Privacy For Sale

A study on data security in used mobile devices & hard drives

blancco technology group

Kroll Ontrack

Introduction

The fascination with buying new electronics is part of our global DNA, and consumers tend to replace their technology frequently. As a recent global study from Blancco Technology Group found, 35 per cent of consumers in the U.S., Canada, U.K. and Australia recycle, sell, donate or trade in their mobile devices every two to three years and another 17 per cent do so even more frequently – either every year or when a new device model is launched.

But tightened personal budgets and steeper device prices can put a damper on the desire to purchase a new smartphone or tablet. According to data from ABI Research and The Wall Street Journal, the average price of a new iPhone jumped to $687 USD in the fourth quarter of 2014, and the average price of a new Android device is $254 USD. While hard drives may not be considered the sexiest electronics purchase, they are still a key component of computer architecture and an often necessary expense. In fact, it is common for users to purchase a new one every few years – either to replace an old hard drive or to use for additional storage.

The desire for new electronics and their high price tags play a considerable role in driving consumers to sell and buy used electronics, particularly computers and mobile devices. For buyers of second-hand electronics, the motivation is often related to cost savings. They can save a few hundred dollars (if not more) and still come out with a highly usable and functional piece of equipment. Meanwhile, sellers can recoup part or close to all of the cost of the new piece of equipment they intend to purchase.

Study at a glance

- 122 second-hand mobile devices and drives purchased from US, Germany and the UK
- 16% Mobile Devices
- 73% Hard Disk Drives
- 11% Solid State Drives
- 46% of mobile devices and drives combined contained data

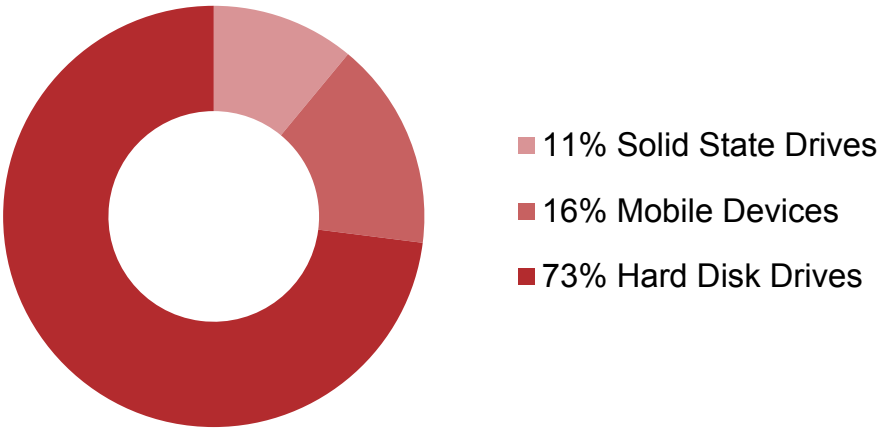
To sell or buy used electronics, buyers and sellers often head to online marketplaces like eBay, Amazon and Gazelle.com. Considered one of the largest online retailers, Amazon has nearly 244 million active members and continues to attract shoppers by offering new and improved features, speedy delivery options and on-going enhancements to the overall customer experience. With over 149 million active buyers around the world, eBay has become synonymous with making it easy, fast and convenient for consumers to sell their products on the ecommerce site. Then there is the newer ecommerce site, Gazelle.com, which began allowing consumers to sell their used phones directly to them in 2008. By March of 2014, they had accepted their two millionth trade-in device.

What precautions are sellers taking with their personal data when they post their device to one of these ecommerce sites? Do sellers use a type of deletion process to protect that data? How likely is it for the new owner to find residual data on the device? How can consumers better equip themselves to protect their privacy?

