blancco

CERTIFIED DATA ERASURE

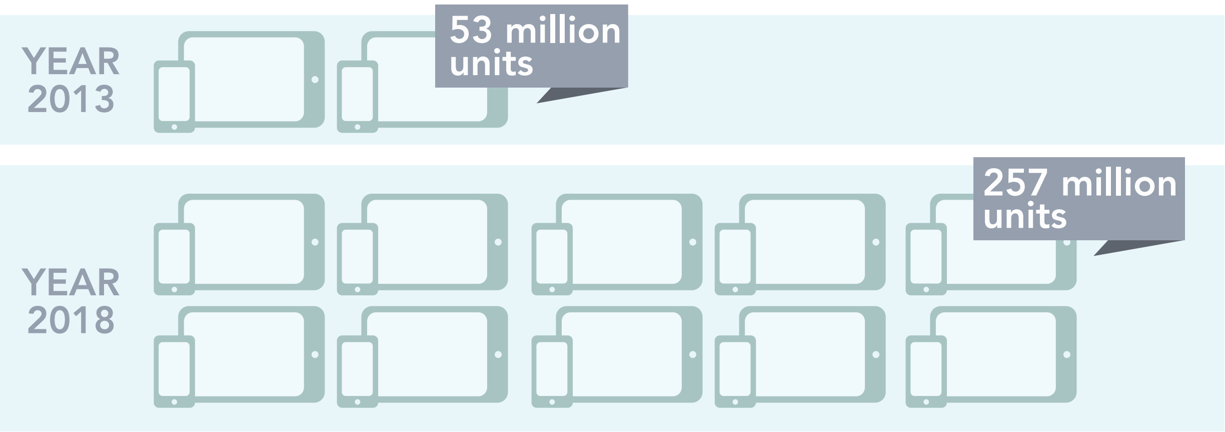
Mobile Network Operators and the Used Mobile Device Market:

SAFELY CAPTURING VALUE WITH ADVANCED DATA ERASURE

Blancco White Paper
Published 21 February 2014

Table of contents

THE GROWTH OF THE SECONDHAND MOBILE MARKET



Introduction

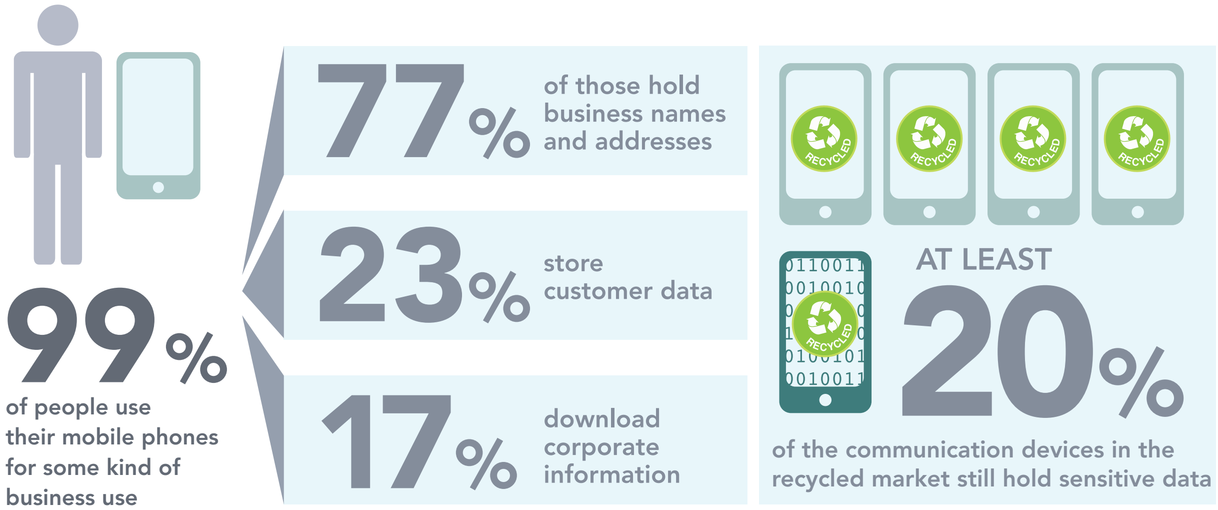
Value added-services are not the only way for mobile network operators (MNOs) to incrementally increase their average revenue per user (ARPU). With the predicted growth in sales of secondhand smartphones and tablets, there is considerable revenue potential through recouping value from previously owned mobile devices.

