INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

SUMMER 2016 VOLUME 7 ISSUE 3 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

Inherent Risk Associated with Internet Exposed Critical Infrastructure

By Bob Radvanovsky

For most of us, our daily lives within our countries take for granted three tactical infrastructure sectors (often referred to as the *"Triad Sectors"*): Energy, Water, and Transportation. These make modern-day living possible. If one (or any combination) of these three infrastructure sectors is substantially disrupted or destroyed, the consequences will be undeniably significant. Many things can disturb these sectors, but one very *Read more*

Intellectual Property Protection for Big Data in Canada and the United States

By Jason Tsoukas and Nathaly J. Vermette

In the summer of 1960, Senator John F. Kennedy accepted his party's nomination to run for the Presidency of the United States of America. In his address, he famously ushered in a new era and spoke of a new frontier and of unprecedented changes in society. He spoke of the challenges of modernity, of the management of a technological revolution. He pointed to an output explosion on farms but lamented the fact that *Read more*

Making the Business Case for Defensible Disposition

By Dan Nichols and Diana Fasching

Over-retention of information imposes unnecessary high costs and risks. Disposition mitigates those costs and risks, but it must be defensible to avoid the potentially catastrophic costs of deleting the wrong information at the wrong time. Fortunately, recent amendments to Rule 37 of the Federal Rules of Civil Procedure and advances in technology make the cost-savings and risk reduction more accessible. Specifically, these *Read more*

The Internet of Things: Data Protection and Data Security in a Global Environment

By Jami Mills Vibbert

The Internet of Things or IoT is an interconnected network of physical and virtual objects (like wearable health monitors) with embedded sensors that allow communication of information across and among those devices. IoT devices are characterized by their capture of a large amount of data, automatic data transfer, and interoperability. The IoT is comprised of pervasive sensors, collecting large amounts of data, *Read more*

2016 (1H) Information and Internet Law Updates: Cases, Statutes, and Standards

By Thomas J. Shaw

In the first half of 2016 and the end of 2015, there have been many developments in U.S. and international information and Internet law cases, statutes, and standards. These developments include international and U.S. state and federal statutes and regulations passed or coming into force, civil and criminal cases and enforcement actions brought by regulators, and new standards, guidelines and legal ethics opinions. To briefly *Read more*

Making the Business Case for Defensible Disposition

By Dan Nichols and Diana Fasching

Over-retention of information imposes unnecessary high costs and risks. Disposition mitigates those costs and risks, but it must be defensible to avoid the potentially catastrophic costs of deleting the wrong information at the wrong time.

Fortunately, recent amendments to Rule 37 of the Federal Rules of Civil Procedure and advances in technology make the cost-savings and risk reduction more accessible. Specifically, these changes provide a catalyst for organization to invest in reasonable and legally defensible approach to keeping or discarding information.

The High Costs of Keeping Too Much Information

Given the risks of destroying the wrong information at the wrong time, it may be tempting to simply "save everything" in response to the daunting problems of managing increasing data volumes and the growth of "dark data." ("Dark data" refers to data that was generated for a purpose but is no longer being used by the organization). However, retaining too much information negatively impacts companies in a myriad of ways, including: cumulative storage costs, data breach exposure, increased litigation costs and risks, costs to comply with privacy regulations, and, ultimately, decreased profitability. Additionally, over-retention leads to inefficiencies as employees struggle through an information "fog" to find the desired information.

Storage Costs

The most obvious cost of storing too much information is the cost of storage. Over the past decade, the cost of storage trended dramatically downward, dropping by a 100-fold. However, at the same time, the increased volume of generated data also grew exponentially, eating up potential cost savings. In addition to the hardware and infrastructure costs, organizations employ various software solutions to manage all of that data. Broadly speaking, such storage software needs include: data protection and recovery, archiving (including email archiving), storage replication, storage management, storage device management, storage infrastructure, and file system. The global market for such software has remained relatively constant, even while storage costs have dropped, indicating that cheaper storage platforms do not necessarily equate to net cost savings. Moreover, the budget line item for server farms or cloud space does not capture the full costs of information storage, including real estate, energy, disposal, and environmental costs. And storing large amount

of data over time can lead to additional costs attendant to maintaining legacy systems that are no longer supported by the original distributor.

