IMPLICATIONS OF CIRCULAR ECONOMY ON USERS DATA PRIVACY: A CASE STUDY ON ANDROID SMARTPHONES SECOND-HAND MARKET

Mariia Khramova, Sergio Martinez, and Duc Nguyen

Blancco Technology Group

Abstract: Modern electronic devices, particularly smartphones, are characterised by extremely high environmental footprint and short product lifecycle. Every year manufacturers release new models with even more superior performance, which pushes the customers towards new purchases. As a result, millions of devices are being accumulated in the urban mine. To tackle these challenges the concept of circular economy has been introduced to promote repair, reuse and recycle of electronics. In this case, electronic devices that previously ended up in landfills or households are getting the second life, therefore, reducing the demand for new raw materials. Smartphone reuse is gradually gaining wider adoption partly due to the price increase of flagship models, consequently, boosting circular economy implementation. However, along with reuse of communication device, circular economy approach needs to ensure the data of the previous user have not been "reused" together with a device. This is especially important since modern smartphones are comparable with computers in terms of performance and amount of data stored. These data vary from pictures, videos, call logs to social security numbers, passport and credit card details, from personal information to corporate confidential data. To assess how well the data privacy requirements are followed on smartphones second-hand market, a sample of 100 Android smartphones has been purchased from IT Asset Disposition (ITAD) facilities responsible for data erasure and resell. Although devices should not have stored any user data by the time they leave ITAD, it has been possible to retrieve the data from 19% of the sample. Applied techniques varied from manual device inspection to sophisticated equipment and tools. These findings indicate significant barrier in implementation of circular economy and a limitation of smartphone reuse. Therefore, in order to motivate the users to donate or sell their old devices and make electronic use more sustainable, data privacy on secondhand smartphone market should be significantly improved. Presented research has been carried out in the framework of sustainablySMART project, which is part of Horizon 2020 EU Framework Programme for Research and Innovation.

Keywords: Android, circular economy, data privacy, second-hand phones

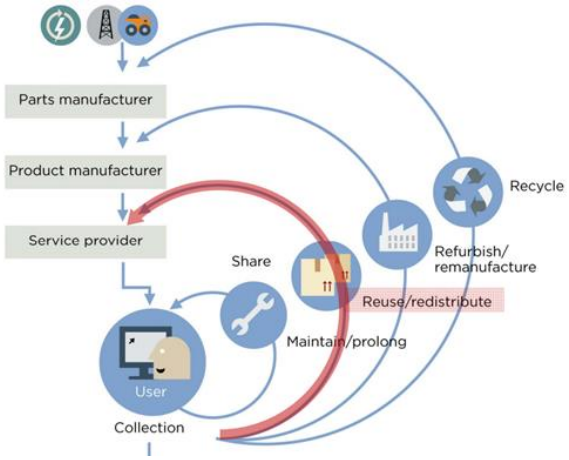
1. INTRODUCTION

Accelerated development of smartphone technologies has revolutionised the way people live and maintain communication. By 2015 smartphones have moved from the fringe of computer technology to the mainstream [1]. Significant technology and design improvements have turned bulky feature phones that supported only basic functions such as making calls and exchanging text messages into slick and slim smartphones with vast range of features. If previously, cell phones were featuring high prices and were not widely available, modern smartphones have become more affordable offering broad range of price categories. In addition to that, smartphones brought such benefits as absolute connectivity, portability and diversified functionality that allowed integration e.g. of PDA, camera, GPS, music and video players into one device. Responding to the speed of technology improvements, the rate at which consumers purchase, use and discard mobile phones has also rocketed [2][3]. Short product lifecycle combined with high environmental footprint of smartphone production have negatively affected sustainability of modern electronic devices. Mobile phones contain such rare earth metals as Tantalum,

Table 1: Main elements by functional component [5]

