new mobile devices every two years. Many trade in their old device, some donate to a worthy cause, and others simply throw them away. Not many people stop to think - What happens to all of the "you" collected on that old phone once it leaves your hands? This study examines thirty five phones that had been donated to charity to discover how much of the digital life of the previous owner has been left behind.

Keywords: Identity Theft, Mobile Forensics, Digital Footprint, Cybersecurity

1. INTRODUCTION

A digital footprint is considered to be the data related to a person that exists as a result of their online activity (IS, 2014). This footprint has grown larger and more diverse as more and more everyday functions and services have moved online. The amount of data that exists pertaining to each person varies, but regardless of size it has become a primary source of investigating people for jobs, relationships, or for darker motives such as identity theft. Much of this data exists outside of any individual's complete control, leaving people at the mercy of security and ethical practices of someone else.

For many, the primary device on which they access the internet has now become their phone or mobile device. While the educational efforts of raising awareness have informed masses of people on the enormity of data that exists about them "in the cloud" many have lost sight on just how much that footprint extends onto their physical devices, such as their phone, which they do have control over and possession of.

The Pew Internet project fact sheet for January of 2017 relates that 95% of Americans own a cell phone of some kind, with smartphone ownership at 77% (Pew, 2017). In the same study, it is also reported that nearly 20% of 18 to 29 year olds report that their smart phone is their only personal connection to the Internet. In January of 2016 the International Data Corporation reported that more than 1.4 billion smartphone shipped globally (Gartner, 2016).

With that use, the smartphone has become the epicenter of the digital footprint repository. Through the force of carrier contracts and pace of market/technology development, many consumers cycle through new mobile devices every two years. Many people trade in their old device, some donate to a worthy cause, and others simply throw them away. Not many people stop to think - What happens to that repository of "you" once that old phone leaves your hands?

The purpose of this paper is to investigate the following research question: How much personal data can be found on cell phones donated to charity?

2. BACKGROUND

Digital Footprint

A digital footprint is a trace of identifying information that is created through online activity (Internet Society, 2014). A digital footprint is created as we share information on the Internet, be it through posts on social media, comments on online forums or even using cloud storage servers (Osborne & Connelly, 2015). Digital footprints can be strung together to create trails of interaction on the Internet, posing dangers and risks to personal information not intended to be seen by the public eye. When a user sends an email, updates her Facebook status or posts a picture on Instagram she adds to her digital footprint, thus elongating the trail which she has established over her time in the digital age.

Digital footprints should be a significant privacy concern for Internet users, because they can be used to track user actions and are a basis for "profiling" by online service providers and others. Over time, the technology to create profiles of Internet users has become increasingly sophisticated. Few users realize how extensive their digital footprints are, and or how commonly the resulting data is shared by third parties (WSJ, 2012). The more information a user offers to the public over digital mediums, the greater the concern for her personal information security.

Increasingly awareness has been drawn to the extension of the digital footprint to multiple devices. Cached content, temporary files, deleted but not overwritten drive sectors, backup tapes, public access computers, retired laptops, et al, the amount of places that data can exist on hardware is almost incalculable. This has become increasingly complicated with the advent and adoption of automation and smart devices in business and the home. Mark Stokes, the head of Scotland Yard's cyber and communications forensics unit has increased the focus on training investigators to detect evidence on everything from internet-connected refrigerators, light bulbs, washing machines, vacuum cleaners, coffee makers and voice-controlled robotic assistants (Smith, 2017). Several cases have recently worked through the court system relying on evidence from IoT devices. In Bentonville, Arkansas a search warrant was granted to search the memory of an Amazon Echo device in relation to a murder investigation (Novet, 2016). The same police department has successfully utilized data from an internet connected water meter in a 2013 murder investigation (Sitek and Thomas, 2016).

In November of 2013, WTHR of Indianapolis ran an investigative report focused on Goodwill Industries of Central Indiana. In the investigation, a reporter visited one of the main distribution centers that allows access to mass bins of unsorted donated items. Merchandise is not on hangers, not organized, and not even priced. It is sold by the pound. The reporters were at this location because of a whistleblower consumer who repeatedly found boxes, furniture, or even luggage containing personal documents that included everything from pay stubs, medical records, and tax returns. After the segment aired, Goodwill responded by changing their internal policy to shred documents whenever found. However, subsequent visits proved a spotty enforcement of the policy at best (Segal, 2013).

