INFORMATION MANAGEMENT AND THE COURTS – AN UPDATE

By

John C. Montaña J.D., FIIM, FAI

October 1, 2018

Project Underwritten by:

ARMA METRO NEW YORK CITY CHAPTER

www.armaedfoundation.org

Table of Contents

Introduction

Information governance has had a relatively long history of making published court cases. The first cases, involving spoliation and similar matters, date from the mid-1800s. Spoliation is the intentional or negligent concealment, alteration or destruction of potential evidence to prevent an opponent in a legal action from gaining access to it. More recently, cases involving modern concepts such as records retention schedules first started showing up in the decided cases of the United States in the 1970s and 1980s.

The cases involving information governance have evolved over time. Where once the legitimacy of records retention schedules and similar matters were cutting-edge topics that frequently rose during litigation, the law surrounding them has since become settled, and today there is general acceptance of routine records and information management practices.

That is not to say that information governance has ceased to be of interest to the courts. To the contrary, what in the 1980s and 1990s was a relative trickle of cases has turned into a torrent. There are several reasons for this:

- Electronic records systems and increasing density of data storage have created a host of novel issues regarding discovery and litigation;
- Courts unsophisticated in both records and information management and electronic data systems have often struggled with how to deal with this new world of massive and fluid data sets;
- Although the law in this area has become somewhat settled, at least insofar as what constitutes reasonable practice, the ever-evolving ways data is captured and stored make this a continuing area of interest;
- As data became more distributed, both within a given system and amongst interlinked systems, ownership of data and its associated rights have become increasingly attenuated. This creates novel situations, both in discovery and in other areas, that the courts must address;
- The sheer size of data sets – so-called Big Data – creates an assortment of novel issues ranging from discovery to privacy to data security, to basic management and operation

functions which increasingly wind up in court. Another is navigating uncharted territory, both legally and operationally.

As a group, these cases are of significant value to anyone whose job it is to deal with information governance, whether as a governance professional, an IT practitioner, a lawyer or anyone else whose job involves records and information management. Cases typically involve new concepts, new technologies, new methods or novel situations that have not been thoroughly dealt with in the past. Anyone dealing with information governance as part of their job will likely deal with each of these points in the course of their work. And in so doing, they will inevitably confront the same issues that challenge the courts when these issues are presented to them. Court cases therefore offer guidance in several ways:

- They call attention to situations and issues which have not been thoroughly decided from a legal standpoint – that is why they are in court;
- They present opposing theories for analysis as to what constitutes acceptable or good practice;
- They offer an increasingly reasoned and informed analysis by the court of the opposing viewpoints;
- In the court's decision, the reader is guided as to what at least one court believes to be acceptable or good practice, and that court's legal justification for its decision;
- The loser's perspective is equally instructive as a course of action to be avoided, knowing that at least one court disapproved, with other courts likely to take that opinion as precedent.

The complexity of information governance in the 21st century is such that case decisions involving records and information management span a wide panoply of topics, far too many to cover a monograph of this length. Therefore, four topics likely to be of wide interest to information management professionals have been chosen. They are:

1. Data Breaches and Liability – Who owns data collected in cloud-based systems? Who has standing to litigate when breaches occur?
2. E-discovery – What constitutes ownership, custody and control of records and data, particularly as the lines blur between personal and business devices, and data

distributed amongst systems is shared by business partners, contractors, vendor and others?

3. Records and information policies and procedures – how do the courts view them; how do these policies and procedures operate in litigation?
4. Data rights – What rights does an organization have to data that it receives/collects from clients and other third parties?

The collection of cases in this monograph is a small sample of decided cases, which number in the thousands. However, the facts and laws of each case herein are of interest because they either contain novel or interesting facts, or they illustrate an important point of law.

Custody, Ownership and Control

Information collection and assimilation have become increasingly decentralized and distributed by technology advances. Email, both business and personal mobile devices, cloud-based storage and collaboration, the proliferation of third-party information vendors of all sorts, and our increasing willingness to share data with a variety of parties via all these channels increases the complexity of this issue. This cascade of information shared amongst devices and platforms has created novel legal issues of ownership, custody and control, and, indeed, of what constitutes a record.