Material		Common Use	Content per smartphone (g)	Content in all smartphones made since 2007(t)
Aluminium	**Al**	Case	22.18	**157,478**
Copper	**Cu**	Wiring	15.12	**107,352**
Plastics	**-**	Case	9.53	**67,663**
Cobalt	**Co**	Battery	5.38	**38,198**
Tungsten	**W**	Vibration	0.44	**3,124**
Silver	**Ag**	Solder,PCB	0.31	**2,201**
Gold	**Au**	PCB	0.03	**213**
Neodymium	**Nd**	Speaker magnet	0.05	**355**
Indium	**In**	Display	0.01	**71**
Palladium	**Pd**	PCB	0.01	**71**
Gallium	**Ga**	LED-backlights	0.0004	**3**

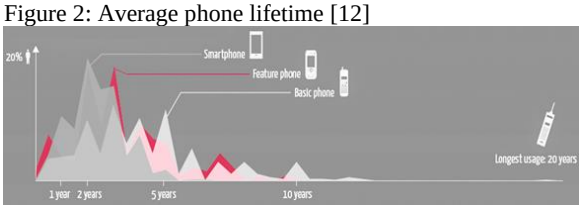
Figure 1: Circular view on electronics lifecycle [9]



Indium, Neodymium, Tungsten, Palladium, Yttrium as well as critical metals and hazardous substances [3][4].

Discarded and replaced phones, being often in a good and working condition, is an underused source of valuable resources including fully functioning products, components and materials [3]. However, low recycle and reuse rates alongside with difficulty of smartphones disposal have resulted in this potential to not being fully utilised. Green Alliance [1] has estimated that in the US 89% of mobile devices were thrown in the landfill in 2010. Implementation of circular economy approaches aims to mobilise these unused resources through reuse, repair, recycling, redesign and recovery of materials (Figure 1). Circular view also known as zero waste society is based on minimisation of used resources and reduction of the waste [7]. It challenges traditional linear economy approach, where resources are disposed once they reach the end of product lifetime [7]. Linear industrial economy is based on low production costs and abundant availability of raw materials at low cost [8]. Due to growing production costs and limited availability of raw resources, circular economy concept has recently become one of the EU's main priorities [8]. The European Commission defines a circular economy as a set of activities in which "the value of products, materials

Figure 2: Average phone lifetime [12]



and resources is maintained in the economy for as long as possible and the generation of waste minimised" [6]. Circular economy would help to close the wasteful loop and keep products, components and materials in use for longer, maximising their value throughout lifecycle and transforming them into new goods [7].

If product redesign, repair and material recovery are only taking first steps to gain wider adoption, extension of smartphone lifetime through longer product usage and further resell in second-hand market is increasingly strengthening.

Watson et al. [3] emphasise that penetration rates of smartphones in Europe and Nordic countries is unprecedentedly high while phone replacement rates are slowing down. The main reasons are high prices of flagship and middle range devices and rather incremental improvements over the models. At the same time the demand for the second-hand devices has increased. According to IDC [10], the growth of second-hand phone market is forecasted to reach 222.6 million units by 2020 while recent research from Mintel on mobile phones in the UK shows that 39% of smartphones are already enjoying their second-life [11]. Another study on the UK, US and Indian market shows that a two years old flagship smartphone can be still more attractive than today's mid to low range best sellers [1]. Most common approach for implementation of circular economy concept in smartphone market has been engagement in take-back and buy-back, which opened opportunities for refurbishment and resell businesses that are already reporting rapid growth in demand [3].

1.1. IT Asset Disposition

There is a plethora of platforms supporting the trade of used mobile phones that allow individuals to buy and sell second-hand devices. Among most popular of them are, for example, eBay, Craigslist, Bestbuy, Amazon, Gazelle, Fonebank. Moreover, it is also common that mobile operators and large electronics retailers run take-back / buy-back programs to collect and resell smartphones. Collected phones undergo several stages before they are ready to be resold. These intermediate operations, including device diagnostics and data erasure, can be either fully performed by collecting organisation or sent to the IT Asset Disposition (ITAD) facilities. The major

source of retired equipment for ITADs is, however, corporate and governmental organisations [13]. ITADs help their customers to securely dispose outdated, unviable or undesired equipment in an environmentally safe and responsible manner, therefore, representing an important element in green initiatives [13][14].