On April 10, 2010 CBS News aired an investigative report that provided further example that our digital footprints are large and often hidden from our primary sight. The piece by Armen Keteyian came during the 50th anniversary of the ubiquitous steady workhorse of office machinery – the copy machine (Keteyian, 2010). In those fifty years the copy machine had undergone drastic evolution from a more manual piece of machinery such as mimeograph machines, to devices that are as complex and powerful as standalone personal computers. Since the early 2000's, almost every

ISSN: 2473-3857
v3 n4338

multifunction printer/scanner/copier (MFP) is a computer. In the segment, it was shown that a grave vulnerability lies within these printers – the hard drive. MFP's have become very expensive pieces of office equipment. Most companies do not own their own, opting to lease. Often they are rotated out after three to five years. Their greater lifespan can be ten to fifteen years or more. The aftermarket for used machines is great with high demand for their cost savings over new models. It is not uncommon to see a MFP that has been in four or more different offices for different companies over time. In the report, 4 copiers were purchased from a used equipment warehouse for an average of $300 each. All four held sensitive documents. One machine was from a sex crimes division of a metropolitan police force and held documents related to criminal cases. A second was found to be from another police department narcotics division that contained documents that included details of suspects in drug raids amongst other information. The third had been used in an architectural firm and it contained structural design plans for building in Manhattan, one a block from Ground Zero as well as 95 pages of Human Resource documents for payroll that included social security numbers and pay stubs. The final MFP had been placed with a medical insurance company and produced over 300 pages of private medical records including prescriptions, blood test results, and a cancer diagnosis.

Mobile Phones

A similar situation is occurring with the evolution of cell phones which have moved from single purpose devices to multipurpose with multiple channels of connectivity. Early mobile phone efforts revolved around radio phones and other existing technologies. In 1973, Martin Cooper made the first phone call over a handheld subscriber network as a researcher for Motorola (Shields, 2003) (Cooper, et al. 1973). By 1983, the Motorola DynaTAC 800x was released commercially to be the first to take advantage of the 1G network (AP, 2005). It was priced at around $4,000 and lasted for 30 minutes of talk time.

Between 1983 and 1999, most phones remained just that, a phone and primarily used to simply make calls. Pagers were still very much a relevant stand-alone device, and several Personal Data Assistant (PDA) devices also made in roads to the market place. However, it was not until the Blackberry 850 released late in 1999 that an integrated phone, texting, and e-mail connected device provided a single solution (Davis, 1999). The Blackberry was an instant and massive success. Their dominance of the market was not to last, however. As the Blackberry integrated four services into one device (E-mail, pager/text, PDA, and E-mail), Apple was about to remind the public that they liked music too.

Debuting in 2001, the Apple iPod was not the first mobile digital music player, but it did take over the market and overwhelm all others. Through integrating the iPod and iTunes Store with early smart phones, it is said that Steve Jobs became very frustrated with the existing devices of the era and proceeded to develop the iPhone which deputed in January of 2007 (Lewis, 20017). As with the iPod, the iPhone was not the first "smart phone" but it did combine existing features in a package unlike any of the other options in the market at the time (Mather, 2007).

As iOS for the iPhone has its origins in a music player, so too Android began its life with a distinctly different purpose. Android Inc. originally pitched their project as having "tremendous potential in developing smarter mobile devices that are more aware of its owner's location and preferences" (Elgin, 2015, para. 3). By mid-2005 Google had bought Android for $50 million (Manjo, 2015). A growing Google clearly had eyes set on entering the phone market throughout 2006 and in later years a never-to-market prototype surfaced that showed the first Google phone design to be very similar to a Blackberry with no touch screen and a physical QWERTY keyboard (Ziegler, 2012). The subsequent appearance and initial dominance of the iPhone pushed Google's efforts back to late 2008.

