Special Disposal Management Issue

ITAK

Information Technology Asset Knowledge

Volume 8 Issue 1

Safe Harbor Revisited

Updating End-of-Life Cycle Asset Disposition Guidelines and Standards

Mobile Asset Disposition
Are You Prepared for End-of-Life Management of Mobile Devices?

R2 Certified Recyclers
How R2 Recycling Offers Peace of Mind, and Why You Should Care

IAITAM

Safe Harbor Revisited

Updating End-of-Life Cycle Asset Disposition Guidelines and Standards

By: **Sean O'Leary**
Director of Communications, ***DestructData, Inc.***

A safe harbor is a provision of a statute or regulation that minimizes liability on the condition that the party performed its actions in good faith.

Introduction

End- of- life cycle media sanitization continues to occupy a limited area at the intersection of several larger worlds. As a result, guidelines and standards for information destruction have evolved in a somewhat haphazard manner, sometimes appearing to be an afterthought on the part of regulatory entities. A few years ago, I spent a lot of time reading the Federal Register in an effort to find a simplified approach to compliance with data security legislation. This was possible because the primary concern at that point fell under the purview of government privacy legislation. In a nutshell, Safe Harbor provisions in most federal and state laws pointed to NIST Special Publication 800-88: Guidelines for Electronic Media Sanitization as the source for best practices (more on that below).

Things have changed since then, adding electronic recycling / e-waste factors into the mix, as well as the ascendancy of non-governmental accrediting organizations. Further, NIST's "go to" Special Publication 800-88 document has been revised and is presently in the public comment stage. Technology also promises to change the game, as Solid State Drives enter the marketplace and mobile devices become pervasive.

Also, Congress has new Federal Privacy legislation in the works, which is the government's usual approach to clarifying uncertainty by adding new layers of regulation. I assure you that adding layers is the opposite of my intention here. What I hope to offer is an updated perspective on these matters, while noting in advance that, to some degree, the future is unknowable.

Although end-of-life-cycle media security is still wedged in among larger privacy, environmental and business considerations, it's fair to say it is no longer considered an afterthought.

Creative Visualization

It helps me to imagine the relevant regulatory and compliance entities as a series of interlocking spheres (see diagram). Two of the spheres fall under the category government: Privacy Laws and E-Waste/Recycling Laws. Although their core intents are not related, these spheres intersect in the media sanitization zone. Privacy and eWaste regs apply to quite different enterprise segments (IT professional vs. e-cyclers for example) that operate in relative isolation from one another. For media sanitization, there are powerful arguments for combining these professional domains in a single location, but this kind of convergence is just beginning to gain traction.

The third sphere contains standards and certification organizations, which we will cover in more detail later as we argue that these agencies are already supplanting government regulations in terms of establishing practical guidelines and standards. Although this could appear confusing, we believe it ultimately provides some clarity in an emerging marketplace.

Is the Safe Harbor Still Safe?

In earlier times, end-of-life-data destruction compliance anxiety was driven by state and federal privacy legislation. In

addition to better known Federal legislation such as Sarbanes-Oxley, FACTA and HIPAA, there are now forty six state and territorial laws that regulate the management of private electronic data.

- The individual acts differ with regard to:
- Classes of entities covered
- Definitions of personal information
- Identification of agencies selected for rulemaking
- Enforcement and other considerations

Regardless of other variations, privacy legislation consistently includes a provision that covered entities must securely destroy end-of-life cycle electronic private data. This is because, despite an IT propensity to focus on protecting data-in-motion, a significant percentage of data theft involves retired storage media.

The preponderance of legislation often creates a perception among compliance professionals that they are up against an interlocking, conflicting and overlapping matrix of government oversight. They are essentially correct about the interlocking and overlapping characteristics, but the "conflicting" attribute is not necessarily the case for end-of-life-cycle disposal issues.

This is because the specific technical nuts and bolts of data erasure and physical destruction are not referenced in any actual legislation language I know of (so it isn't strictly accurate to describe a company or procedure as "FACTA compliant" or "HITECH approved" or even "NIST-approved"). Instead, the various legislative acts describe the *intent* of the law, then direct a government agency to develop real world "guidance" that determines rules governing practical execution.