The used smartphone market, for example, is on the verge of significant growth, fueled in part by new trade-in and buyback programs. Analysts estimate that the market will grow from 53 million to 257 million units over the next five years. By 2018, used phones will cannibalize eight percent of total new smartphone sales, according to predictions, up from three percent in 2012.[1]

As the smartphone market rapidly expands, a new mobile ecosystem is evolving to support it. While MNOs and retailers may offer the trade-in and buyback programs, other downstream partners are engaged to make sure the phones are ready for resale. Service providers may purchase the used phones from various MNOs, then sell them to information technology asset disposal (ITAD) specialists or cell phone recyclers for refurbishment, after which they are sold through various outlets.

Along this reverse logistics chain is a great opportunity for players in the mobile ecosystem to capture residual value from used mobile devices like smartphones and tablets. However, the downside is that there is an equal opportunity to compromise the growing amount of personal and business data on these devices if they are not completely erased. Without fully erasing mobile device data or employing a partner who performs this process, mobile network operators risk as much damage to brand reputation as if a laptop with customer data was stolen or a network was compromised.

In addition to the potential for brand damage, there are a number of other factors driving mobile device erasure, including a growing number of standards and regulations that impact business data. MNOs, service providers and ITADs need to understand and respond to these drivers with effective, efficient and full erasure of all areas of the device as opposed to simple factory resets alone. Certified, advanced data erasure software provides the technology and reporting capabilities to safely remove all data and provides proof it has occurred, while securely supporting increased revenue throughout the mobile ecosystem.


99% of people use their mobile phones for some kind of business use

77% of those hold business names and addresses

23% store customer data

17% download corporate information

AT LEAST 20% of the communication devices in the recycled market still hold sensitive data

Drivers for fully erasing mobile devices

An estimated 2.2 billion smartphones and tablets will be shipped in 2014, according to Gartner.[2] Fueling this growth is the high residual value of smartphones, which has incentivized MNOs to change user plans and pricing so that upgrades are allowed at 12 and even six months, creating faster cell phone replacement cycles.[1]

With faster technology refreshes and consumers taking advantage of trade-in opportunities, mobile device lifecycles will extend and the secondhand market will experience an influx of smartphones – and data, especially as ARPU shifts from voice to data dominated. These small yet powerful devices are vulnerable, so mobile network operators need to recognize the need for full data erasure, either by themselves or their service provider and ITAD partners in the mobile ecosystem.

Your customer's data; your brand reputation

Data breaches continue to be a fact of life in the business world, causing a plethora of headaches for corporate brand teams. Many of these breaches are in the retail sector, as occurred with the Target store chain,[3] but MNOs are no strangers to the repercussions for brand reputation from cybercrime.[4] Studies show the total costs of a data breach between $184 million and $330 million,[5] and from 15%-30% of customers indicate they would terminate services upon receiving notification their data was breached.[6,7] Along with significant financial impacts, legal experts say reputational damage is the longer term injury from data breaches.[8]

While mobile network operators may be more attuned to the damages from hacking and malware, many underestimate the impacts from improperly decommissioned equipment like tablets and smartphones. Documented cases of smartphones with residual data reaching the secondhand market have occurred, with negative publicity for the MNO.[9] And, given that Gartner predicts that 90% of businesses will support corporate applications on personal devices in 2014, such breaches have an increasing potential for wide ranging impacts on both individuals and businesses.[10]

Resets leave residual data

MNOs and their service providers often assume that resetting a smartphone back to a factory default setting, or using a device's Erase Storage feature, will destroy data in its internal memory, but in many cases the data actually still exists. Furthermore, assuming that it requires a forensic expert to access data on reset phones is incorrect. In the case of Android phones, which comprise over 79% of the global market,[11] a quick visit to YouTube will reveal precise instructions for recovering data from reset devices by simply accessing them as a disk drive from a PC.

Individuals who reset a phone before resale often assume a false sense of security. In a UK study, 81% of respondents claimed to have wiped their mobile phones prior to selling them, with six in 10 confident the information was removed.[12] Most of those claiming to wipe their phones had done so manually with resets, leaving data retrievable. Identity theft experts have even cautioned against selling cell phones with storage capabilities, due to the residual data they have discovered when purchasing used cell phones that had reportedly been reset.[13]

Small devices, big risks

With more computing power than the Apollo 11 when it placed man on the moon, mobile devices hold a wealth of information despite their small size, with some smartphones and tablets having internal memory capacity up to 64 GB. This data capacity is further compounded by a mobile device's access to even larger amounts of sensitive data from cloud-based applications like Facebook, Outlook and even company applications such as Salesforce and Yammer. As these memory rich devices become smarter and more popular, helping people become more productive in both work and personal tasks, they are more likely to contain emails, customer data, passwords and other sensitive information that could lead to data breaches if disposed of without first fully erasing the information.