Data Breaches

According to a Ponemon Institute Report, the average cost of a data breach in 2014 was $3.79 million or $154 per sensitive or confidential record that was unintentionally made available to the public.[1] And according to that report, those costs are rising. At the higher end, data breaches can pose hundreds of millions of dollars in direct damages to a business. In addition to the hard costs of a security breach, an organization may suffer reputational damage that amounts to billions of dollars.

High profile breaches such as the Sony Pictures Entertainment hack in 2014 remind us that leaked emails can be as damaging as stolen credit card numbers. One can wonder how much of the damage to Sony's reputation could have been avoided if at least some of the obsolete emails had been purged before the hack. Information that no longer exists poses no security risk.

And as the so-called "Panama Papers" scandal recently demonstrated, service providers such as law firms are not immune to the risk of data breaches. Indeed, there is evidence that cybercriminals are specifically targeting law firms because of the sensitivity of the information held by firms.[2] In short, every business is a potential security target.

Litigation Cost and Risk

Having too much information increases the costs and risks of litigation. Preserving, collecting, reviewing, and producing information in response to litigation or a government inquiry can be an extremely costly undertaking. For example, Microsoft reported that it spent over $600 million on eDiscovery vendors and outside counsel over the past ten years.[3] eDiscovery costs depend in part on the volume of data processed for a given case. The charges per gigabyte for preservation, collection, and production of data in litigation can add up quickly. Even with the advent of Technology Assisted Review and other innovations, organizations continue to incur substantial legal fees for review.

In addition, information that no longer has business, regulatory, or legal value to a company can be used against it in litigation. One company's information trash can be an adverse party's treasure. An unfavorable email that could have been defensibly deleted prior to litigation may cause real

---

[1] The Ponemon Institute, *2015 Cost of Data Breach Study: Global Analysis,* May 2015 (http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF).
[2] The American Lawyer, *'Panama Papers' Put Spotlight on Law Firm Data Security*, April 4, 2016 (http://www.americanlawyer.com/id=1202753986288/Panama-Papers-Put-Spotlight-on-Law-Firm-Data-Security?slreturn=20160410125027).
[3] *See Preliminary Draft of Proposed Amendments to the Federal Rules of Civil Procedure*, No. USC-Rules-CV-201300002, Cmt. by David M. Howard, Microsoft Vice President & Deputy General Counsel, 5 (Feb. 15, 2014).

damage in the hands of an opponent at trial. Information that is disposed defensibly need not be preserved, collected, analyzed, reviewed of produced.

Managing Privacy and Other Protections on Information

Organizations are subject to many privacy regulations. In the United States, we have no comprehensive data privacy regulation, but rather a web of piecemeal state and federal regulations on discrete topics.[4] Virtually every federal agency has responsibility for overseeing some privacy regulation (including the Federal Trade Commission, Federal Communications Commission, Consumer Financial Protection Bureau, and the Department of Health and Human Services Office for Civil Rights), and State Attorneys General have parallel jurisdiction under some regulations. Complying with all of these various directives and responding to government inquiries require legal representation and significant investments in information governance.

Europe has its own set of rules, including the recently enacted General Data Protection Regulation ("GDPR", due to take effect in 2018). In what has been described as "the world's single most significant — and severe — data privacy law to date,"[5] the GDPR protects the privacy of European consumers' data wherever it is located. Additionally, many other jurisdictions throughout the World have comprehensive regulatory schemes. In the globalized economy, neither the GDPR nor the other regulations can be regarded as merely regional concerns.

Privacy laws primarily protect the improper disclosure or use of Personally Identifiable Information (PII). The definition of PII is quite broad and can include information that would be available on a person's driver's license, as well as social security numbers, specific financial information such as credit card numbers, personal characteristics and other biometric data.[6] Penalties for releasing PII can be substantial ranging from thousands of dollars per violation to 4 percent of global revenues (under the GDPR).

Additionally, organizations may be subject to other regulations regarding the handling of information. For example, under the Protected Critical Infrastructure Information Program, the Department of Homeland Security works with infrastructure owners to secure critical infrastructure and protected systems.