Once the initial guidance or "rule" has been written, it is published in the Federal Register for public comment. I know this because I am the guy that reads it instead of watching Dancing with the Stars. Eventually – after industry lobbyists have done their best to water it down and activists have done their best to strengthen it - the final rule goes into effect. Although many laws identify multiple agencies for oversight, the lead federal agency for rulemaking in this aspect of privacy law is almost always the Federal Trade Commission (FTC).

In terms of practical solutions then, a privacy or compliance professional will be looking to the guidance rule rather than to the legislation itself. Almost all laws reference the same rule. In almost every case I know of, these guidelines are expressly meant to be flexible and to be consistent with similar laws.

Furthermore, most agency rulemaking specifies that compliance with rules imposed by other jurisdictions is satisfactory. As a result, most federal guidance is notably (and perhaps notoriously) non-specific, tending toward "examples" than requirements. For instance, the FTC describes its key Disposal Rule as allowing covered organizations to "determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology." Reasonability, of course, is a word that invites many alternative interpretations.

This self-referencing rulemaking process has resulted in de facto adaptation of the recommendations published in the National Institute of Standards and Technology's (NIST) Special Publication 800-88: Guidelines for Media Sanitization. Issued in 2006, this report identified multiple methods for destroying data on electronic storage media and ranks them according to security level. It also recommended bare bones protocols for program structure and auditing processes.

The prevailing consensus is that the language found in government data disposal rules establishes a Safe Harbor scenario for covered entities that have applied technologies and methods referenced in the guidance. A safe harbor is a provision of a statute or regulation that minimizes liability on the condition that the party performed its actions in good faith. Good faith is a term that also invites a range of alternative interpretations.

In summary, government guidance does not require specific data sanitization methods, but acknowledges that, if used, they will "create the functional equivalent of a safe harbor" for security levels below top secret classification. Nevertheless, data destruction solutions and products that are described as NIST-approved are not being strictly accurate. NIST establishes guidelines. It does not approve or disapprove of any product. It is therefore up to the organization to match its objectives with a particular method or combination of methods.

The Data Security and Breach Notification Act of 2012, Oh My

The Federal government is by nature compelled to preempt as much power from the states as it can, especially if they have succeeded passing laws the U.S. Congress should have passed. Whenever Congress looks to bring new legislation in areas states have already covered, the explanation will be that they are trying to eliminate confusion and conflicts among state laws.

To this end, major new federal privacy breach notification acts have been sitting in Congress for several years now. But because they can't seem to make it to the Senate or House floor, Senator Pat Tomey (R) PA has introduced Senate Bill 3333 (Data Security and Breach Notification Act of 2012), which proposes to do what the now defunct HR2221 and DATA were previously going to do.

Some people wonder how this new and comprehensive data breach notification bill could manage to exempt banks and financial institutions, but we are not among those who wonder. The good news is that should SB 3333 pass, it will have no impact on your professional life. As was the case with its predecessors, the bill fuzzily "Requires commercial entities

that acquire, maintain, store, or utilize personal information (covered entities) to take reasonable measures to protect and secure data in electronic form containing personal information." Like most previous legislation, it charters the FTC as the lead enforcement agency, so there will be no threat to NIST SP 800-88 as the guiding light for media disposal compliance.

Of course, this venerable 2006 publication is also in a state of transition…

Updates to NIST SP 800-88

The first revision of Special Publication 800-88 is currently posted on the NIST website (www.nist.gov) in draft form, meaning it is open for public comment. This means the final form is uncertain until the final version is vetted and adopted.

However, we can gain some insight into what to expect by comparing the original version with the current draft. The most notable changes are the expansion of the types of storage media included in the recommendations, notably Solid State Drives, and specific smart phone and tablets that didn't exist in 2006. Equally important, the Verify and Documentation sections have been significantly expanded. This update reflects the increasing focus on the overall of end-of-life cycle process as opposed to specific sanitization methods. There is no reason to expect that this revision will require any major changes to asset disposal protocols.