For example, a 2009 survey showed that 99% of people use their phones for some type of business use. Seventy-seven percent of those in the survey used their phones to hold business names and addresses, 23% stored customer data, and 17% downloaded corporate information like documents and spreadsheets.[14]

As the pace of technology refreshes for mobile devices escalates, so does the opportunity for data breaches. Research shows that personal and business data from smartphones and tablets does make its way to the secondhand market. A 2008 survey found that one in five mobile communications devices in the recycled market still held sensitive information,[15] while other informal surveys have seen numbers as high as 60% to 99%.[16,17] Many devices end up in developing countries around the world, contributing to both data security and environmental concerns.[18]

> *While mobile network operators may be more attuned to the damages from hacking and malware, many underestimate the impacts from improperly decommissioned equipment like tablets and smartphones.*

Legislation poses ongoing challenge

Legislation and standards related to data breaches, including requirements for erasing digital equipment, continue to grow around the world, with impacts for MNO customers. While it varies by region, the evolving trend is for more restrictive measures and penalties. A bring your own device (BYOD) breach could result in industry specific regulatory fines like those for revealing credit card and other personal customer data under the Payment Card Industry Data Security Standard (PCI DSS) or protected personal health information (PHI) under HIPAA in the United States.

In Europe, changes in data protection legislation have been proposed that revisit rules from the European Union (EU) Data Protection Directive of 1995. EU member states are reviewing a draft of updates, which contain requirements for deleting online data and using auditable procedures for companies processing personal data, as well as encouragement to use certified tools and processes. Sanctions for violations of these new requirements are predicted to range from 250,000 euros up to 0.5% of global annual turnover for lesser offenses and 1 million euros up to 2% of turnover for more serious ones.

MNOs must consider that the negative repercussions from a major breach through an improperly decommissioned mobile device may also extend to them.

Also, the European Network and Information Security Agency (ENISA) has specifically recognized that improper decommissioning of smartphones without a full data wipe poses one of the highest risks to information safety, yet those devices are not subject to many of the erasure processes now in place for used hard drives.[19] This is especially troubling given that an estimated 170 million mobile phones per year are recycled globally.[20]

While the US does not have a comprehensive privacy and data protection law, 46 states have enacted legislation requiring notification of security breaches involving personal information. Each law varies slightly, and many of them impose civil and criminal sanctions for failure to comply. In 2013, at least 23 states introduced—and eight states enacted—security breach legislation.[21] Those enacting legislation amended existing security breach laws, for example, to expand definitions for personal information, set additional requirements for breach notification or change penalties for those responsible for breaches. On the federal level, the Obama Administration introduced the Consumer Privacy Bill of Rights in February 2012, which provides a model for enabling innovation in new information technologies while offering strong privacy protection, including a requirement for deletion of data.

Businesses lack strong mobile device policy

The repercussions of a data breach from a tablet or smartphone are just as severe as if it originated from a server or laptop. This is especially true if the mobile device is used for business purposes and carries the potential to compromise the data of thousands or more customers as opposed to one individual. While a business itself may hold the ultimate responsibility for data that is accessed by a mobile device from a security and regulatory standpoint, MNOs must consider that the negative repercussions from a major breach through an improperly decommissioned mobile device may also extend to them.

One reason that a major data breach is possible from a smartphone or tablet is that most businesses lack a fully developed mobile device policy, with one study showing that only 14 percent of companies have such.[22] While 65 percent of survey respondents in the study said the BYOD environment is a growing security threat, almost 64 percent said they have no plans to impose any restrictive policies on mobile devices, apparently due to budget constraints in many cases. Also, mobile device management (MDM) systems for remote "erasure" may not be the quick security fix these businesses assume, as they only perform a factory reset instead of full erasure.