Nowadays ITADs operations do not only focus on recycling of old IT equipment, but also cover data security, environmental accountability and cost savings throughout asset lifecycle. Therefore, there are 2 fundamental ITAD functions: maximisation the value of IT asset investment over entire lifecycle and the value recovered at the end; minimisation of data security risks and compliance with environmental regulations. Consequently, ITADs remove the burden associated with business, legal and environmental risks related to IT retirement [13].

Although, the exact process steps may vary depending on the operations performed by ITAD facility, typical procedures include the following [15]-[18]:

1- De-installation (removal of IT equipment and preparing for transportation)
2- Secure collection of assets
3- Scan and registration in tracking system
4- Secure transportation of customer assets to ITAD facilities (cars are typically equipped with GPS)
5- Triage: assets without value undergo physical destruction and further recycling; asset with value are securely sanitized
6- Testing and quality check
7- Remarketing
8- Resell

Optional process steps may also include e.g. device cleaning and repair or end-of-life recycling that involves device disassembly, parts harvesting, material separation and recycling. Large number of second-hand equipment is further sold through different B2B and B2C distribution channels, including web sites, online auctions, direct retail, local and regional value-added resellers, and overseas brokers.

1.2. Data privacy in context of smartphone re-use

Significant increase of internal device storage combined with diversification of applications and features resulted in enormous amount of data stored on smartphones. In case of personal usage, the broad range of data stored on devices vary from multimedia files and call logs to documents, email history, application data, banking details, geolocation, passwords and health data. In the context of corporate use, mobile devices may also hold trade secrets and other confidential information such as financial transactions, contracts, customer information, account numbers, and insurance data [13]. Therefore, if device undergoes reuse, it is extremely important to securely remove previous owner's data from the phone. Data sanitisation allows destruction of the data stored on the device and prevents data breach incidents. Noteworthy, issues related to data security and privacy have been identified as a barrier for mobile phone and IT equipment recycling, particularly for business or commercial customers [19]. By different law and regulations corporate and governmental organisations are obliged to ensure data privacy when the IT asset is retired, which represents the challenge of complete and efficient removal of the data remaining on the device [13]. The use of ITAD service provider transfers the data security risks and help organisations comply with data privacy regulations. Considering individual users, previous studies on consumer attitudes towards recycling highlight that maintaining data privacy on resold devices represents one of the major obstacles for smartphone recycling. Welfens, M.J. et al. emphasise that fear of personal data misuse because of non-transparent recycling process heavily influences the return and recycling of mobile phones. This is one of the reasons why people prefer to keep their old devices instead of selling them or returning them for recycling upon purchasing a new device [20]. Tanskanen [21] considers transparency of recycling system as one of the ways of how to motivate recycling behaviour. Research on consumers' perceptions towards smartphone recycling done in Finland has discovered that information security issues are one of the inhibitory reasons for mobile phone re-use and recycling [22]. Therefore, data security plays an important role for both private and corporate users and is integral part in enablement of smartphone re-use.

1.3. Literature review

Data remainance on various type of media circulating on the second-hand market has been in the focus of researchers and practitioners attention for many years. Jones et al. [23]-[30] have done extensive research on hard disk drives to examine to which extend they have been securely sanitized and whether the data were still recoverable with a use of freely available tools. These studies show the trend of gradual decrease of the number of devices containing previous owner data. In the study on the UK market [29], out of 110 devices sample, only 43% of drives were wiped and didn't contain any data. 41% of devices still stored meaningful data such as corporate and personal information. Types of information recovered included full names of previous owners, email accounts, picture galleries, documents and

social media accounts. Corporate data were enough to identify the original organisation with information like names, staff details, bank statements and more. Similar research on the UAE market shows that 26 out of 40 drives contained remnant information, from which the data on 11 devices have been easily recovered and 15 devices have been improperly sanitized [30]. There are 9 devices that contained enough information to identify the original organisation, 20 drives can be used to identify individuals and 17 devices contain malware. According to the research performed by Blancco Technology Group [31], 78% of the devices purchased through eBay and Craigslist also stored previous owner's data. Device sample contained hard drives and solid state drives of different manufacturers. Out of 200 drives 11% contained corporate information and 67% contained individual data. Recovered corporate information included company emails, spreadsheets, customer data and CRM (Customer Relationship Management) records. Recovered personal information contained photos with and without GPS tags, social security numbers, financial data and resumes.