In the years since, both platforms (iOS and Android) have continued to develop into multifunction computer operating systems, to the point where the primary use of the device is hardly ever to simply make a call.

Phone market place is determined in multiple ways. Two of the most accepted metrics are Units sold in quarter and Browsing (page view) statistics.

The Gartner Group reported the following statistics from the third quarter of 2016 (Gartner, 2016):
Android: 87.8%
iOS: 11.5%
Windows: 0.4%
Blackberry: 0.1%
Others: 0.2%

For the April of 2017, StatCounter reported the following browser page view statistics (StatCounter, 2017):

Android: 71.42%
iOS: 19.95%
Windows: 0.99%
Blackberry: 0.33%
Others: 7.31%

The Pew Internet project fact sheet for January of 2017 relates that 95% of Americans own a cell phone of some kind, with smartphone ownership at 77% (Pew 2017). In the same study, it is also reported that nearly 20% of 18 to 29 year olds report that their smart phone is their only personal connection to the internet. In January of 2016 the International Data Corporation reported that more than 1.4 billion smartphone shipped globally. It is becoming apparent that for many, the smartphone has become their primary computing device.

Identity Theft

According to the US Department of Justice, "Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain" (USDOJ, 2017, para.1).

With a digital age, criminals no longer have to "dumpster dive" to find personal information about a potential victim. With so much of a life lived online, the digital footprint provides all the points of data a thief could need. Once that data is collected, the next step for a criminal is to pose as that person to take control of bank accounts, social media and e-mail accounts, and in some cases even to live as the person (Hegeman, 2013). At Defcon, the leading conference for all things cybersecurity, traditionally one of the most popular events annually is the Social Engineering CTF (capture the flag) contest (Weise, 2016).

While these contests might make social engineering and impersonation seem to be a fun game, it is certainly not - and certainly illegal. As with most crimes related to fraud, the numbers are presumed to be underreported, but the US Federal Trade Commission Consumer Sentinel Network has been working to collect statistics related to identity theft across several law enforcement organizations including the FBI, state Attorney Generals offices, the US Secret Service, and other agencies. The Consumer Sentinel Network data book for January through December 2016 reported nearly 400,000 complaints officially filed. These cases amounted to over $744 million in losses (FTCCSN, 2016).

Not all identity theft is for monetary gain. In a harrowing story, Wired magazine reporter Mat Honan detailed the moments he lost his digital life to a "hacktivist". The story begins, "In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook (Honan, 2012a, para. 1)."

The details of this "hack" are scary in many ways. The victim was no neophyte, he worked as a technology writer for a leading technology magazine. The hacker never needed what many consider to be the key piece of data for this type of takeover, the social security number. It all happened within an hour. When he was finally able to confront the hacker by creating a second twitter account to message the hacker on his original twitter account, the reason that he was a target was very surprising, "the hack was simply a grab for my three-character Twitter handle. That's all they wanted. (Honan, 2012a, para. 29)."

Mobile Phone Forensics

In a follow-up article, Mat Honan was able to write about the process he had to go through to resurrect his digital life. Of all the items that he had lost, the most valuable to him were locally stored pictures of his family that had been erased when his laptop had been compromised. His laptop was a MacBook Air, which contains a SSD (Solid State Drive) for mass storage. He was able to have much of the drive recovered through a company that specializes in drive forensics, DriveSavers (Honan, 2012b).

Mobile phones also use a form of SSD storage to maintain their operating system and storage space, however it is different than a regular computer. Mobile devices do not store data in the same fashion as a standard computer, which typically utilizes a hard drive for secondary storage. Instead, mobile devices make use of flash memory for non-volatile memory (Simon & Anderson, 2015). Flash memory is also a form of solid state storage, but it allows faster access to data than a traditional hard drive in addition to its lack of moving internal parts (Tyson, 2000).

ISSN: 2473-3857
v3 n4338

Flash memory is a type of electronically erasable programmable read only memory (EEPROM), allowing for storage of smaller sized pieces of data but makes each piece capable of being deleted and overwritten.