Meeting security and regulatory requirements are especially challenging for small businesses, where overall budgets and IT resources are limited. Many small businesses, for example, modify smartphones to become credit card terminals, with security implications. Also, one study showed that 80% of US doctors now use smartphones and medical applications in their daily practice,[23] while another highlighted how small physician practices comprise a disproportionate amount of data breaches, likely due to lack of awareness and resources. [24]

Identifying effective data erasure technology

Given the serious potential for data breaches of personal and business data, MNOs have a unique opportunity to both protect their brand and assure consumers and businesses that they use technology to fully secure data as part of a trade-in or buyback program. To do so, they, or their service and ITAD partners, must be backed by a failsafe method for removing all information from the internal and external memory of mobile devices before they are reused, recycled, stored or destroyed. This goes beyond simply destroying the SIM card to include erasure of internal memory and external memory cards, which are not as easily accessible. Also, physically destroying a mobile device leaves open the possibility of data recovery from fragmented digital media, while presenting an environmental predicament.

One method of removing data is with software that completely overwrites the device's memory. Some phone manufacturer applications use this technique, but these applications do not provide a critical element – a verifiable report with electronic serial numbers and other hardware details that prove the data is gone, which is necessary for eliminating the risk of human error, regulatory compliance and a risk-free resale or reuse of the device. In addition, these applications only work with the particular device's operating system and are manually executed.

Advanced technology answers security challenges

Approved, advanced data erasure is a type of overwriting software with many security and technical benefits. Not only can it remove all the data from a mobile device, it provides a detailed report as proof to assure consumers, businesses and MNOs the phone has been decommissioned properly. Because of its advanced functionality, data erasure offers numerous advantages:

Detailed reporting — For the mobile ecosystem, comprehensive erasure reports provide critical information for auditing, resale and security purposes, including condition of the hardware, relevant serial numbers and asset tags, software details for license harvesting, and how and by whom the erasure was done. Serial numbers can then be compared against databases to identify stolen phones.

This tamperproof and verifiable reporting is also an essential part of compliance, regulatory and legal auditing requirements; without it, mobile network operators cannot prove to individuals and businesses that their data is completely secure.

> *An automatic erasure process can be set up in just a few minutes and is highly efficient, allowing a single operator to erase hundreds of smartphones per day.*

Adherence to legislation and standards — Advanced data erasure technology adheres to the most stringent of data overwriting standards like HMG Infosec and DoD 5220.22-M, which are required for data removal by many governments and some industries. Advanced data erasure from vendors like Blancco is certified to a variety of other international standards throughout the world.

As of yet, however, there are no mutually common erasure standards specifically defined for all smartphones and tablets. The National Institute of Standards and Technology (NIST) is in the process of updating its guidelines for erasing both mobile devices and solid state disks (SSDs), while the Device Renewal Forum (DRF) looks to establish a single certification process for testing and certifying renewed smartphones, feature phones, USB modems and other wireless devices to ensure they meet rigorous product quality and performance standards. Advanced data erasure vendors like Blancco collaborate with DRF members to contribute to guidelines for a secure data sanitization process that ensures privacy and data removal from renewed mobile devices.

Third-party approvals — MNOs and mobile device recyclers should look for an advanced data erasure tool that is approved as effective in sanitizing data by an internationally recognized testing agency like TÜV SÜD. Such an approval provides the MNO, or third-party ITAD and recycling specialists who support it, with an extra level of assurance that all data has been wiped from mobile devices.

Productivity benefits for the mobile ecosystem

While full erasure of smartphones and tablet takes longer than a simple factory reset, the full security and reporting features outweigh this factor in terms of overall security and brand protection in the long run. MNOs and their partners, however, may not be aware of how advanced data erasure's automation and platform support expedite the erasure process.

Automated erasure process — With advanced data erasure, operators at refurbishing and recycling centers in the mobile ecosystem can automate and execute the same erasure process for multiple mobile devices from a normal desktop or laptop. This automatic erasure process can be set up in just a few minutes and is highly efficient, allowing a single operator to erase hundreds of smartphones per day.

The erasure software also automatically sends the erasure reports to a central console, supporting a more productive IT staff and operations for businesses and recyclers, as well as easy sharing of reports with MNOs.

Broad platform support — In addition to its efficiency, advanced data erasure software can detect and simultaneously erase data from different types of mobile device and tablet platforms because it communicates directly with their operating systems. These devices range from iOS to Nokia Symbian, Android, Windows, and BlackBerry. This platform flexibility is increasingly important as varying types of personal devices make their way onto the market, requiring different erasure processes.

Advanced data erasure benefits entire mobile ecosystem

The benefits of using advanced data erasure to fully remove all information from smartphones and tablets start with the customer and extend throughout the mobile ecosystem's entire reverse logistics chain. Brand status, security, customer loyalty and operational efficiency are some of these advantages.