Besides hard drives, data recovery studies have also been undertaken on second-hand USB and memory cards. Out of 10 USB drives bought from eBay in the UK, 6 pieces retained sensitive information such as names, addresses, invoices and health records, 2 devices stored media files and only on 2 USB keys nothing was found [32]. Another study [33], carried on the UK and Australian market, tested 43 USB drives purchased through different channels and found data on 46% of the devices that have been formatted or in other way improperly sanitised, 44% had easily recoverable data and only 5% of the sample have been properly erased. Remaining 5% of the USB drives have been damaged or unreadable. Later study [34] examined the remnant data on various memory cards used for consumer electronic devices including mobile phones and tablets and proved that confidential data are present on 60 devices out of 78. The study indicates that in many instances there is no evidence that the data have been erased by any mean. Another research carried on the US market involved not only purchase of the second-hand thumb drives from eBay and Amazon market places, but also involved arranging a take-back study with a survey component on data deletion methods [35]. Entire sample consisted of 260 devices with over 60% of devices where the previous user data were still present. The growth of the second-hand smartphone market also initiated some interest towards examining the remnant data that they may potentially store. Research done on 135

Android and iOS smartphones [36] reveals that data were not accessible on 61% of the mobile phones due to damage or hardware failure, 20% of devices didn't contain any data that could be recovered using standard tools, 7% of the phones contained sufficient amount of personally identifiable information such as phone number, address, user name. Corporate data have been identified on 9% of the devices. Research on 20 Android phones performed by Avast shows that over 40 000 images alongside SMS and chat messages have been possible to recover from the second-hand devices [37]. In joint study of Blancco Technology Group and Kroll Ontrack [38] residual data have been found on 35% out of 20 second-hand iOS and Android mobile devices.

Existing research on data remanence raises the concern that individuals are unknowingly selling their personal privacy alongside with their devices [38]. From the data security point of view, presence of user information on resold devices imposes the risk of data privacy violation, fraud, identity theft or potential data breach. In the circular economy context particularly in case of re-sell, it represents the barrier for higher recycling rates and second-hand device collection.

2. METHODOLOGY

For this study we have chosen 100 Android mobile devices purchased directly from the ITADs. The choice in favor of Android devices is explained by the dominance of this OS across smartphones in Europe. It has been consistently proven from studies in [23]-[30] that user data and even corporate data can be found in second hand hard drives, USB devices, and smartphones sold on Amazon, eBay, Craigslist, Gazelle [35][37][38]. This proves that online auction websites and trading platforms do not provide reliable data security on second hand devices. Therefore, in this study we raise the question of whether companies offering IT disposition service properly secure previous owners' data from second hand Android smartphones.

The devices for the test sample have been chosen based on the prevalence of the phone manufacturer, device model and OS version. The target is to make the sample as representative to the actual second-hand market as possible. In addition, some devices have been purchased based on availability and affordability of the models to cover the range from older to the most recent ones. To maintain unbiasedness test devices have been purchased from 3 different sources and in 3 different periods of time (October 2016 – July 2017).

As shown in Figure 3, the year of release of the test devices ranges from 2010 to 2016. Most devices are 2-3 years old, whereas 26 devices have been released in 2014 and 26 phones in 2015, following by