The Broadening Concepts of Both Ownership and Records

Such issues are illustrated in *PhoneDog v. Kravitz*,[1] a case illustrating both the evolving nature of records themselves, and the complexity and novelty of the legal issues arising from that evolution. In *PhoneDog*, plaintiff PhoneDog sued the defendant over ownership and control of a Twitter account with 17,000 followers, used by the defendant for selling communications services. As is common in such cases, the defendant set up the account in his own name, and there was never a formal agreement between the parties as to ownership, custody and control of the account, its associated list of usernames for followers, and the communications made on it.

The defendant appears to have changed employers and commenced using the Twitter account on behalf of his new employers. The plaintiff then sued, alleging an assortment of improper behavior based upon the following legal theories:

- The Twitter account itself was commercial property subject to ownership claim by the plaintiff;
- Usernames and communications on the account were likewise property subject to an ownership claim, and in addition were a kind of trade secret;
- The course of dealing between the two parties was such as to negate the fact that the account had been opened in the defendant's personal name; and
- The course of dealing between the two parties had the effect of negating Twitter's terms of service, which had been agreed upon by the defendant upon opening the account, and which expressly provided that the account and the information in it were Twitter's property.

The case appears to have been settled prior to going to judgment, as it disappears from the record after some initial hearings. However, it is noteworthy that the Court accepted the plaintiff's legal theories to the extent that several of its stated claims survived motions to dismiss. Clearly, the Court concluded that the Twitter account had enough of the significant characteristics of property to justify the case proceeding past a motion to dismiss and into trial on the merits.

In re CTLI, LLC[2], the Court addressed a similar set of questions. In that case, the question at issue was ownership of a Facebook account related to a firearms store and firing range. In a bankruptcy proceeding, the Court determined that page was the property of the reorganized business, not the former owner, based upon the following factors:

- The page category was "businesses, brands and organizations," not individual;
- The page linked directly to the business's web site;
- Many or most of the posts on the page related directly to the business;
- Other employees of the business also made business-related posts on the site; and
- The page was named after the business.

The fact that the former owner personally opened the page and sometimes made personal posts on it was insufficient to overcome the presumptions of the other factors.

These cases and others[3] illustrate the judicial recognition that, as social media continues to gain prominence as business tools, they acquire the characteristics of business property, with the many downstream consequences that flow from that. And, given the informal and ad hoc way in which both employers and employees create such accounts, custody and control disputes are likely to continue to arise. Businesses are well advised to have a clear policy concerning ownership and control of such accounts when they are used for business activities. Perhaps more importantly, they illustrate the following:

- The data in these accounts are stored in third-party systems in unknown locations, and are probably subject to a user agreement created by that third party, but nonetheless the courts are willing to ascribe ownership and control to one of the parties, and to grant them property rights accordingly; and
- The data itself is considered by the courts to be discrete, tangible and valuable property subject to the judicial process not involving the third-party vendor.

As we will see, these concepts have far-reaching implications for electronic data and the organizations that use it.

Custody and Control of Information Held by Third Parties

As cloud-based computer systems and data storage become predominant, an increasing percentage of our data is being held by third-party custodians of many sorts. They may be merely vendors of storage space – the electronic equivalent of commercial records box storage vendors – but they may also be many other things, including the parties that design, operate and control the software, and the parties that do most or all of the significant processing of data collected on behalf of others. The legal relationship between these parties and the data that they possess on behalf of others is therefore increasingly important.

Custody and control may depend upon legal requirements specifically addressing the situation at hand. A long line of cases[4] stands for the proposition that information such as email content, text

messages, photos and other data objects in the possession of a telecommunications provider as part of its provision of telecommunications services is protected from unauthorized access by the Stored Communications Act,[5] meaning that a subpoena, warrant or other legal process is required for a third party to obtain access to it. But what about the copies of those same data objects that reside in the customer's cell phone? Are they too covered by the Stored Communications Act (SCA)?

The Court in *Garcia v. City of Laredo*[6] considered this question. The plaintiff had been discharged by her employer for violation of various policies. Evidence of the violation was obtained by removing a cell phone from an unlocked locker and examining its contents without the plaintiff's permission. The plaintiff argued that this conduct violated the SCA and was therefore improper.

The Court disagreed. In examining the language of the SCA, it concluded that by its terms, the SCA protected only information in possession of the telecommunications provider as part of its provision of services, and that the protection did not extend to a cell phone or other device used by the customer to access those services. Thus, while attempting unauthorized access to the provider's copy of the data is a criminal offense, the copies of the same data objects in the customer's cell phone have no legal protection whatsoever under the terms of the SCA:[7]

> An individual's personal cell phone does not provide an electronic communication service just because the device enables use of electronic communication services, and there is no evidence here that the Defendants ever obtained any information from the cellular company or network. Accordingly, the text messages and photos stored on Garcia's phone are not in "electronic storage" as defined by the SCA and are thus outside the scope of the statute.