Protect brand reputation

Given the enormous costs associated with inadvertently leaking a customer's data,[5] advanced data erasure is a minor investment in brand reputation with major security benefits. Mobile network operators can easily employ this technology by choosing mobile ecosystem partners who use it, avoiding the false sense of security provided by factory resets while receiving detailed auditable reports as proof.

With secure data erasure, MNOs and recyclers can also safely enhance their brand status by donating smartphones and tablets to a variety of charities.[12] The same holds true in providing a secure, green alternative to disposing of the used devices.

Attract and keep customers

Avoiding the negative publicity of a data breach is one factor in attracting and keeping customers, but mobile network operators who use advanced data erasure software can also offer positive, value-added differentiators for their service and buyback programs outside of monetary or trade-in compensation. In addition to the opportunity for educating the marketplace about the importance of the data erasure services they provide, MNOs can obtain a copy of the erasure report from their recycling partner and provide it to the customer – a service that may be especially important for business and BYOD customers.

Secure personal and business data

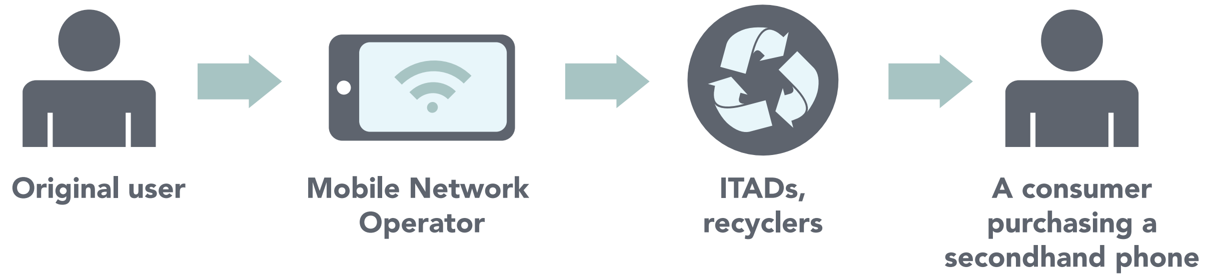
Improperly decommissioned smartphones and tablets can deliver an individual's entire digital footprint into the wrong hands, not to mention thousands of sensitive customer records if it is a BYOD device. By employing advanced data erasure software, the MNO secures personal photos, contacts and emails, as well as information from business applications, for its customers.

Advanced data erasure adheres to the strictest of technology and overwriting standards, including the creation of detailed erasure reports. By fully erasing business data and providing reports as proof, an MNO shows its commitment to helping businesses, especially small ones, develop better mobile device security policies and adhere to standards and regulations.

Capture value throughout the reverse logistics chain

Mobile network operators are not the only players in the mobile ecosystem's reverse logistics chain who stand to benefit from the use of advanced data erasure by increasing their ARPU. Service providers, ITADs and specialized mobile phone recyclers also have the opportunity for extra revenue. This may be achieved both from offering value-added services in the form of full data erasure services to MNOs and the potential for processing higher mobile device volumes as consumers and businesses become more comfortable with safe trade-ins of smartphones and tablets. MNOs themselves may also choose to offer customers full data erasure as a value-added service. And, because it is an automated, simultaneous process, advanced data erasure can be offered without impacting costs and operational efficiencies.

RECOUPING VALUE FROM PREVIOUSLYOWNED MOBILE DEVICES



Summary

The impending growth in the secondhand mobile device market, driven by consumer-friendly plans with faster technology upgrades, is not without risk. However, by conforming to stringent technology standards and third-party certifications or approvals, advanced data erasure software provides peace of mind that no data is left behind prior to resale of mobile devices. With this assurance, everyone from the original user and MNO to the ITAD recycler and individual who purchases the secondhand device can safely capture value, with no security repercussions along the way.

In addition, because advanced data erasure automatically provides a detailed erasure report, supports multiple device platforms, and can erase a number of devices at one time, it is a practical choice for MNOs, ITADs and recyclers that want to secure data without a time consuming manual process.

References

[1] Forbes.com, "Used Smartphone Market 'Poised to Explode,' Apple iPhone Holding up Better than Samsung Galaxy," 7 August 2013, www.forbes.com/sites/connieguglielmo/2013/08/07/used-smartphone-market-poised-to-explode-apple-iphone-holding-up-better-than-samsung-galaxy/

[2] Gartner.com, "Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 4.5 Percent in 2013 as Lower-Priced Devices Drive Growth," 21 October 2013, www.gartner.com/newsroom/id/2610015.