In addition to overall differences between mobile device internal storage and standard computers, supplementary onboard storage components also vary between Android operating devices and iOS operating devices. Primarily, devices manufactured to operate a version of Android are designed to allow users to insert a microSD card, allowing the user to expand the non-volatile memory. With varied storage situations among mobile devices, mobile forensic technology must be progressively versatile to comply with these dissimilarities. However, the countless assortment of mobile devices available to consumers has made forensic imaging more difficult, and it is believed that only half of all mobile devices in existence can be imaged in the same way as a computer, bit-by-bit, using forensic software (Messemer, 2012).

When Apple first debuted the original iPhone in June 2007, the storage specifications were meek compared to newer models. The maximum capacity of the original iPhone ranged from 4GB to 16GB of flash memory, without the option of expanding by means of additional storage devices such as micro SD cards. These original iPhones also only had up to 128MB of RAM (Sanford, n.d.). As the iPhone evolved over the years, the basic idea of two types of memory, Flash and RAM, remained consistent. The latest model of the iPhone, the iPhone 7 has storage specifications of up to 256GB of flash memory and 2GB of RAM (Apple iPhone 7, 2017). Devices that operate iOS are all manufactured by Apple Incorporated, and therefore, have narrower variations on device storage components.

Devices that operate the Android operating system have far more expansive variations than iOS devices. The storage specifications for devices operating Android vary because there are many different manufacturers which distribute devices with the same base operating system, as opposed to mobile devices manufactured by Apple Incorporated. The basic specifications of the Android operating system are similar across all devices, but each device has variations on storage specifications and what version of Android is in use. One of the primary differences between Android operating devices and iOS devices is that the former allows for expanded secondary storage using micro SD cards. These micro SD cards can vary in sizes from as small as 2 gigabytes to as large at 256 gigabytes.

Forensic examiners have pointed out the issues that arise from the fragmentation of Android operating devices. The security patches that reach some devices do not reach all, and firmware updates do not reach the whole Android operating community. In 2012, approximately 800 variances of Android operating devices were in existence that were not all operating the same version of the operating system (Messemer, 2012).

The inconsistencies between these devices makes it difficult to implement a truly efficient mobile forensic software that works across all platforms (Bennett, 2012). Mobile technology's constant growth calls for greater needs in the development of effective forensic software, tools and techniques to successfully image mobile devices of all operating system variations.

3. METHODOLOGY

Based on the experience of Wired reporter Mat Honan, and unfortunately many others, very little personal information is necessary for an identity thief to take control or do damage. For this study, a list of fourteen personal data markers was developed based on multiple sources advising the public on what details of their personal lives they should protect to prevent Identity theft. (Pacer, 2016; Acuant, 2016; CIMIP, 2016; IS2013) The markers used for this study were: Name (First, Last); Address; Phone Number; Primary E-mail Address; Secondary E-mail Address; Birthday; Text Messages; E-mail Messages; Personal Pictures; Calendar Entries; Social Media (A: Account; B: Social Media content); and Documents.

As a source for phones, Goodwill Industries operates ShopGoodwill.com as an online auction site. Regional distribution centers are able to place items up for auction that they deem more valuable, attractive to a broader audience, or not practical for display in a retail location. As a charity, the staff at the distribution centers is primarily comprised of volunteers. It is not expected that they would have specific technical training in relation to computers or other technical equipment. Goodwill makes no promises or guarantees on electronics they sell through their stores or online. Most of the distribution centers will simply gather cell phones in a larger plastic bag or cardboard box and place them on

ISSN: 2473-3857
v3 n4338

the auction site priced by the pound. Others will gather lots of up to 100 devices and display a mass picture with no detail on the makes or models represented. Normally, none of the phones have been processed to determine if they are working, or if they have been reset to factory default settings.

At the beginning of our research we were able to win one auction from a Goodwill distribution center in Mobile, AL. The auction lot was described as "8.5 Pound Cell Phone and Chargers Lot" and the final price was $22.96. When received, 43 phones were contained in a large plastic bag. Smartphones accounted for 14, feature/flip phones counted 25, non-cellular cordless home phones accounted for 4. Of the 14 smart phones, 8 were able to be powered on and investigated. Further auctions were successfully bid on from distribution centers in Buffalo, NY (5 usable); Cleveland, OH (11 usable); Missoula, MT (7 usable); and Tacoma, WA (4 usable). For this project a smartphone was defined as having an operating system of one of the following: Android, Blackberry, iOS, or Windows.