It is equally clear, however, that via appropriate legal process, data objects – including electronic data – in the possession of third parties are subject to discovery as any other records and data relevant to a legal matter.

In *EEOC v. Original Honeybaked Ham,*[8] the Court viewed the matter as one of practical control and availability, not of legal ownership. The precise conditions of storage or location were

reviewed by the Court as essentially irrelevant. In this case, the Equal Employment Opportunity Commission (EEOC) brought a class action against the defendant, and the defendant sought discovery of a wide range of personal information from the members of the class, much of which was contained on social media pages and in text messages. The EEOC objected to production of this information, based on a theory that the relationship of the data to the lawsuit was too attenuated. The attenuation was twofold: (1) The data was personal data of the individual members of the class, not the named plaintiff; and, (2) In many of the cases the data was in accounts on Facebook and other social media sites. The Court rejected this, and instead conceptualized these accounts as being a folder belonging to the class members, containing information about them potentially relevant to the lawsuit. In concluding that this information is discoverable, the Court said:

> If there are documents in this folder that contain information that is relevant or may lead to the discovery of admissible evidence relating to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.[9]

The question of control has other variations as well. Today's business relationships are complex, and the use of modern information technology and communications devices leaves records and data in a variety of locations, under at least the nominal control of different parties. Therefore, the resolution of the question of whether or not a party controls a data set will often depend on the particular facts of the case.

In Ronnie Van Zant, Inc. v. Pyle,[10] the question was whether the defendants should be sanctioned for spoliation of evidence for failure to produce text messages that were resident on the mobile phone of an independent contractor who had done work for the defendants. The contractor was a nonparty and was not an employee of the defendant.

The Court concluded that sanctions were warranted. Citing Rule 37 of the Federal Rules of Civil Procedure, the Court determined that the defendants had failed to preserve electronically stored information. The Court found that the contractor's messages were effectively under the defendants' control because of the contract relationship, and because the contractor had a financial interest in a movie production that was part of the underlying series of transactions.

The Court in *Golden Trade v. Lee Apparel Co*.[11] reached a similar but broader conclusion about information in the hands of third parties. In this case, the issue was a patent infringement. Plaintiff resisted discovery of patent prosecution files held by a sub-licensor of the patent, arguing that the sub-licensor was a different legal entity and that, therefore, files in its possession were not in the custody and control of the plaintiff. The Court rejected this argument citing the cooperative arrangement between the parties in concluding that production could be compelled under Federal Rules of Evidence Rule 34 if the party had the practical ability to obtain the documents, regardless of any legal entitlement to them.

Other courts have concluded differently. In *Hatfill v. New York Times*,[12] the plaintiff sought discovery of a nonparty reporter's notes (the reporter was employed by the paper, but was not a party to the lawsuit) on a flash drive owned by and in possession of the reporter. The plaintiff asserted the same doctrine cited in the above cases, that the reporter was an employee or agent of *The Times*, and it could simply order the reporter to turn the material over, on pain of dismissal.

The Court disagreed, citing: the newspaper's long-standing policy of ceding ownership of reporters' notes to the reporters; a collective bargaining agreement between the newspaper and its reporters, embodying the same policy; and the newspaper's records retention policy. In the Court's view, a Rule 34 analysis concluded that the newspaper did not have the ability to compel the reporter to produce the notes.

The Broadening Definition of Recorded Information

A somewhat different scenario played out in *Columbia Pictures Indus. v. Bunnell*.[13] The data in question in this case was server logs held on servers owned and controlled by a third-party contractor. Although the logs were in the custody and control of the contractor, the same information was held temporarily in the random access memory (RAM) of the defendant's server.

The plaintiff argued that the logs were in the custody and control of the contractor, and that requiring it to turn on its own logging function would require it to create *new* records for discovery, something not required by the Rules of Civil Procedures.

The Court disagreed. Citing prior cases,[14] the Court concluded that the temporary storage of the log data in the RAM of the defendant's computer "fixed" the data in a tangible medium and as such classified it as electronically stored information under the terms of Rule 34(a) of the Federal Rules of Civil Procedure, making it fully discoverable. And, since the defendants had the ability to control how the information was routed (from their server to a log, or from their server to the contractor's server), it was in their custody and control.[15] The Court then ordered the defendant to turn on the logging function of its computers for purposes of collecting the data for discovery.