[3] NBC News, "Target estimates breach affected up to 110 million," 10 January 2014, www.nbcnews.com/business/target-says-stolen-info-data-breach-hit-70-million-people-2D11894083

[4] Infosecurity-magazine.com, "Massive Data Breach Hits Millions of Vodafone Germany Customers," 12 September 2013, www.infosecurity-magazine.com/view/34504/massive-data-breach-hits-millions-of-vodafone-germany-customers/

[5] Ponemon Institute—Experion Study 2011, www.prnewswire.com/news-releases/new-survey-by-the-ponemon-institute-finds-that-data-breaches-can-cause-lasting-and-costly-damage-to-the-reputation-of-affected-organizations-132682688.html

[6] Ponemon Institute—Experian, 2012 Consumer Study on Data Breach Notification, www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf

[7] Javelin Strategy & Research—DEBIX, Consumer Survey on Data Breach Notification, June 2008, mortstern.net/PDFSArticles/consumersurvey.pdf

[8] Law Technology News, "Reputational Damage Is the Lingering Data Breach Injury," 21 November, 2013, www.lawtechnologynews.com/id=1202629029759/Reputational-Damage-Is-the-Lingering-Data-Breach-Injury#ixzz2r9pBZLYG

[9] The Guardian, "Vodafone rings up complaints selling my old iPhone and data as new," 23 November 2013, www.theguardian.com/money/2013/nov/24/consumer-rights-money-internetphonesbroadband?CMP=twt_gu

[10] Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," 2010, www.gartner.com/it/page.jsp?id=1480514

[11] thenextweb.com, "Canalys: Android on 79% of the 998 million smartphones shipped in 2013, Windows Phone fastest growing platform," 30 January 2014, http://thenextweb.com/insider/2014/01/30/canalys-android-80-998-million-smartphones-shipped-2013-windows-phone-fastest-growing-platform/#!uosKX

[12] CPPGroup plc, "Second Hand Mobiles Contain Personal Data," 22 March 2011, www.prnewswire.com/news-releases/second-hand-mobiles-contain-personal-data-118434314.html

[13] NBC News, "Why you should never sell your old cell phone," 8 May 2012, www.nbcnews.com/business/why-you-should-never-sell-your-old-cell-phone-759723

[14] Government Technology, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," 19 March 2009, www.govtech.com/security/42-Million-Cell-Phone.html

[15] Businessweek, "The Recycled Cell-Phone Trap," 3 November 2008, www.businessweek.com/technology/content/nov2008/tc2008113_981236.htm

[16] PC World, "Your Old Smartphone's Data Can Come Back to Haunt You," 10 July 2011, www.pcworld.com/article/235276/your_old_smartphones_data_can_come_back_to_haunt_you.html

[17] Dark Reading, "Old Smartphones Leave Tons Of Data For Digital Dumpster Divers," 15 December 2011, www.darkreading.com/mobile-security/167901113/security/news/232300628/old-smartphones-leave-tons-of-data-for-digital-dumpster-divers.html

[18] New York Times, "Where do old cellphones go to die?", 4 May 2013, www.nytimes.com/2013/05/05/opinion/sunday/where-do-old-cellphones-go-to-die.html?_r=0

[19] ENISA, www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/ top-ten-smartphone-risks?searchterm=Top+Ten+Smartphone+

[20] CNET, "Your smartphone's secret afterlife (Smartphones Unlocked)," 19 August 2013, www.cnet.com/8301-17918_1-57556225-85/your-smartphones-secret-afterlife-smartphones-unlocked/

[21] National Conference of State Legislatures, 14 November 2013, www.ncsl.org/research/telecommunications-and-information-technology/2013-security-breach-legislation635200257.aspx

[22] Kasperky Lab-B2B International, "Global Corporate IT Security Risks: 2013," May 2013, media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

[23] Healthcare Technology Online, "Bracing For Healthcare's Mobile Explosion," 6 January 2012, www.healthcaretechnologyonline.com/article.mvc/Bracing-For-Healthcares-Mobile-Explosion-0001?sectionCode=Welcome&templateCode=EnhancedStandard&user=2431702&source=nl:32854\

[24] Health Information Trust Alliance, "HITRUST's Analysis of U.S. Breach Data Finds Little Progress and Concern for Un-reported Breaches," 5 December 2012, www.hitrustalliance.net/news/index.php?a=119

Kroll Ontrack®

For more information, call or visit us online.
0800 5765 565, info@krollontrack.nl
www.ontrackdatarecovery.nl