Data Recovery Analysis & Methodology

As a joint endeavour, Blancco Technology Group and Kroll Ontrack designed a data security study to highlight the security implications of data found on used IT equipment. Between May 2015 and August 2015, our teams purchased a combined total of 122 second-hand hard disk drives, solid state drives and mobile devices sold in the U.S., Germany and the U.K. from the following online marketplaces: Amazon, eBay and Gazelle.com. All second-hand equipment was randomly selected and purchased based on availability.

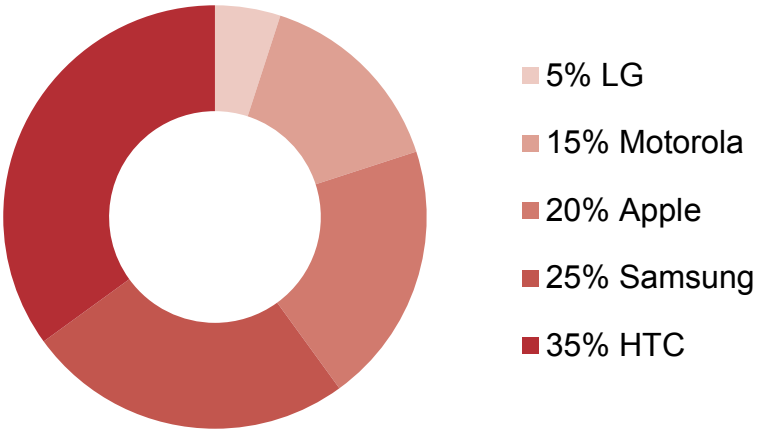
Which types of electronics were purchased and analysed in this study?



Analysis and results were organised into two categories: (1) mobile devices and (2) hard disk drives (HDD)/Solid State Drives (SSD). For the random sample of mobile devices, 20 used mobile devices were purchased from five different manufacturers, with devices running on both iOS and Android operating systems. We then compiled the total amount of data retrieved, the varying types of data recovered (i.e. emails, text/SMS messages, photos, videos, instant messages, owner identified, call logs), as well as the breakdown of data recovered by operating system.

For the random sample of HDDs and SSDs, we purchased a total of 102 used drives and extracted the amount of data recovered, the varying types of data found, as well as the wiping method performed by the original owners.

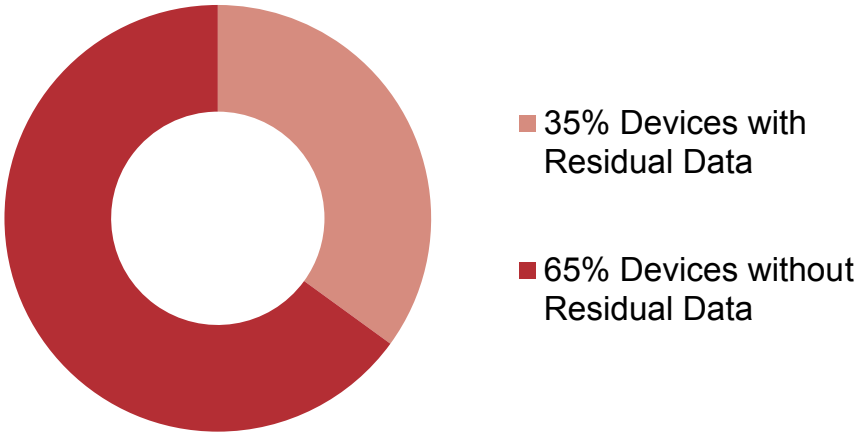
Which manufacturers were included in the sample of used mobile devices analysed for this study?



Mobile Devices: Results & Discussion

In examining the 20 second-hand mobile devices (20 per cent iOS devices and 80 per cent Android), our team found residual data of varying types and amounts on 35 per cent of the total devices purchased. Interestingly, no residual data was found on the iOS devices analysed in this study. Residual data was found on some of the Android devices, raising the concern that individuals are unknowingly selling their personal privacy when they sell their device.