E-Waste Legislation and Standards

The second sphere is colored green by virtue of the fact that the objective of the regulations is to bring about a less toxic planet. If the goal is to keep electronic hardware out of landfills or prevent shipment overseas, it follows logically that the need to be able to erase data housed on assets that will be re-marketed or re-purposed in any other way is a critical linchpin in the economic model. Unfortunately, in the realm of the rapidly emerging e-waste sector, Congress has failed to take meaningful steps. The EPA website says:

"At present, there is no Federal mandate to recycle e-waste. There have been numerous attempts to develop a Federal law. However, to date, there is no consensus on a Federal approach."

Even the "no-brainer" Responsible Electronics Recycling Act of 2011 (HR2284) remains a victim of Washington DC gridlock.

Into this breach have stepped state legislators and two third-party certification organizations. Led by California, twenty-five states have passed e-waste and electronics recycling laws (according to the Electronics Recycling Coordination Clearinghouse). However, very few of these laws include requirements for the sanitization of recycled media, with the notable exception of New Jersey. The most comprehensive law in terms of covered devices, New York State's Environmental Conservation Law, does not include the terms "data", "security" or similar terms. It is clear from the language of the regs that the primary concern of the law is to remove hazardous materials from the environment, with concern for data security lagging.

However, some sort of patchwork regulation is slowly emerging among the states with regard to data security. For example, New Jersey's proposed Senate bill S3159 establishes new protocols that require a verifiable chain of custody for the equipment. Note also that many electronic storage media is already covered under existing privacy law.

