The Case for Mandating End-of-Life Media Destruction in Data Privacy Legislation

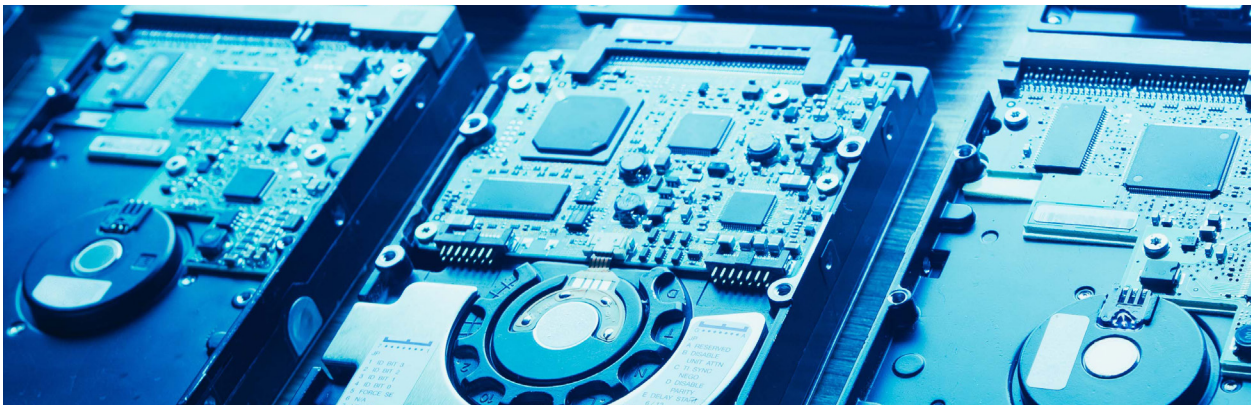
SEM®

Global Leader in High Security Information End-of-Life Solutions for Over 50 Years

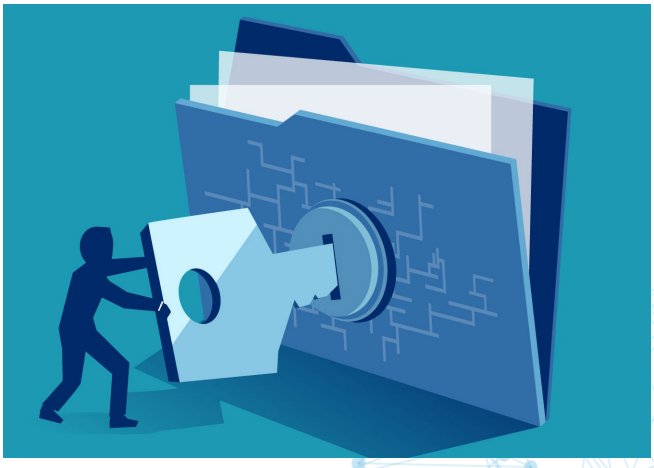
Data privacy regulations affecting United States citizens have been increasing in recent years.

From the General Data Protection Regulation (GDPR) that affects businesses selling to citizens of the European Union (EU) to the California Consumer Protection Act (CCPA) and New York's SHIELD Act, data security legislation is being enacted in parallel with the exponential increase in cybercrime and data theft. In 2019, the United States led the world by having the highest cost per data breach at $8.19 million, and the largest component of that number is attributed to lost business. Also, out of 26 factors studied that contribute to a data breach, third-party breach was the largest cost amplifier. (IBM Security and Ponemon Institute, 2019). As the US rushes to catch up with other developed nations in drafting and implementing data privacy legislation, one item is clear: data privacy regulations should include mandates for destruction of end-of-life media because failed and erased drives contain recoverable data, criminals target this data on end-of-life media for nefarious reasons, and breaches containing sensitive data have the potential to cause catastrophic damage to both organizations and individuals.

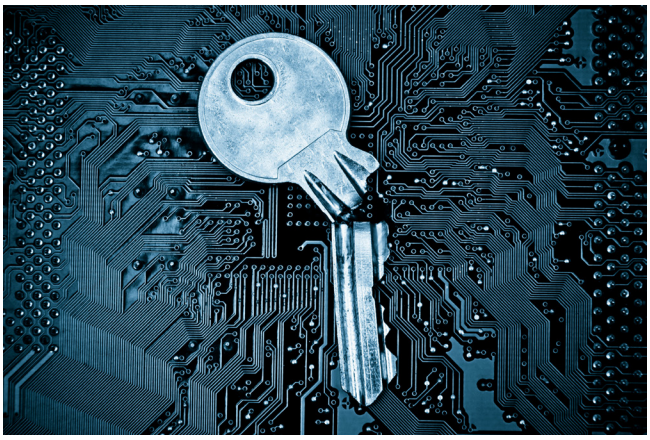
Many individuals and organizations make the argument that electronic devices should be recycled so the world consumes fewer resources. While this is arguably an important goal, it fails to consider the privacy concerns surrounding the staggering amounts of residual data left on end-of-life media,