---

[4] *See* Stephen Cobb, *Data privacy and data protection: US law and legislation* (http://www.welivesecurity.com/2016/04/26/data-privacy-data-protection-us-law-legislation-white-paper/) ; *see also* (http://www.privacyjournal.net/_center_compilation_of_state_and_federal_privacy_laws__center__3077.htm)

[5] TechCrunch, *Don't Sleep on New Data Privacy Regulations* (Feb. 5, 2016) http://techcrunch.com/2016/02/05/dont-sleep-on-new-data-privacy-regulations/

[6] Ericka McCallister, Tim Grance, and Karen Sarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology, Apr. 2010, (http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

A central tenet of privacy regulation is that such information must be kept only so long as necessary. If information is defensibly deleted, the risks associated with improper access from a security breach or other improper use are avoided, as well as of course the costs to store and maintain.

The High Costs of Keeping Too Little Information

The disposition of information must be *defensible* to achieve cost savings and avoid the potentially catastrophic consequences of improper deletion. The cost of indefensible disposition can be enormous.

Litigation horror stories of failures to preserve ESI (Electronically Stored Information) that should have been preserved for litigation and resulting sanctions have been in the news for some time now. The destruction of relevant ESI has landed quite a few organizations in hot water, resulting in monetary sanctions and fees and costs, exclusion of evidence, adverse inferences, terminating sanctions, and even criminal prosecution. Monetary sanctions, exclusion of evidence, and adverse inferences are the most common remedies employed by the courts. Such remedies can be quite damaging, such as a $1 million sanction for modifying file dates and wiping disks clean of their data (*Rosenthal Collins Grp., LLC v. Trading Technologies Int'l, Inc.*, 2011 WL 722467 (N.D. Ill. Feb. 23, 2011)) or evidentiary sanctions that essentially end the litigation. When the facts call for it, courts will end litigation for discovery abuses. *Hosch v. BAE Sys. Info. Solutions, Inc*., 2014 WL 1681694 (E.D. Va. Apr. 24, 2014).

Additionally, sanctions for spoliation can cause long-lasting reputational harm. In one case, the court ordered the offending defendant to file a copy of a sanctions order in every case for the next five years, detailing how the defendant failed to preserve relevant evidence. Even without the unique requirement to file such an order in every case, an adverse finding or other sanctions can haunt a party or its law firm.

Aside from the circumstances regarding litigation, retention of critical information in the ordinary course of business is equally significant. For example, having adequate evidence of insurance policies and coverage over time can be significant in order to make claims in the event of latent emergence of liabilities. As such, indiscriminately purging corporate information is simply ill-advised.

The Return on Investment for Defensible Disposition

The overall cost of retaining information can be conceptualized as follows:

storage costs (including hardware and software management costs)

\+ costs of security per unit of information

\+ risk of security breach * cost of breach (including reputational)

\+ future eDiscovery litigation costs to preserve, collect, and process

\+ risk of "bad" evidence found in litigation * injury to litigation position

\+ costs to comply with privacy and other information regulation

\+ risk of violation of privacy or other regulation * cost of violation

cost to retain information

In many instances, the cost to retain a given piece of information is worth it. Business needs, regulatory requirements, or other legal obligations can justify—even mandate—retention of information. However, when the law does not require retention and business needs do not justify it, the cost of retention exceeds the price of disposition.

While litigation and security risks often drive the disposition discussion, a business can enjoy other business benefits when it gets rid of information no longer needed for business, regulatory, or litigation purposes.

Less Clutter

Although the problem can be challenging to quantify, an excess of obsolete or useless information contributes to an "information fog," leading to lower productivity.[7] The less information organizations are forced to comb through, the more readily employees can find the information with real value needed to make informed business decisions. Even with advanced analytics, having a corpus of "good" data to assess will almost always provide better (and faster) results than forcing algorithms to digest and consider data that is known to be obsolete or incomplete.

More Efficient IT Infrastructure

Organizations cannot indefinitely maintain legacy systems and the information contained within them. Institutional knowledge of older systems disappears over time as people leave or change jobs. Organizations can achieve cost savings when they take defensible steps to archive, migrate, and/or delete data before upgrading or retiring legacy systems. Indeed, with the right process, organizations can eliminate certain legacy systems and data altogether. Even where outright disposition is not available, organizations can achieve cost savings by migrating information from immediately available "active" storage to less expensive, lower-tier secondary storage.