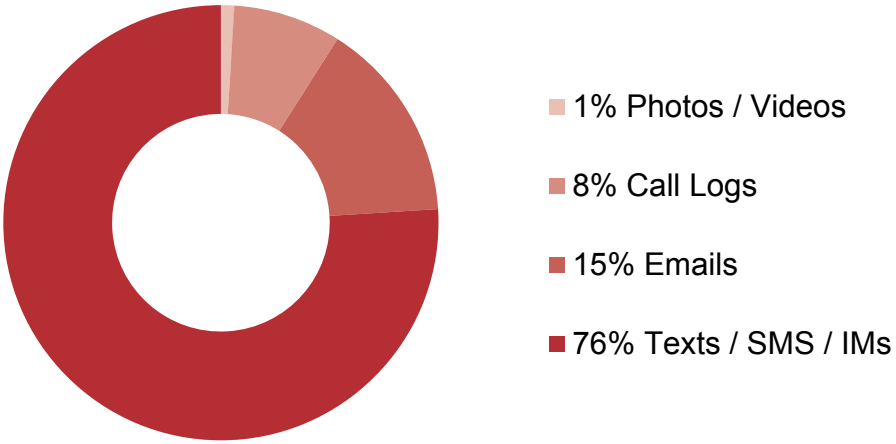
What percentage of used mobile devices contained residual data?



Leftover emails, text messages and instant messages can cause personal, financial and reputational damage to users and their employers.

Deeper analysis into the types of residual data lingering in used mobile devices revealed some interesting findings. When you consider the quantity of data types left behind, sellers may be underestimating the data privacy and security concerns associated with their emails, text messages and instant messages.

Which types of data were recovered from second-hand mobile devices?



A total of 2,153 emails and 10,838 text/SMS/instant messages were retrieved from the devices analysed, which is cause for concern to mobile users and businesses. Mobile device owners use their device for anything and everything – banking, scheduling appointments, ordering food, shopping, taking photos/videos and even work-related activities. According to a recent study by Tech Pro Research, 74 per cent of organisations already use or plan to implement a bring your own device (BYOD) policy in order to provide best practice guidance around the use of personal devices for work purposes. As more companies will welcome BYOD into their workplaces, it is important for organisations to understand that personal devices can open the door to security risks, especially when employees leave the business. As a result, proprietary company information could be divulged, new product information could unknowingly be communicated and confidential revenue and stock price information could fall into the wrong hands.

Old photos and videos can come back to haunt smartphone sellers.

When we looked at the different types and quantities of residual data found on the mobile devices, 1 per cent of the total residual data was in the form of photos and videos. This may stem from the erroneous assumption that deleting a file means the file is gone. In truth, hitting the 'delete' button on photos and videos saved on mobile devices does not guarantee that photos and videos are securely removed from the device.

The information potentially gleaned from remaining photos and videos can be dangerous, especially if it falls into the wrong hands. Photos may contain very specific geolocation data about where they were taken. This means that not only the photos themselves but also the location data could be shared publicly, raising concern that a user's location and actions are no longer private. Additionally, a skilled cyber criminal could use a tool like Photoshop to copy the faces of sellers onto other images or sites that are explicit or inappropriate in nature.

As Paul Henry, IT Security Consultant for Blancco Technology Group, explains: "Even if the smallest amount of data falls into the wrong hands, it can be harmful to an individual. With the Ashley Madison hack, in particular, users who wanted to make sure all of their data was erased from the dating site put all of their trust into the site's $20 'full delete' program. While those customers who paid for the 'full delete' service had their real name, username, email and profile information removed, other data was still left intact – including date of birth, gender, weight, height and zip code. Even though the obvious identifiers had been removed, enough information was left to expose an individual. The big lesson for Ashley Madison – and any other type of business – should be to test that your deletion methods are complete and to not blindly trust that simply 'deleting' data will truly get rid of all of it for good. Remaining data can still be accessed and recovered."

Data is difficult to delete and can easily resurface after mobile devices are resold.