Figure 3: Distribution of test devices over release years

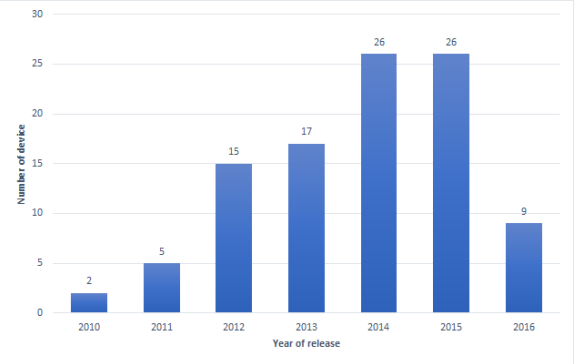


Figure 4: Distribution of test devices across vendors

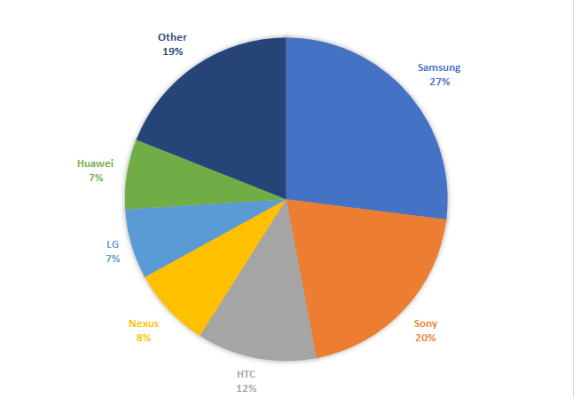
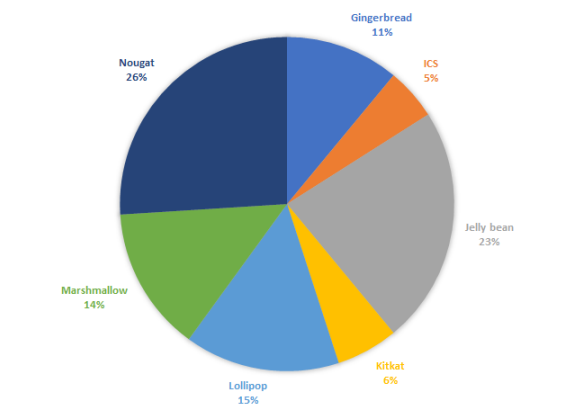


Figure 5: Distribution of test devices across OS versions



slightly smaller number of devices from 2012-2013. Smartphones of the very old and very new models have the minor share in the distribution due to their small presence in the second-hand market. Figure 4 illustrates the share of the major phone vendors in the sample. The leading vendor is Samsung represented by 27 test devices, followed by Sony and HTC having 20 and 12 devices correspondingly. Remaining phone manufacturers have significantly smaller portion in the sample. Out of 100 devices, a wide range of Android OS versions have been covered starting from Gingerbread to Nougat. The OS versions with the largest number of devices are Nougat (26%), Jellybean (23%) and Lollipop (15%).

Table 2: Classification of recovered data

Category	Data	Sensitivity
Entertainment	Music, Videos	Low
Photographic	Pictures	High
Documents	Excel, Word, PDF	Low
Messaging	SMS, MMS, WhatsApp	High
Call logs	Incoming, Outgoing	Low
Emails	Personal, Corporate	High
Internet	History, Cookies, Bookmarks	Low
Passwords	Accounts, Wi-Fi	High

More details can be found in Figure 5. Test procedure performed on device sample consists of the following steps:

1. Manual check of the device condition and content from user interface
2. Memory acquisition
3. Analysis of extracted memory
4. Analysis of results

In the first step, every test device has been checked individually to identify whether it is functional. Even though, devices undergo diagnostic checks in the ITAD facilities, few smartphones were proven to be faulty as they were not able to boot. Later, it has been discovered that these devices have faulty LCD which prevented from navigating the device manually. However, it was still possible to acquire memory image through more sophisticated techniques and analyse it. In the second step, the copy of internal device memory has been extracted. This process has been performed with the consciousness of not damaging device content integrity. Ideally, the goal was to acquire the binary image that is a bit-by-bit copy of internal memory containing everything stored on the device including deleted files. In case the retrieval of binary image was not possible, we choose other alternative options provided by the commercial mobile forensic tools. The data recovery tools also handle the analysis of extracted memory images. The main product used for testing was Oxygen Forensic Detective [39]. In addition, the demo versions of Cellebrite Physical Analyzer [40] and Axiom Magnet Forensics [41] have been utilised to maximise the amount of data identified from the extracted memory images. In case of device physical failure or device not being supported by commercial tool, low-level hardware-based memory acquisition techniques have been applied to retrieve the device memory directly from the memory chip. Further analysis of these extractions has been performed by physical image analysers or binary viewer. Combination of several data acquisition approaches and different mobile forensic tools helped to improve the quality of the obtained results and diversify the data recovered. After finishing the analysis of acquired memory, the results from all the methods and tools have been combined and investigated to draw final conclusions.