The OS makeup of the phone samples:

Android	**iOS**	**BB**	**Windows**	***Total***
15	7	9	4	35

This sample size can be considered appropriate as an initial pool in that it represents each of the major operating systems for mobile phones, and was procured through multiple locations around the United States.

Phones were examined in two passes. The first pass was performed without the aid of any forensic software. Phones were charged and powered on. The device was then examined through the primary user interface to search for identifying data. This included texting and e-mail applications, system settings, and other file system applications. Once completed, phones were then attached to a workstation through USB connections and their file systems mounted and browsed.

A secondary search was performed on the 35 devices utilizing Paraben Electronic Evidence Examiner and Device Seizure. Paraben E3:DS is a specialized software suite that is utilized in law enforcement and private practice for investigative work as well as data recovery (Paraben, 2016; Stephenson, 2016). A license was purchased for this and other ongoing projects.

For each of the 35 phones in the study, an attempt was made to create a forensic image. That image was then investigated through the Paraben Evidence Examiner interface to identify any of the 14 indicators. The Evidence Examiner interface scans the forensic image and organizes files found through applications, and file types. Files can be previewed in the application or opened outside in their native application or viewer.

In two cases, one Android and one Blackberry, the phone device was inoperable, however a microSD storage card had been left in the device by the previous owner. This storage media was then mounted to the examination station through a USB convertor. The contents were browsed first. With a second pass through the forensic examination software.

While some of the target flags are self-evident when found (presence of calendar entries, text messages, e-mail messages, etc.), other needed to be derived through content of files or messages. For example, birthday was determined on most phones through a calendar entry the previous owner had made for themselves, or in several cases, text messages from others on their birthday with well wishes.

Address was established through several methods. Some addresses were established through signature blocks on e-mail messages. Addresses were also found as content in text messages and also receipt files from purchases.

4. RESULTS

Thirty five phones were examined. Of those 35 phones, three appeared to have had a factory reset performed on them.

Three devices were protected by a screen lock passkey or pattern. Efforts to bypass these screen locks were unsuccessful.

One unique device appeared to have been compromised by a ransomware attack and no functions could be performed through the screen. However, once attached to an examination computer station, the file system of the phone could be browsed directly.

Figures 1 and 2 display tables of the amount of phones containing the various personal markers:

ISSN: 2473-3857
v3 n4338

	Android	iOS	BB	WIN	*Total*	%
Name	11	4	3	0	18	51%
Address	6	3	3	0	12	34%
Phone #	12	4	5	0	21	60%
E-mail	11	4	3	0	18	51%
2nd E-Mail address	4	2	0	0	6	17%
Birthday	3	1	1	0	5	14%
Text messages	12	4	3	0	19	54%
E-mail messages	7	3	3	0	13	37%
Pictures	9	4	3	0	16	46%
Calendar entries	11	3	3	0	17	49%
SM Account	5	3	0	0	8	23%
SM Content	2	0	0	0	2	6%
Browsing history	9	0	0	0	9	26%
Documents	8	0	3	0	11	31%

Figure 1: Results of search without Forensic Software

	Android	iOS	BB	WIN	Total	%
Name	14	6	7	0	27	77%
Address	9	5	7	0	21	60%
Phone #	14	6	9	0	29	83%
E-mail	14	6	7	0	27	77%
2nd E-Mail address	4	2	0	0	6	17%
Birthday	3	1	1	0	5	14%
Text messages	14	5	5	0	24	69%
E-mail messages	8	5	5	0	18	51%
Pictures	13	5	3	0	21	60%
Calendar entries	12	4	5	0	21	60%
SM Account	8	4	0	0	12	34%
SM Content	5	2	0	0	7	20%
Browsing history	13	4	0	0	17	49%
Documents	12	2	5	0	19	54%

Figure 2: Results of search with Forensic Software, Paraben E3:DS

5. CONCLUSIONS

When this project began, it was originally thought that it would be difficult to come across a phone that could be used as an example of personal data left behind. It was thought that we may be looking for a needle in a haystack. Within the first batch of phones that were examined, it became apparent that the phone without any personal data was the exception and not the norm.