even after erasing, reformatting, or overwriting. In a 2003 study conducted by then-MIT student Simson Garfinkel (et al.), who is now arguably one of the most respected experts in the field of data security and a leader at the National Institute of Standards and Technology (NIST), researchers purchased 158 used hard drives from secondary markets — mostly eBay — that were of varying sizes, conditions, and usages. Most of the drives had been erased or reformatted prior to being listed for sale, and those that weren't were mostly damaged or failed, or completely unbootable. Through various means of recovery, including both commercial and forensic data recovery tools as well as file structure analysis, the team of two student-researchers ended up recovering thousands of credit card numbers, personal emails and letters, hospital and financial records, personnel files, as well as other less sensitive data. One drive, which had been purchased as failed, had been used in the computer of an ATM and contained every transaction, account number and balance, and personal information that had been processed through the ATM. (Garfinkel, Shelat, 2003).



In a similar study conducted by Appalachian State University, researchers acquired 55 used hard drives of varying sizes and conditions from secondhand stores and charitable donations. Using readily available data recovery software, the team was able to recover over 300,000 files containing sensitive information such as social security numbers, financial and bank records, tax returns, wills,



credit and debit card numbers, email and chat content, and a plethora of personally identifiable information (PII). (Medlin et al., 2008). In yet another study conducted by the University of Glamorgan, over 100 hard disk drives that had been discarded for reuse or recycling by various organizations were found to have extensive amounts of sensitive data on them. The disks had originated from individuals as well as a pharmaceutical company and a university, among others, and the recovered information was concerning in its completeness. The data provided enough information to enable industrial espionage, network hijacking, and personal identity theft and subsequent fraud. A major leisure service company's disk actually contained complete financial records including an accurate financial forecast. (Jones, 2005).

While all of the aforementioned data recovery is certainly concerning, savvy organizations who implement some type of a more sophisticated data erasure, overwriting, or basic physical destruction methodology may assume their hard drives are unrecoverable. This reveals another data security flaw: unless a hard drive has been sanitized to standards adopted by the National Security Agency (NSA) of the United States of America for classified information, there is a chance of recovery. Depending on the extent of the erasure or damage, the recovery method may require sophisticated forensic or exotic processes, but the fact remains that the data still remains on the drive. Consider the tragedy of the Shuttle Columbia: in 2003, as it was minutes from landing at Kennedy Space Center after returning from an outer space mission to complete microgravity experiments, the Spaceship Columbia broke apart upon reentry into the Earth's atmosphere, instantly killing all seven astronauts on board. The remains of the crew and the ship's major components were recovered over the month following the accident, but the ship's hard drive was not recovered until seven months after the disaster. (Dooling, 2020).

The drive recovered after the Columbia explosion

The hard drive had started to melt upon reentry into the atmosphere, partially shredded when the ship blew apart, fell 40 miles to the Earth, and landed in a riverbed that had ultimately left the seal on the drive broken. The drive then stayed in that riverbed weathering the elements for months. Kroll OnTrack, data recovery experts, were given the drive to see if there was anything they could salvage. In fact, Kroll OnTrack ended up recovering 99% of the data from the drive, and the results of the experiments conducted by the deceased astronauts were published into a research paper that validated their pre-mission hypothesis. (Berget al., 2008). To the other researchers on the project, it provided some sense of closure. To data security professionals, it provided a sense of alarm. How could a drive that had suffered so much abuse be almost entirely recoverable? In the end, the platters inside the magnetic rotational hard drive had not been too damaged, and the platters are what store the information. (Valette, A. 2017).

As previously mentioned, the NSA maintains the most stringent classified data end-of-life destruction requirements worldwide. For magnetic rotational hard disk drives like the one in the Spaceship Columbia and like those traditionally used in laptop and desktop computers, the NSA mandates a two-step process: 1) they must be degaussed in an NSA evaluated and approved degausser, and 2) they must then be physically destroyed in an NSA approved crusher or shredder. Degaussing is the process by which either an extremely strong fixed magnet or an electromagnetic pulse is used against the magnetic media, scrambling the magnetic field along with the zeroes and ones. A drive that has been degaussed isn't just overwritten: it is rendered completely useless. Degaussed drives cannot be reused or repurposed. However, because the NSA is tasked with protecting national security, they take it one step further and require physical

destruction of the drive in an NSA approved crusher or hard drive shredder; the platters of the drive must be irrevocably deformed or broken. Admittedly, not every organization has the tools available to the federal government or to Kroll OnTrack for data recovery, but enough data has been retrieved off supposedly sanitized hard drives by regular people to give even the most casual user pause. After all, if there is a way to retrieve data off hard drives for studies, then there is also a way to retrieve data off hard drives for nefarious reasons. And there are plenty of criminals looking to mine data.