3. RESULTS

Out of 100 devices sample, it has been possible to recover data from 19% of the smartphones right after they have been received from the ITADs. As it has been mentioned, test sample was purchased in three batches, however, the test procedure was the same in all cases related to the data extraction and analysis.

Based on the obtained results, all data found on the secondhand phones have been classified into several categories according to their types. Table II specifies what category do the data belong to and determines the level of information sensitivity.

In addition, it has been considered important to further distribute recovered data into the following groups:

- Non-critical data (SMS, call logs and contacts from the carriers only)
- Critical
    - Personal data (pictures, contacts, emails, SMS, call logs, WhatsApp messages)
    - Corporate data (pictures, contacts, emails, SMS, call logs)

Among 19 devices where data were found, 10 of them have the remnant data from the mobile carrier, such as SMS, call logs and contacts. Since these data do not allow identification of the previous owner, this information has been categorized as non-critical data.

The rest of devices storing data contained individual and corporate information. The share of these devices represents 9% of the sample, i.e. 9 out of 100 phones. These data are critical as it belong to individuals or companies. Distribution of the data across categories is shown on Figure 6.

Based on the analysis of the stored content, it has been found out that the previous owner of the device is identifiable in 7 out of 8 cases. Pictures recovered from the social media profiles and device gallery helped even to determine the identity of the individual.

Similarly, the country of residence of the previous owners was identified on 9 devices. Three devices belonged to users located in Sweden, two owners were from Germany and the same number from Spain, followed by United Arab Emirates and South Africa with one device per country.

One device contained corporate information where the previous owner belonged to, including such sensitive information as the photos of product prototypes, shipments information and contacts. Email addresses are also part of the items with high sensitivity. Two devices contained both personal and corporate email addresses and one more phone where only the personal email address was found.

Figure 6: Results of data recovery tests

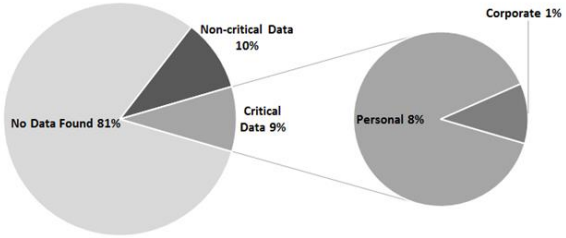


Table 3: Analysis of recovered data

Type of data	Number of devices	Ratio
Browser	3	5.66%
Call logs	5	9.43%
Contacts	9	16.98%
Documents	3	5.66%
Emails	2	3.77%
Pictures	11	20.75%
MMS	2	3.77%
Music	1	1.89%
SMS	10	18.87%
Video	2	3.77%
WhatsApp	3	5.66%
Wi-Fi Passwords	2	3.77%

The most frequently found types of information are represented in the Table III. The most popular data residing on second-hand phones included pictures (21%), followed by SMS (19%) and contacts (17%).

Interestingly, accessibility of user data across devices varied greatly. Few devices had content visible on smartphone interface, which, consequently, required no effort or special tools to access the files. Another device was not supported by any of the commercially available mobile forensic tools. However, we were able to recover the data applying low-level acquisition techniques which required connection to the phone's memory chip and reading directly from it bypassing the OS level. These devices contained so much data that it was clear that the phones didn't undergo proper data erasure process. The rest of devices had residues of user data present but inaccessible from the smartphone interface. In these cases, data have been recovered using commercial mobile forensic tools. Noteworthy, the analysis of extracted memory images indicates that sometimes user data files have been deleted, however, manual deletion or resetting the device to factory settings have proven to be unreliable [42]. It is hard to explain why the devices leaving ITAD facilities still store residues of the previous owners' information, although devices are supposed to go through data erasure process. We can assume that a potential reason could be the human factor (device has been overlooked), inefficient testing and diagnostics or unreliable data erasure solution. However, it is worth mentioning that in contrast to the research done on devices purchased through e.g.

eBay or Amazon, the number of devices acquired from the ITADs that still store user data is significantly lower than in case of online trading platforms.