While over one-third (35 per cent) of the second-hand mobile devices purchased contained data that was still intact, it is even more disturbing that 57 per cent of the devices with residual data had a deletion attempt made on them. In fact, two of those devices still contained 179 texts, 252 instant messages, over 75 photos and two SMS messages. From that data, the identity of the original phone owners were discerned!

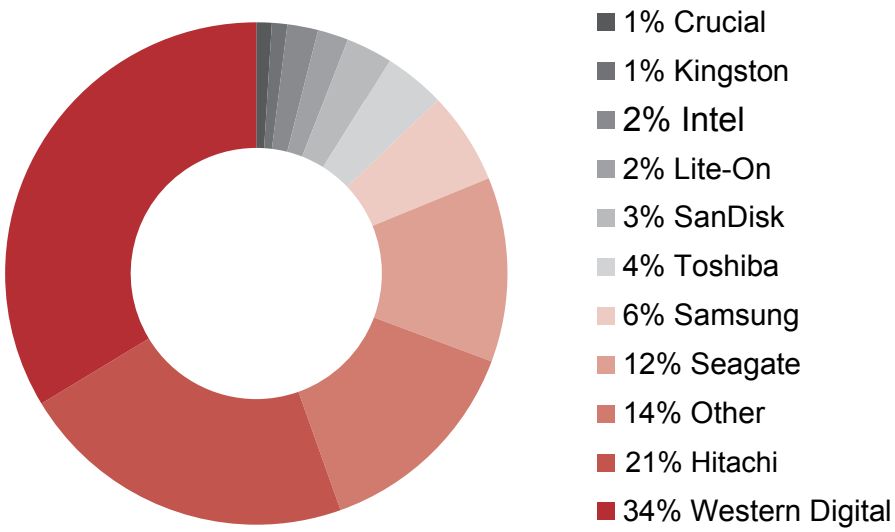
The takeaway is that not all mobile data erasure methods are effective at completely erasing data. Some of the methods commonly used still leave a significant amount of data. Additionally, failure to completely and properly wipe electronics could leave behind data as well. In the case of Android devices, ineffective deletion may occur because users assumed the factory reset would suffice in completely removing their data. The bottom line is information often considered 'deleted' (including external SD or SIM cards) by the examples noted in this study still leave a considerable amount of data intact.

In reality, manually deleting data or simply logging out of an app will not erase the data from the phone. Deleting data only removes the ability for the mobile device to find the data again. The data still remains and can be recovered. In order to make the data unrecoverable, it needs to be overwritten. Factory reset – a heavily relied upon deletion method – has been proven effective in some cases but not in others. Each device's operating system is different and the same wiping method that works on iOS devices does not work on Android devices. These methods are not only specific to the operating system, but they are also unique to the device manufacturer and can vary by device model produced by the same manufacturer. If the factory reset applied is not completely effective, it is extremely easy to perform a simple Google search to find software that can quickly recover that data.