Criminals follow the money, and there is significant money to be made in data theft. Not surprisingly then, cybercrime has increased exponentially in parallel with the explosion of data. In a 2019 report, IBM Security found that malicious attacks were the costliest and the most prevalent type of data breach, costing on average $4.45 million per breach (as opposed to $3.5 million per non-malicious breach) and representing 51% of all breaches. Also concerning, malicious breaches represented 42% of all breaches in 2014, meaning breaches resulting from nefarious actions increased by 21% in just five years. (IBM Security and Ponemon Institute 2019).

Piles of e-waste in Agbogbloshie, Ghana

In addition to targeting online data for illicit purposes, criminals also seek out discarded hard drives. One such instance of this is in Agbogbloshie, Ghana in Africa. Developed nations— the United Kingdom and United States are by far the top two contributors —send about 215,000 pounds of e-waste to Ghana every year as an inexpensive solution for "recycling" or discarding used electronics such as cell phones, computers, tablets, and monitors. Anything that is functioning is resold is repurposed, and anything that isn't is sent to Agbogbloshie. One of the largest digital dumping grounds worldwide, Agbogbloshie contains giant piles of discarded e-waste through which local children rifle, mostly from slums, looking for gold or copper parts to resell. In addition to contributing to poverty and environmental pollution, Agbogbloshie is also home to a large contingent of criminals. While the local children are searching for precious metals, criminals look for computers from which they can take the hard drives. With some basic tools, these thieves are able to retrieve an exorbitant amount of data off these discarded drives that they then sell to cybercriminals on the dark web. These disposed drives are known to contain a plethora of data that is of extreme value to criminals.

In addition to the endless supply of financial institution, credit card, and personal info from which crooks can easily steal identities, hard drives and computers mined from Agbogbloshie have been found to contain some extremely sensitive information. One drive held information on $22 million worth of Northrop Grumman's government contracts, many of which were with the United States Military. Another drive from the computer of US Congressman Robert Wexler was found by a Ghanaian criminal to contain the Congressman's

personal information; this criminal then threatened to sell Congressman Wexler's social security number to identity thieves unless a ransom was paid. Additionally, equipment from US federal government organizations such as the US Army and Homeland Security has been found dumped in Agbogbloshie. (Global Commission on Internet Governance, 2017).

While the US government has strict standards for classified and top secret digital data destruction, there are no such standards for Controlled Unclassified Information (CUI) or Unclassified information. The US government for the most part follows standards set forth by NIST SP 800-88 *Guidelines for Media Sanitization*. NIST 800-88 specifies a final particle size of no more than 1mm x 5mm for paper, but makes no such specification for e-media, instead providing three options for e-media sanitization: clear, purge, or destroy. Clearing and purging have been proven to be ineffectual, and the destroy option provides only the vague guideline of "Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator." (Kissel, 2012). Information from federal government systems is mostly not classified, yet would still contain vast amounts of sensitive information including PII such as social security numbers and complete personal details, employee information and personnel files, personal health information (PHI), taxpayer information, court records, etc. In other words, simply because data is not classified does not preclude it from being highly sensitive as well as extremely valuable to criminals. Had there been a mandated end-of-life destruction policy on these computers and drives, the information they contained would never have found its way to Agbogbloshie to be breached and exploited by cybercriminals who cause devastating damage to businesses and individuals.

Breaches are not only becoming more prevalent, they are also becoming more costly, both in terms of financial impacts and reputation damage. Heartland Payment Systems suffered a calamitous breach in 2008 when Cuban-American Alberto Gonzalez and two unnamed Russian accomplices took advantage of a known vulnerability to perform an SQL injection that compromised 134 million credit card numbers. Not only did Heartland have to pay over $145 million in fraudulent payments and other compensation, they were also found to be in non-compliance with Payment Card

Industry (PCI) Data Security Standards (DSS) regulations and were thus disallowed from processing credit card transactions — of which they were processing over 100 million per month — for five months. In 2013 and 2014, Yahoo suffered two breaches that compromised three billion records, which included names, dates of birth, passwords and their associated security questions, and email addresses. Individuals suffered identity theft while Yahoo, who was in the midst of selling to Verizon, saw its selling price drop by an estimated $350 million. (Swinhoe, 2020).