As detailed in many stories of identity compromise, including a demonstration video produced for LexiHut, a consortium of lawyers, barristers, and accountants (LexiHut, 2016) the amount of personal data needed to carry out an attack and takeover of a target's accounts can be startlingly low. Many times it is the small details that are sprinkled into a social engineering story that give enough factual evidence to make a customer service representative believe they are speaking to a different person on the phone. Items such as birthday, e-mail addresses, social media account handles, calendar events, and other contacts can help to weave a tale that becomes very believable.

From the data shown in the results, even without specialized forensic software, the predominance of the phones examined gave up some data about the previous owner. In many cases, almost no efforts had been taken by the previous owner to either protect their phone, or to reset the device to factory default.

Further searching through forensic software did extend the results, producing more evidence. However, in the case of two of the screen locked phones it did not yield any evidence. Both of these phone were iPhones.

The four Windows Phone samples returned no results. One had been reset and was in a setup mode. The other three were clear of any data remnants.

To answer the research question: How much personal data can be found on cell phones donated to charity? In this sample of phones - a lot. Even with masses of news features and stories highlighting personal security and identity theft fears, it appears many are still not taking basic precautions when letting go of a personal device, their phone, which could contain so much data about them.

ISSN: 2473-3857
v3 n4338

6. FURTHER WORK

This study has raised some privacy concerns regarding some issues facing charitable organizations that may collect electronic devices. Our researchers have reached out to Goodwill to alert them to some of the issues they may be facing. Attempts at contact were made through phone and e-mail. However, of the five distribution centers contacted, only three replied through e-mail all pointing to a disclaimer relating that Goodwill Industries is not responsible for any data left on donated electronics and that it is the responsibility of the party making the donation to ensure any identifying data has been erased prior to donation. It is hoped to continue to try and reach this organization and others to help educate them to the issue and possibly establish protocols and simple procedures to erase electronic storage on devices.

With the majority of phones in our study displaying personal data, and showing no efforts at protection, one conclusion can be drawn that public awareness of this issue needs to be increased. The researchers of this paper have reached out through local news agencies and have been able to produce a consumer report advisory segment to advise the public on how easy it is to wipe a phone prior to donating. This segment has been syndicated through CBS and has aired in many markets around the country (Koppen, Serapiglia, 2017). It is hoped that these outreach efforts can be continued through other outlets and mediums.

Continuing research will attempt to procure more samples of phones from different areas of the country. Work is also planned to determine the effectiveness of the factory reset process for different phone models in completely erasing data from phone flash memory.

7. REFERENCES

Acuant (2016). 101 Ways Your Identity Can Be Stolen and Exploited. Retrieved on April 12, 2017 from https://www.acuantcorp.com/101-ways-your-identity-can-be-stolen-and-exploited/

Alabaster, J. (2013, April 16). "Android founder: We aimed to make a camera OS". PC World. International Data Group. Retrieved May 9, 2017 from https://www.pcworld.idg.com.au/article/459186/android_founder_we_aimed_make_camera_os/

Ayers, R., Brothers, S., & Jansen, W. (2014, May). Guidelines on Mobile Device Forensics. NIST Special Publication 800-101, Revison 1. U.S. Department of Commerce. Retrieved April 1, 2017, from http://dx.doi.org/10.6028/NIST.SP.800-101r1

CIMIP (2016). Center for Identity Management and Information Protection. Retrieved on March 16, 207 from http://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm

Cooper, M. et al., "Radio Telephone System", US Patent number 3,906,166; Filing date: 17 October 1973; Issue date: September 1975; Assignee Motorola

Cowen, D. (2013). Computer Forensics InfoSec Pro Guide. McGraw Hill, Osborne Media.