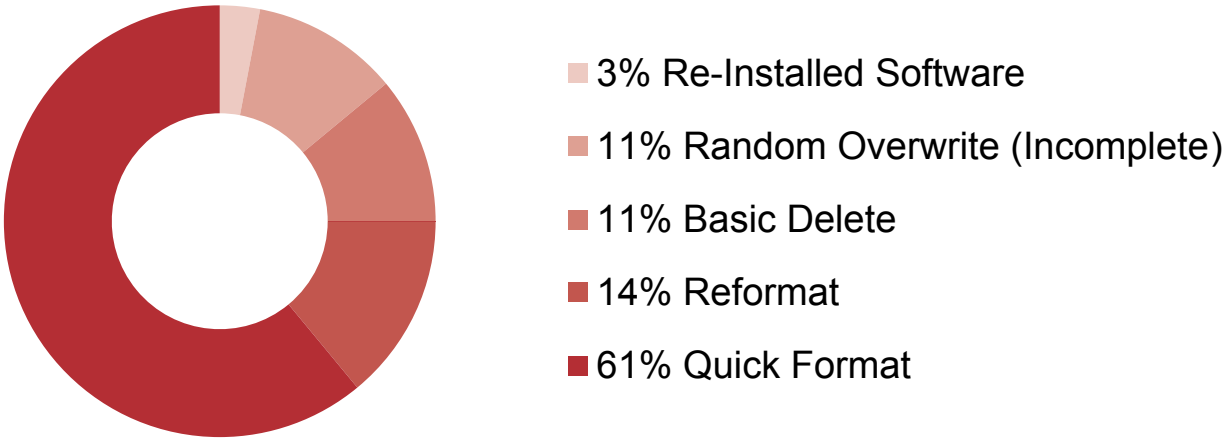
Hard Disk Drives: Results & Discussion

In reviewing and analysing the hard disk drives and solids state drives from 10 different manufacturers, nearly half (48 per cent) still held data on them, which could pose a security risk to the original owner.

What is the mix of hard disk drive / solid state drive manufacturers included in this study?



Which method was used to erase / wipe data from the drives containing data?



Basic file deletion commands leave users with a false sense of security.

For hard disk drives and solid state drives found to have residual data, 75 per cent showed that a deletion attempt was performed. Only 25 per cent were resold without any deletion method applied to them. This demonstrates that sellers are attempting to permanently wipe data, but they are failing to use a fully effective solution. On four of the drives containing data, or 11 per cent, only a basic delete was performed, meaning that the user simply deleted the file or sent it to the recycle bin. This type of deletion method made it easy to retrieve 100 per cent of the data stored on the drives. To be specific, a total of 444,000 files were found on these four drives.

When you simply delete files from your HDD or SSD, the file data remains on the drive. In reality, you are only deleting the pointers to the data. Imagine your drive is like a library. To find the book you want, you get a reference number from the library's database, which leads you to the section of the library where the book can be physically found. Imagine if the book was removed from the library's database and pointers to its location no longer exist. The book still remains in the library, but it now becomes a case of using more sophisticated methods to locate it. This same analogy can be applied to deleting files.

Quick format and reformatting tend to be default tactics used to wipe personal information clean from old hard drives.

Drives are like humans – they are not invincible nor do they live forever. When they reach end of life and replacement is inevitable, most people use very basic methods of wiping data in an attempt to protect their information and their online identities. Our study of 102 used HDDs and SSDs reaffirmed this common method, showing that quick format had been conducted on 61 per cent of the drives with data present.

This can be a serious problem, especially considering that 81 per cent of the quick format drives showed data still present. This falls in line with a recent study conducted by BT and SIMS Recycling Solutions, which revealed that 34 percent of discarded hard drives still contain confidential data.

For these reasons, it is extremely important to know that there are three types of hard drive formatting – low-level, quick and full – all of which work in slightly different ways.

- **Low-level Formatting:** This involves pattern filling the drive at the lowest level to reset it back to the factory settings. This is a time-consuming, but effective process and one that is rarely used. More commonly used are quick and full formatting.
- **Quick Format:** This method recreates the metadata area of the drive in order to create additional storage, but does not erase the data.
- **Full Reformatting:** The basic function of a full format is to scan all sectors of the drive, including bad sectors, remap them and wipe any active data. Results can vary by operating system.

According to Mike Burmeister, Director of Data Recovery at Kroll Ontrack, "Formatting to securely delete data can lead to varying results as each operating system performs the action differently. To successfully delete data to a state where it cannot be recovered, one must completely overwrite the data using reputable deletion software".

Impatience may be an invisible, but formidable, culprit in the incomplete sanitisation of hard drives.