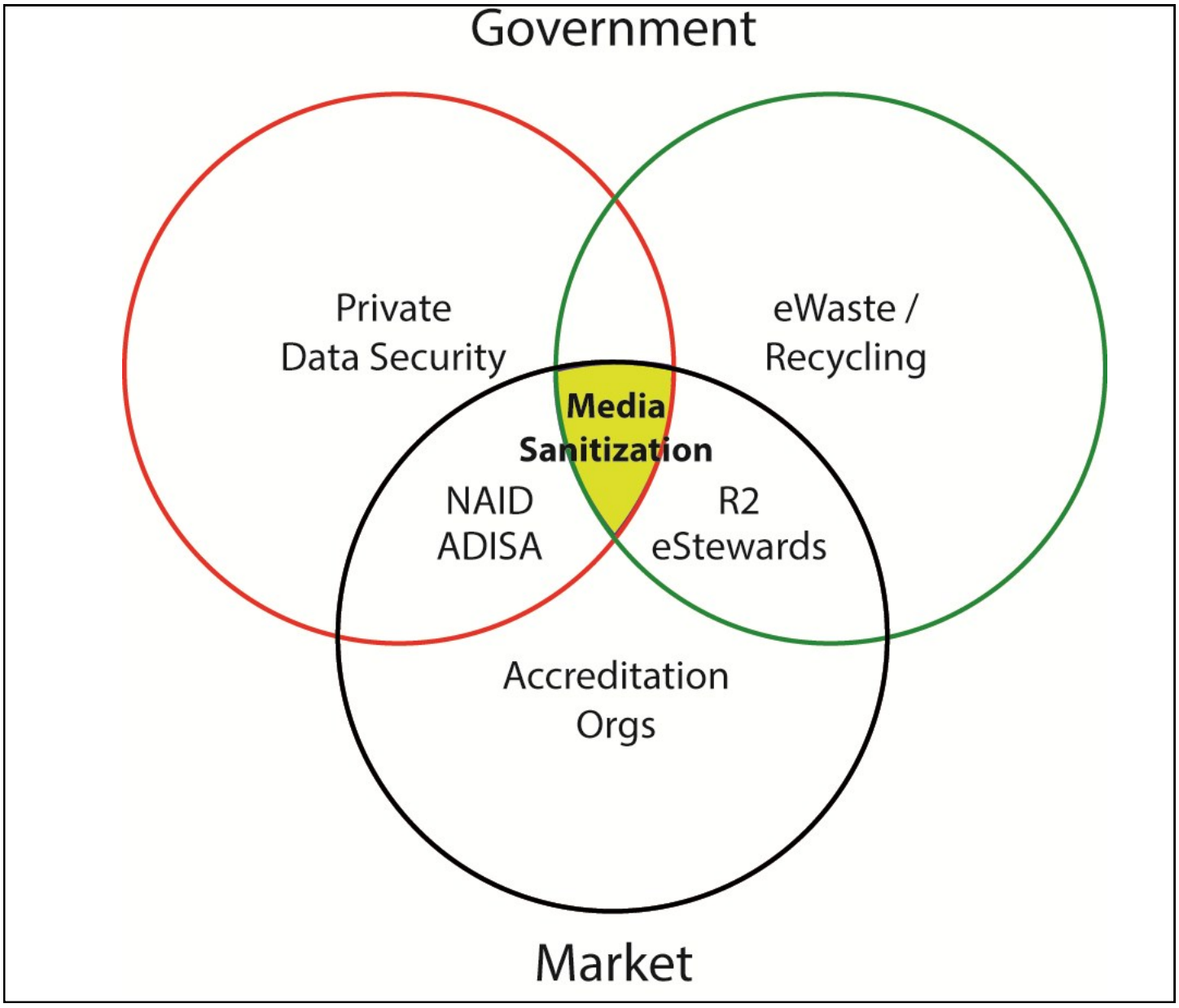
Third Party Certification

Nevertheless, it is obvious to any reasonable person that data must be removed from digital storage assets if asset reuse is to be economically viable. Two non-profits have established certification standards for e-recycling: the Basel Action Network's eStewards watchdog initiative and Responsible Recycling (R2). With the February 2012 incorporation of R2 standards within the larger e-Stewards program, the guidelines for **media sanitization** have been standardized between these two accrediting organizations. Again, both eStewards and R2 point to NIST SP 800-88 in their sanitization guidelines, but with the addition of more specific guidelines for process control. According the official eStewards documents, "The Steward's operational framework must govern 1) what must be done, 2) how the operation must be performed, and 3) how to manage exceptions/errors. The record keeping system must document execution of everything above in detail, and with transparency."

Similarly, the National Association of Information Destruction (NAID) first introduced a data destruction certification program nearly a decade ago. Due to its roots in the document destruction industry, NAID originally focused on physical destruction and degaussing, both of which render hard drives unusable. As the trend toward recycling and remarketing of drives emerged, however, NAID was compelled to develop media sanitization standards which are also based on the guidelines in SP 800-88. As is the case with eStewards and R2 accreditation, the NAID program has expanded and narrowed what NIST has to say about auditing, quality controls and best practices.

In the international arena, UK based Asset Disposal and Information Security Alliance (ADISA) was launched in 2010. This global certification body is expected to roll out its own IT Asset Disposal standard in North America in 2013 with an emphasis on globalization of processes.

The upshot of these relatively recent developments is that the "requirements" for media sanitization in data at rest scenarios is rapidly becoming market-driven rather than government driven. Organizations in the business of IT asset disposal now find that certification of some kind is necessary for credibility within their industry segment.



Is this all good? Having observed the development of similar standards in a number of other industries, I am comfortable stating: this is a welcome trend and it's great for business, with the caveat that we need to make sure it does not become burdensome. In their time, the rather vague guidelines set forth in existing privacy laws and even the original NIST SP 800 -88 served the purpose of allowing individual organizations to establish data security programs that made sense for their business model. The NIST 800-88 guidelines don't eliminate the need to take relevant technical, cost/benefit, environmental and custody/control factors into consideration, rather, they provide an outline for evaluating these parameters.

So, while deeper guidance is usually valuable, I want to make passing reference to what I call the ISO syndrome, which can limit flexibility in member businesses by locking in processes. Having said that, I hasten to add that we are a long way from that point; DestructData has been busy developing new tools in anticipation of expected upgrades to verification and auditing requirements.

Although we can't predict the future, we are now in a position to answer our original question: it appears for the time being that compliance with any of these third-party certification programs will well exceed any government regulatory requirements, so the "Safe Harbor" umbrella is still in place.