Davis, J. (1999, January 20). "Short Take: BlackBerry wireless email device debuts". CNET. Retrieved December 28, 2016 from https://www.cnet.com/news/short-take-blackberry-wireless-email-device-debuts/

Elgin, B. (2005, August 17). "Google Buys Android for Its Mobile Arsenal". Bloomberg Businessweek. Retrieved April 15, 2017 from http://tech-insider.org/mobile/research/2005/0817.html

FTCCSN (2016). Consumer Sentinel Network Data Book. Retrieved on December 28, 2016 from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

Gartner (2016). Gartner Says Chinese Smartphone Vendors Were Only Vendors in the Global Top Five to Increase Sales in the Third Quarter of 2016. Retrieved on January 21, 2017 from http://www.gartner.com/newsroom/id/3516317

Guido, M., Buttner, J., Grover, J. (2016) Rapid differential forensic imaging of mobile devices. DFRWS USA 2016 — Proceedings of the 16th annual USA digital forensics research conference. Retrieved on January

ISSN: 2473-3857
v3 n4338

21, 2017 from http://www.sciencedirect.com/science/article/pii/S1742287616300457

Hayes, D. (2015). A Practical Guide to Computer Forensics Investigations. Pearson, Indianapolis

Hegeman, R. (2013, March 25). Woman gets prison time in 'total identity theft'. US News and World Report. Retrieved April 15, 2017 from https://www.usnews.com/news/us/articles/2013/03/25/woman-gets-prison-time-in-total-identity-theft

Honan, M. (2012a, August 6). How Apple and Amazon Security Flaws Led to My Epic Hacking. Wired Magazine. Retrieved April 15, 2017 from https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Honan, M. (2012b, August 17). Mat Honan: How I Resurrected My Digital Life After an Epic Hacking. Wired magazine. Retrieved April 17, 2017 from https://www.wired.com/2012/08/mat-Honan-data-recovery/

Internet Society (2014). Your Digital Footprint Matters. Retrieved November 21, 2016 from http://www.internetsociety.org/your-digital-footprint

Ketyean, A. (2010, April 19) Copy Machines, a Security Risk? CBS Evening News, Retrieved April 17, 2017 from http://www.cbsnews.com/video/watch/?id=6412572n

Koppen, S., Serapiglia, A. (2017) Consumer Warning: Personal Data Found On Used Phones. KDKA, CBS Pittsburgh. Retrieved May 10, 2017 from http://pittsburgh.cbslocal.com/2017/02/17/consumer-warning-personal-data-found-on-used-phones/

Lewis, P. (January 12, 2007). "How Apple kept its iPhone secrets". CNN Money. Retrieved November 12, 2016 from http://archive.fortune.com/2007/01/10/commentary/lewis_fortune_iphone.fortune/index.htm

LexiHut (2016). Real Future: What Happens When You Dare Expert Hackers to Hack You Episode 8. Retrieved May 1, 2017 from https://www.youtube.com/watch?v=F78UdORll-Q

Limer, E. (2015, May 30). Why You Need to Encrypt Your Android Phone Before You Wipe It and Sell It. Popular Mechanics. Retrieved November 12, 2016 from http://www.popularmechanics.com/technology/gadgets/a15748/android-factory-reset-flaw/

Manjoo, F. (2015, May 27). "A Murky Road Ahead for Android, Despite Market Dominance". The New York Times. Retrieved March 12, 2017 from https://www.nytimes.com/2015/05/28/technology/personaltech/a-murky-road-ahead-for-android-despite-market-dominance.html

Mather, J. (2007, February 19). "iMania". Ryerson Review of Journalism. Retrieved November 10, 2016 from http://rrj.ca/imania/

McGrane, K. (2013) The Rise of the Mobile-Only User. Harvard Business Review. Retrieved April 2, 2017 from https://hbr.org/2013/05/the-rise-of-the-mobile-only-us.com

Messemer, E. (2012, October 12). Getting forensics data off of smartphones and tablets can tough, experts say. Computerworld. Retrieved November 12, 2016 from http://www.computerworld.com/article/2492331/data-center/getting-forensics-data-off-of-smartphones-and-tablets-can-be-tough--experts-say.html