[7] *See* The Economist, Schumpeter, *Too much information: how to cope with data overload* (June 30, 2011).

Lower Records Retention Costs Overall

When retention policies have not been updated, analyzed, or properly synthesized, organizations can spend time carrying out a variety of records retention policies (and de facto practices) for information that no longer needs to be retained. All of this wasted activity is akin to reorganizing the trash bin.

The Costs of Defensible Disposition

Defensible disposition requires employee time and competent legal guidance to regularly update records retention policies and schedules; understand and aggregate the organization's legal holds; and review and analyze the legal defensibility of decisions to preserve or dispose of information.

Additionally, an ESI vendor may be tasked to provide enabling technologies and processes, such as sampling or technology assisted review, to "right-size" retention. Taken together, this investment can generate a profitable return in avoiding the costs of excess retention as well as creating additional business benefits (discussed above).

Recommendations

To be effective, defensible disposition requires a business-oriented approach, prudent planning, and an appropriate use of technology.

Turn a "Legal" Problem into a Business Solution

Frequently, Legal is the over-retention scapegoat. Often, the reason given for over-retaining information is a vague recollection that at one time or another Legal issued an edict to "save everything" into perpetuity, though the precise rationale is no longer clear. Likewise, solving the over-retention problem is sometimes confined to a "Legal" problem.

Defensible disposition works when the critical players are convinced that it is a business solution and not just another directive from Legal. Ideally, each business area is responsible for, and timely acts on, deleting information that the business no longer requires for business use, records/regulatory reasons, or because it is no longer subject to legal hold. By involving the business, legal and business can jointly own the responsibility and well as a jointly own the success.

On a higher level, in a well-run operation, information governance has multiple stakeholders giving input and taking responsibility to proactively set up good records practices. With a solid information governance program and open lines of communication, business areas can get the clarity they need to comply with legal obligations while meeting appropriate and proportional legal hold requirements.

Planning: Find Opportunities for Disposition

Finding opportunities to dispose of information requires planning. The needs and obligations to retain information are dynamic. Regulatory environments change and opportunities to discard obsolete information may arise when a case ends or enters a new phase. The Sedona Conference® has stated that "[a]ny legal hold policy, procedure, or practice should include provisions for releasing the hold upon the termination of the matter at issue so that the organization can adhere to its policies for managing information through its useful lifecycle in the absence of a legal hold."[8]

Windows to dispose can close unexpectedly. If organizations do not dispose of legally destructible information when they have the opportunity, they may find themselves bound to manage the same information for longer than they otherwise would have. Likewise, opportunities to dispose of apparently useless and irrelevant information can disappear when a new variety of previously unforeseen litigation arises.

Even in the middle of litigation, an organization can—with an attorney's assistance—find ways to "right-size" a litigation hold in place to relieve some of the burden of retaining information that is not connected to the claims and defenses in the matter.

Defensible disposition requires putting a protocol in place that:

(a) identifies data potentially subject to disposition;

(b) assesses the (i) business utility of the information, (ii) the relevance to pending litigation, and (iii) any regulatory need to keep the information; and

(c) enables a decision-maker to retain or dispose of data or take other appropriate action.

A thoughtful and well-documented protocol can help an organization achieve the cost-savings of defensible disposition while mitigating the risk of sanctions for destroying evidence.

The amended[9] Rule 37 addresses what happens if ESI "that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it." First, the new rule asks if the lost information can "be restored or replaced through additional discovery." If not, then the Court "upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice." Only if the Court finds that a party acted with "intent to deprive another party of the information's use in the

---

[8] Sedona Conference, *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, at 51 (2d ed. Nov. 2007).

[9] In light of how recently Rule 37 was amended, a note of caution is warranted: courts are still working out frameworks for applying the rule. See, e.g., *CAT3, LLC v. Black Lineage, Inc*., 2016 WL 154116, at *11 (S.D.N.Y. Jan. 12, 2016)); *Living Color Enterprises, Inc. v. New Era Aquaculture, Ltd*., 2016 WL 1105297, at *4 (S.D. Fla. Mar. 22, 2016)); *Marshall v. Dentfirst, P.C.*, 2016 WL 1222270, at *3 (N.D. Ga. Mar. 24, 2016).

litigation," may the Court issue case changing sanctions (discussed above) beyond the remedies that would otherwise be available.