Examining the used hard disk drives and solid state drives revealed that 11 per cent of the hard drives with residual data were wiped, but incompletely wiped, leaving a considerable amount of data waiting to be exposed. While it is impossible to pinpoint the exact cause, users might have become impatient with the length of time it would take to erase their drives. This makes sense when you consider, on average, it can take up to seven hours to erase a 500 GB hard drive. Additionally, incomplete sanitisation could be due to a broader failure in the wiping method or erasure solution that was used.

Personal emails, work emails, business presentations, sensitive financial documents, confidential company documents, photos, videos – these are all created, saved and shared across the digital universe. The challenge is that most people are not technical geniuses, information security gurus or data recovery specialists. They do not have the necessary knowledge, skills or training to fully understand which wipe methods are capable of erasing data forever – and which methods are not. Unfortunately, people and businesses, in particular, make a lot of incorrect assumptions, which can lead to a multitude of dangerous scenarios, including identity theft, online fraud and public shame. One assumption is that all delete methods are equally effective in erasing data. As we have shown in this study, this is not the case.

The best method for securely erasing drives, especially SSDs, is the random overwrite method used by erasure software. Interestingly, only six per cent of the hard disk drives and solid state drives in our study used this method. In each case, however, the random overwrite was 100 per cent effective and resulted in zero data remaining on the drives. Businesses and consumers alike would be wise to understand the effectiveness of the varying data deletion/wiping methods and leverage solutions that protect heir data and privacy.

What to Do to Safeguard Your Data

Before selling your mobile device:

- Research the value of your current mobile device. Prepping a mobile device for resale takes time and could include an added expense for proper erasure. Weighing the resale value versus the upfront investment will assist in making a sound decision whether or not to sell.
- Do your homework on the buyback programmes offered by retailers and online marketplaces like Amazon, eBay and Gazelle.com. Learn how the process works and what selling fees are involved.
- If you use your personal mobile device for work (BYOD program), check your company's data retention and BYOD resale policies for these types of devices.
- Back up any data that is important to you, or that you may need in the future, to another device, hard drive or cloud platform.
- Take stock of all the different types of data you have created, stored, saved and shared from your mobile device. That list will be useful to cross-reference after you have erased your data.
- Securely erase your data:
  - For an Android device, use the device settings to encrypt the data and then perform a factory erase function. Any residual data will remain encrypted and unusable.
  - Remove micro SD card (if applicable), or do not include it with the sale of your device.
  - For an iOS device, use the iTunes restore function, making sure to restore back to the factory setting or use "Erase All Content and Settings" from the iPhone menu. Both of these options delete the encryption key associated with the device rendering any remaining data (if any) unrecoverable.
  - For any mobile device, proven erasure software is the best way to guarantee deletion of all data. Research what software you are purchasing first to make sure it is specifically tailored to mobile devices and provides a certificate of erasure.
- If you used an external SD card to transfer data from one device to another, or to increase the storage size of your device, make sure to erase data from it too. To securely erase an external SD card – so that the data can never resurface – you first have to remove the SD card and insert it into a computer, which can correctly detect all of its sectors and run software to securely erase everything.
- Make sure the data erasure solution adheres to legally required overwriting standards, such as HMG Infosec and DoD 5220.22 M. Make sure the solution is approved by government agencies and bodies like NATO, Department of Defense, CESG, TUV SUD and DIPCOG, just to name a few.
- Ask for proof of erasure – this should be a tamper-proof certificate that cannot be altered after-the-fact. Think of it like an audit trail you would provide when filing your taxes. It is protection of privacy for the reseller and is also due diligence for the buyer of your used device.
- Double check that all of your data was, in fact, erased. Refer to your list of data types from number 5 on this checklist. If the reseller cannot provide proof of erasure, there are free data recovery solutions available to check your device.