Novet, J. (2016, December 27). Amazon Echo murder case amplifies the question of what 'always on' really means. Venture Beat. Venture Beat. Retrieved April 2, 2017 from https://venturebeat.com/2016/12/27/amazon-echo-murder-case-amplifies-the-question-of-what-always-on-really-means/

Osborne, N., & Connelly, L. (2015). Managing your digital footprint: possible implications for teaching and learning. Paper presented at European Conference on Social Media, Porto, Portugal. Retrieved November 2, 2016 from http://www.research.ed.ac.uk/portal/en/publications/managing-your-digital-

ISSN: 2473-3857
v3 n4338

footprint(9c4a5cc7-c74f-4e26-b282-0ace71e55562)/export.html

Pacer (2016). Types of Personal Information Identity Thieves Steal. Pacer Center. Retrieved April 2, 2017 from http://www.pacer.org/publications/possibilities/protect-your-identity/86-types-of-personal-information-identity-thieves-steal.html

Paraben Corp. (2017) Paraben Corporation, About Us. Retrieved December 30, 2016 from https://www.paraben.com/company/about-us

Pew Research Center (2017, January). Mobile Fact Sheet. Pew Internet & American Life Project. Retrieved April 2, 2017 from http://www.pewinternet.org/fact-sheet/mobile/

Sanford, G. D. (n.d.). iPhone. Apple History. Retrieved November 2, 2016 from http://apple-history.com/iphone

Segall, R. (2013). Goodwill makes changes after WTHR finds charity selling personal information. WTHR, Indianapolis. Retrieved November 2, 2016 from http://www.wthr.com/article/goodwill-makes-changes-after-wthr-finds-charity-selling-personal-information

Shields, M. (2003, April 21). "BBC interview with Martin Cooper". BBC News.

Simon, L., & Anderson, R. (2015, May 25). Security Analysis of Android Factory Resets. University of Cambridge Computer Laboratory. Retrieved November 12, 2016 from http://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf

Sitek, Z. and Thomas, D. (2016, February 23). Bentonville PD Says Man Strangled, Drowned Former Georgia Officer. KFSM5NewsOnline. Retrieved April3, 2017 from http://5newsonline.com/2016/02/23/bentonville-pd-says-man-strangled-drowned-former-georgia-officer/

Smith, M. (2017, January 2). Cops to increasingly use digital footprints from IoT devices for investigations. Network World. Retrieved March 10, 2017 from http://www.networkworld.com/article/3154064/security/cops-to-increasingly-use-digital-footprints-from-iot-devices-for-investigations.html

StatCounter (2017, May) Global Stats: Top 8 Mobile Operating Systems on Apr 2017. Retrieved May 20, 2017 from http://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201704-201704-bar

Stephenson, P. (2016). Product Information, Paraben E3:DS. SC Media. Retrieved December 30, 2016 from https://www.scmagazine.com/paraben-ds/review/7125/

Tyson, J. (2000, August 30). How Flash Memory Works. Retrieved November 2, 2016 from How Stuff Works: http://computer.howstuffworks.com/flash-memory2.htm

USDOJ (2017) What Are Identity Theft and Identity Fraud? The United States Department of Justice. Retrieved November 2, 2016 from https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Vijaykumar, M. (2015, January 8). Smartphone: Today's Primary Computing Device. Silicon Valley: Software Developers, Inc. Retrieved November 2, 2017 from http://www.softwaredevelopersinc.com/blog/2015/01/08/smartphone-todays-primary-computing-device/

WSJ (2012). What They Know. The Wall Street Journal. Retrieved November 10, 2016 from http://www.wsj.com/public/page/what-they-know-digital-privacy.html

Weise, E. (2016, August 15). A hackers best friend is a friendly employee. USA Today. Retrieved November 3, 2017 from https://www.usatoday.com/story/tech/news/2016/08/15/hacker-social-engineering-defcon-black-hat/88621412/

Ziegler, C. (2012, April 25). "This was the original 'Google Phone' presented in 2006". The Verge. Vox Media. Retrieved March 12, 2017 from https://www.theverge.com/2012/4/25/2974676/this-was-the-original-google-phone-presented-in-2006