4. CONCLUSIONS

Extending product lifecycle is one of the key principles of circular economy model. While phone repair, component reuse and material recovery represent much more demanding and harder approaches to implement, smartphone reuse gained wide adoption through the development of a second-hand market. Its steady growth is supported by rapid development of mobile technologies and high replacement rates. Considering enormous amount of personal and in some cases corporate data stored on modern smartphones, it is extremely important that these data or their remanences are not resold together with the device. Previous research on data remaining on the second-hand phones shows that devices resold through online trading platforms still have previous owner information present on them. In our research, we aimed to investigate if the secondhand smartphones handled by specialised IT asset disposition facilities still store the previous owner information. The results of analysis of 100 Android devices demonstrate that despite data erasure being part of second-hand phones handling procedure, 19% of phones still leave the ITAD facilities with previous owner's information or the remanence of it. Although the degree of data accessibility varied, it has been possible to recover it via different techniques and identify the former owners, their occupation and geographic location. The fact that critical information is still recoverable on 19% of the sample represents high data security risks. Taking into consideration that global used smartphone shipments have reached 140 million units [43], it means that potentially over 26 million resold smartphones still store user data. The consequences of compromised data privacy can vary from identity theft and fraud for individuals to data breach and trade secrets disclosure for corporations. Therefore, ensuring data privacy is a crucial element for smartphone reuse. It would help to build the trust towards circular economy approach and diminish the barrier for phone reuse, therefore, increasing collection rates. In addition, strong data privacy would strengthen the loyalty of already existing users.

5. ACKNOWLEDGMENT

For more information on the sustainablySMART project, its partners and publications please refer to https://portal.effra.eu/project/1544

The project sustainablySMART has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no.680640.

6. REFERENCES

[1] Green Aliance, "A circular economy for smart devices Opportunities in the US, UK and India".

[2] G.Challen, S.Haseley, A.Maiti, A.Nandugudi, G.Prasad, M.Puri and J.Wang, "The Mote is Dead. Long Live the Discarded Smartphone!".

[3] D.Watson, A.C.Gylling, N.Tojo, H.Throne-Holst, B.Bauer and L.Milios, "Circular Business Models in the Mobile Phone Industry".

[4] "Mining for smartphones: the true cost of tin.", friends of the earth.

[5] Takahashi, K.I., M. Tsuda, J. Nakamura, K. Otabe, M. Tsuruoka, Y.Matsuno and Y. Adachi (2008), "Elementary Analysis of Mobile Phones for Optimizing End-of-Life Scenarios", Journal of Environmental Science 20:1403-1408.

[6] European commission, "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS- 'Closing the loop - An EU action plan for the Circular Economy'", COM (2015) 614 final, 2 December 2015.

[7] S. Gillman, "Tech trends undermine move to zero-waste economy", Horizon 2016.

[8] I. Taranic, A. Behrens and C. Topi, "Understanding the Circular Economy in Europe, from Resource Efficiency to Sharing Platforms: The CEPS Framework", CEPS special report No. 143, July 2016.

[9] "Towards the circular economy", Ellen Macarthur foundation, 2013.

[10] IDC, "Worldwide Market for Used Smartphones Forecast to Grow to 222.6 Million Units in 2020, According to IDC, FRAMINGHAM", Mass. November 21, 2016.

[11] Mintel, "UK Mobile Phones market report", April 2017

[12] M. Guvendik, "Next step in Life Cycle Assessment: Inventory Analysis", Fairphone, June 2014

[13] S. Schiller, J. Merhout, and R. Sandlin (2016), "Enterprise IT Asset Disposition: An Overview and Tutorial", Journal of the Midwest Association for Information Systems (JMWAIS): Vol. 2016: Iss. 2, Article 3.