Before selling your hard drive or solid state drive:

- Research the value of your hard drive or solid state drive before reselling it.
- Back up any important data to another drive or device.
- Securely erase your drive by using one of the following methods:
  - **Low-level Format Only:** Do not rely on a quick or full format to properly sanitise your drive.
  - **Overwriting Data:** This is the best method for SSDs and HDDs. When choosing an erasure software for overwriting, do the following:
    - Confirm the software can perform the right erasure method for your type of drive.
    - Confirm the total number of overwriting passes that are performed by the erasure software. Each pass signifies a complete overwrite of the drive with all 0's, all 1's, or random data. Three passes is enough for the U.S. Department of Defense's "Short" specification and for numerous militaries around the globe.
    - Confirm the company is willing to put the effectiveness of their software into writing with a tamper-proof certificate with all erasures displayed.
  - **Cryptographic Erasure:** Encrypt the data on the drive, verify all of the data is encrypted and then overwrite and delete the encryption key.
- Make sure the data erasure solution adheres to legally required overwriting standards, such as HMG Infosec and DoD 5220.22 M. Make sure the solution is approved by government agencies and bodies like NATO, Department of Defense, CESG, TUV SUD and DIPCOG, just to name a few.
- Ask for proof of erasure – this should be a tamper-proof certificate that cannot be altered after-the-fact. Think of it like an audit trail you'd provide when filing your taxes. Its protection of privacy for the reseller and it's also due diligence for the buyer of your used drive.
- Double check that all of your data was, in fact, erased. As with mobile devices, this step is very important. If the reseller cannot provide proof of erasure, there are free data recovery solutions available to check your device.

Conclusion

Data security threats are an increasing fact of daily life. Corporate data breaches and consumer data theft appear in the news and our lives almost daily. In 2014, the number of U.S. data breaches hit a record high of 783 (an average of 15 breaches a week), according to a recent report released by the Identity Theft Resource Center (ITRC).

With the prevalence of data security issues in our world, too many consumers and businesses are putting themselves at risk by not using effective and proven methods to protect their information before reselling their mobile devices and drives. Cyber theft and hacking is not solely focused on computers or servers any more. Savvy hackers can simply go online and find inexpensive used recovery software from which to steal valuable data.

Even the smallest amount of data can include enough personal or classified company information to cause irreparable damage. This data could be used in a number of ways – making online purchases with stolen credit card information, signing up for a new line of credit with personal/company information, blackmailing individuals or firms for ransom money with the threat of leaking sensitive information, or worse. The inventiveness of cyber criminals is unlimited.

Whether it is a smartphone, tablet or hard drive – used for personal or company purposes – all data should be fully and securely erased prior to reselling or disposal. Otherwise, there is a significant risk that sensitive information could fall into the wrong hands and cause reputational, financial and legal harm. Spending the time to learn the proper methods of data erasure is far more advantageous than waiting to become the next victim of a data breach.

About Blancco Technology Group

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organisations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organisations with an absolute line of defence against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk by xCaliber Technologies, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers' experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk (or Xcaliber Technologies) provides world-class support, pre and post implementation, allowing our customers to derive measurable business results. For more information, visit www.blanccotechnologygroup.com and follow us on Twitter at @BlanccoTech.

About Kroll Ontrack

Kroll Ontrack is the world leader in data recovery and provides technology-driven services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyse, and produce data efficiently and cost-effectively.

With 18 cleanroom facilities worldwide, engineering expertise in every major global region and over 25 years of experience, Kroll Ontrack provides successful solutions for all data recovery, data restoration and data destruction needs.

Data Recovery Services and Software: Recover data located on tapes, hard drives, mobile devices, virtual environments, operating systems or myriad of other storage devices through in-lab, remote and do-it-yourself capabilities.

Ontrack® PowerControls Software: Search, collect, recover, restore and manage data efficiently in Microsoft® Exchange Server, Microsoft® Office SharePoint®, or Microsoft® SQL Server® environments.

For more information about Kroll Ontrack and its offerings please visit: www.krollontrack.co.uk or follow @KrollOntrackUK on Twitter.

blancco technology group

Kroll Ontrack®