A defensible disposition program benefits a company by increasing its ability to show that deleted information was not subject to a duty to preserve in the first instance. In other words, before the litigation bell has even rung, defensible disposition can rid the company of information that might have needed to be preserved and processed – and the company can demonstrate that the information was disposed in the ordinary course.

A formal, documented defensible disposition program protects a party from a charge that it "failed to take reasonable steps to preserve the information." As the rule-making committee recognized:

Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible.

* * *

This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection.[10]

A thoughtful process for disposing of obsolete information has a good chance of taking advantage of the "reasonableness" standard even if it fails to achieve to perfection.

Moreover, even if a company gets it wrong, documenting its defensible disposition efforts can go a long way toward avoiding a finding that the party acted with "an intent to deprive", avoiding the more punitive sanctions available to the courts.

Using Technology in Defensible Disposition

Conducting a manual review of all of the information subject to disposition is simply impractical. Increasingly, companies are using tools and technologies to implement defensible disposition strategies. For example, companies may consider using tools to identify junk data that clearly has no business value (e.g., personal emails, advertisements, and solicitations) to proactively rid their systems of excess data. The same technologies used in eDiscovery (such as advanced analytics and technology-assisted review) can be used to help reduce a company's information inventory. Another example: a company can apply tape indexing or analysis engines to backup tapes without the need to fully restore the legacy environment for the media in order to determine whether the media can be retired. All of these technological innovations can result in higher returns on investments in defensible disposition.

[10] Committee Notes, 2015 Amendment, Fed. R. Civ. Pro. 37(e).

Conclusion

Over-retention of information imposes increasingly high risks and costs in practically every industry. Accordingly, businesses save money and reduce risks when they engage in defensible disposition.

Investments in defensible disposition efforts work best when approached as a business solution (rather than a legal problem). Further, defensible disposition can now take advantage of new technologies to help the business and legal counsel to defensibly categorize and cull the data. Finally, the recent amendments to Rule 37(e) of the Federal Rules of Civil Procedure better frame the risks and benefits by placing them into a more predictable framework, which in turn allows organizations to make defensible disposition decisions in many more circumstances with much greater confidence.

Dan Nichols *is Of Counsel at Redgrave LLP. He is not only a seasoned trial attorney with extensive experience handling eDiscovery in matters ranging from single plaintiff cases to mass tort and class actions, but also a strategist who has worked with large corporations to address information governance challenges. He represents businesses of all sizes in complex commercial, construction, products liability, and environmental litigation. Dan's extensive experience guiding matters from inception at the pleading stage, through all phases of discovery, motions practice, settlement negotiations and trial, provides him with a unique and practical understanding of how eDiscovery strategy impacts budgets and outcomes. Likewise, his past experience representing large oil and chemical companies involved in environment and toxic tort litigation provides Dan with keen insights into large scale corporate and litigation challenges. Dan received a J. D. (magna cum laude) from J. Reuben Clark Law School, Bringham Young University and a B.A., Political Science (magna cum laude), from Southern Oregon University. He is admitted to practice in California, Oregon and Washington.*

Diana Fasching *brings more than 15 years of experience to her role as a Senior Advisor at Redgrave LLP. With a professional background that spans both legal and corporate environments along with a Master of Science in Software Engineering, she has a unique understanding of the significance information plays in litigation and information governance. Diana works collaboratively with clients' legal, business, and information technology teams to understand and manage complex technical systems and infrastructures. From conducting records management and discovery readiness gap analyses to contributing to the development of legacy data disposition plans, Diana plays an integral role in identifying issues and recommending solutions as they relate to the life cycle of information and the integration of emerging technologies. Diana is involved in the Compliance, Governance and Oversight Council and is a member of the International Association of Privacy Professionals. Diana received a B.A. from the University of Wisconsin-Madison and an M.S. in Software Engineering from the University of Minnesota–Twin Cities.*