In addition to the actual costs, lost business is another damage incurred by organizations who are data breach victims. In fact, lost business accounts for an average of 36% of the total losses resulting from a data breach and affects businesses for years after the breach. Lost business comes as a result of reputation damage and distrust from consumers and takes significant effort, time, and expenditure to rebuild. Small businesses with fewer than 1,000 employees are the hardest hit by data breaches, with an average cost per employee of $3,533 versus $204 for large businesses with 25,000 or more employees. (IBM Security and Ponemon Institute, 2019). It should come as no surprise then that 60% of small businesses go out of businesses within six months of a data breach.

Lost business (and revenue) post-breach is fully attributable to loss of consumer trust, which illustrates the true victims of data and identity theft: individuals. Data breaches are typically quantified in terms of lost revenue and damages paid by organizations, without taking into account the suffering and hardship faced by individuals whose sensitive and personal information was compromised. Some people have fought for years to have their names cleared from bad credit card debt and illegally opened accounts, and have had their credit and peace of mind destroyed in the process. Also considering the violation a person feels from the exposure of sensitive personal information, data theft is clearly a crime with far-reaching consequences, both financial and personal, and in the case of government agencies, matters of national security.

Data security is an exceedingly complicated and expensive cost center for organizations, while physical end-of-life data destruction is fairly straightforward and inexpensive; yet, many organizations pour millions into data security without considering the disposal of their end-of-life media. This illustrates that the reason sensitive and personal information is able to be mined form Agbogbloshie and eBay is not due to organizations' concerns over financial expenditures for data destruction equipment – it is due to a simple lack of knowledge that these devices and practices even exist. Any data privacy legislation should include minimum destruction requirements clearly defined for each type of media so that security is prioritized at all times and ignorance of best practices is not a valid defense.

The United States lags behind other developed nations when it comes to the data privacy of its citizens, and while there has been significant chatter in political circles about data privacy legislation and agencies, nothing has yet been formalized. As the US considers drafting any new data privacy legislation, end-of-life media must be part of the conversation. Often overlooked, failed and discarded hard drives frequently contain sensitive, confidential, or personally identifiable information that is highly valuable to criminals who specifically target this information. As data breaches continue to become more prevalent, they are also associated with significant and escalating costs to both organizations and individuals. In the case of end-of-life media, a simple solution exists to safeguard the sensitive information it contains — destroy the media — and any comprehensive data privacy legislation should clearly define and mandate it.

Heidi White, Director of Marketing
Security Engineered Machinery

A self-proclaimed data security geek, Heidi has over 25 years of marketing experience with targeted expertise in digital marketing, communications, branding, and teambuilding.

References

IBM Security and Ponemon Institute (2019). *Cost of a Data Breach Report.* Retrieved from https://www.ibm.com/security/data-breach

Garfinkel, Simson & Shelat, A. (2003). Remembrance of data passed: A study of disk sanitization practices. *Security & Privacy, IEEE*. 1. 17-27. Retrieved from https://www.researchgate.net

Medlin, B. D., Cazier, J. A., & Weaver, R. M. (2008). Consumer's PCs: A Study of Hard Drive Forensics, Data Recovery, and Exploitation. *Journal of Information Privacy and Security*, 4(3), 3–15. Retrieved from https://pdfs.semanticscholar.org

Jones, A. (2005). How Much Information Do Organizations Throw Away? *Computer Fraud and Security*. 5, (3), 4-9. Retrieved from https://doi.org/10.1016/S1361-3723(05)70170-6

Dooling, D. (2020, January 25). Columbia disaster. *Encyclopedia Britannica.* Retrieved from https://www.britannica.com/event/Columbia-disaster

Berg, R.F., Moldover, M.R., Yao, M., Zimmerli, G.A. (April 2008). Shear thinning near the critical point of xenon. *Phys. Rev. E* 77, 041116. Retrieved from https://doi.org/10.1103/PhysRevE.77.041116

Valette, A. (2017, November 1). How Kroll Ontrack Recovered Data from Space Shuttle Columbia. Retrieved from https://www.ontrack.com/blog/2017/06/21/kroll-ontrack-space-shuttle-columbia/

Global Commission on Internet Governance. (2017). *Cyber Security in a Volatile World* (pp. I-II, Rep.). Centre for International Governance Innovation. Retrieved from www.jstor.org/stable/resrep05239.1

Kissel, R. (2012). *Guidelines for Media Sanitization: Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-88r1

Swinhoe, D. (2020). The 15 biggest data breaches of the 21st century. *CSO Online.* Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Security Engineered Machinery Co., Inc.
5 Walkup Drive | Westboro, MA 01581
800.225.9293 | 508.366.1488
contact@semshred.com
www.semshred.com