[14] "ITAD's Meaning and Definition Explained: What is it?", ExIT Technologies

[15] http://www.ironmountain.ca/en/Services/Data-Management/Secure-IT-Asset-Disposition.aspx

[16] http://wastetogreen.com/it-managers-guide-for-it-asset-recovery/

[17] https://www.novastar.net/novastars-asset-management

[18] http://ictcompliance.com/reverse-logistics-steps-1/

[19] J. Baxter, I. Gram-Hanssen, "Environmental message framing: Enhancing consumer recycling of mobile phones", Resources, Conservation and Recycling, Volume 109, Pages 96-101

[20] M.J. Welfens, J. Normann, A. Seibt, "Drivers and barriers to return and recycling of mobile phones, Case studies of communication and collection campaigns", Journal of Cleaner Production, 2015

[21] P. Tanskanen, "Electronics Waste: Recycling of Mobile Phones", Post-Consumer Waste Recycling and Optimal Production, 2012.

[22] J. Yl¨a-Mella, R.L. Keiski, E. Pongracz, "Electronic waste recovery in Finland: Consumers' perceptions towards recycling and re-use of mobile phones"

[23] A. Jones, "How much information do organizations throw away?", Computer Fraud & Security, 2005(3), pp.4-9. DOI: 10.1016/S1361-3723(05)70170-6

[24] A. Jones, V. Mee, C. Meyler, and J. Gooch, "Analysis of Data Recovered from Computer Disks released for sale by organisations", Journal of Information Warfare

[25] A. Jones, C. Valli, I. Sutherland, P. Thomas, "An Analysis of Information Remaining on Disks offered for sale on the second hand market.", Journal of Digital Security, Forensics & Law. Volume 1, Issue 3.

[26] A. Jones, G. Dardick, I. Sutherland, C. Valli, The 2007 "Analysis of Information Remaining on Disks offered for sale on the second hand market", Journal of Digital Security, Forensics & Law

[27] A. Jones, G. Dardick, G. Davies, I. Sutherland, C. Valli, G. Dabibi, "The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand Market", Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia

[28] A. Jones, T. Martin, M. Alzaabi, "The 2012 analysis of information remaining on computer hard disks offered for sale on the second hand market in the UAE", Proceedings of the 10th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia

[29] A. Jones, Dr. O. Angelopoulou1, Dr. S. Vidalis1, Dr. H. Janicke, "The 2016 Hard Disk Study on Information Available on the Second Hand market in the UK"

[30] T.A. Martin, A. Jones, M. Alzaabi, "The 2016 analysis of information remaining on computer hard disks offered for sale on the second hand market in the UAE"

[31] "THE LEFTOVERS: A Data Recovery Study", Blancco Technology Group

[32] A. Adam, N.L. Clarke, "Information Security Leakage: A Forensic Analysis of USB Storage Disks", Advances in Networks, Computing and Communications 6. 2007-2008

[33] A. Jones, C. Valli, G. Dabibi, "The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market", Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2009

[34] P. Szewczyk, K. Sansurooah, "The 2012 investigation into remnant data on second hand memory cards sold in Australia"

[35] S. Diesburg, C.A. Feldhaus, M. Al Fardan, N. Ploof, J. Schlicht, "Is Your Data Gone? Measuring User Perceptions of Deletion"

[36] A. Jones, C. Valli, I. Sutherland, "Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand Market", Journal of Digital Forensics, Security and Law, Vol. 3(2)

[37] "How Avast recovered 'erased' data from used Android phones", Avast 2014

[38] "Privacy for sale. A study on data security in used mobile devices & hard drives", Blancco

[39] Oxygen Forensics, https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective

[40] Cellebrite, https://www.cellebrite.com/en/home/

[41] Magnet Axiom, https://www.magnetforensics.com/magnet-axiom/

[42] L. Simon, R. Anderson, "Security Analysis of Android Factory Resets"

[43] W. Stofega, A. Scarsella, "Just Like New: Understanding the Secondary Smartphone Market", IDC Web Conference, 2017