Courts considering the same questions in the context of federal agencies have reached similar conclusions. In *Burka v. United States,*[16] the Court considered custody and control in the context of a freedom of information request for data tapes created by a third-party organization contracting with the Department of Health and Human Services, applying the relevant two-part legal test:

- The agency must create or obtain the records; and
- The agency must be in control of the records at the time of the Freedom of Information Act (FOIA) request.

The Court concluded that the extensive level of supervision and control exercised by the agency over the collection and analysis of the data rendered the tapes agency records. The Court restated a four-part analysis[17] to determine custody and control:

(1) The intent of the document's creator to retain or relinquish control over the records;
(2) The ability of the agency to use and dispose of the records as it sees fit;
(3) The extent to which agency personnel have read or relied upon the documents; and
(4) The degree to which the documents were integrated into the agency's record system or files.

The Court further noted that the burden was on the agency to disprove custody and control, not on the requestor to prove it.

The Effect of Foreign Law

As commerce and business relations become globalized, and with the increasingly global reach of information systems, the applicability of foreign law is becoming increasingly important.

In *Tiffany (NJ) LLC v. Qi Andrew,*[18] the Court considered custody and control in the context of customer information in bank accounts for China-domiciled banks. Subpoenas were served on the United States branches of these banks, but branches stated that the data was contained solely in the Chinese branches, claiming the branches did not share computer systems or data, and that Chinese banking privacy law prohibited them from obtaining the information. After reciting the standard formulation of control ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action"), the Court considered the effect of Chinese banking law in light of the "comity[19] analysis"[20], which weighs several factors in determining the relevance of the information, including its nexus to the United States and the availability of other means of obtaining the information.

After analyzing relevant factors and governing Chinese law and doctrine, the Court declined to order production and instead directed the plaintiffs to seek discovery directly from the Chinese branches via the Hague Convention on Evidence, an international treaty governing international discovery. The plaintiffs were given leave to re-apply for a motion to produce the information should that avenue prove unproductive.

It is noteworthy that the Court's decision is heavily dependent on the interplay of a number of factors, both facts specific to the situation and legal provisions relevant to the case. In *Gucci America, Inc. v. Curveal Fashion,*[21] the Court was faced with nearly identical facts, but with a Malaysian banking law that limited disclosures to third parties only to cases of garnishment and only pursuant to a Malaysian court order. The Court concluded that the plaintiff's only remedy in this case was to either attempt to have a United States judgment registered in Malaysia, or to initiate an action in Malaysia and obtain a judgment there. No United States remedy was available.

Cases such as these are increasingly relevant to organizations of all kinds and sizes. The number and variety of laws restricting the location and/or transfer of information to other jurisdictions is substantial and increasing over time. Any organization that transacts business internationally, whether through third-party systems or internally on its own systems, may discover that location and restriction laws have the potential to cause significant complications in litigation.

Conclusion

These cases illustrate the reality of records and information management and its treatment by courts in the 21st century:

- The concepts of "stored information", "document"," record", and similar concepts which once referred to discrete paper objects and then to electronic analogues of them such as word processing or PDF documents, have been significantly broadened to include an increasingly wide array of data objects, extending even to information held in computer RAM;
- The concept of custody and control is likewise being increasingly broadened to include the above array of data objects held by a variety of parties in a variety of circumstances. So long as sufficient nexus between the party in the lawsuit and the third party in actual control of the records is there, a court can find custody and control sufficient to trigger a duty to protect and produce;[22]
- The question of custody and control in a given situation is a complex determination, fact-dependent upon a variety of factors, including the relationship and course of dealing between the parties and specific laws and legal requirements that may apply, including foreign law. However, courts tend to be liberal in so determining, and parties may expect increasingly broad doctrines going forward;
- The most basic of concepts – who owns a record or other data object – is itself becoming increasingly complex and unclear, as parties gather, manage and store information in systems and relationships not contemplated by traditional legal concepts and not governed by traditional legal doctrine.

All these considerations should give any organization pause. The circumstances described in the cases above are commonplace in today's business environment. Organizations involved in

litigation may well find themselves facing circumstances very similar to these parties, and if so, the attendant costs and potential adverse outcomes will be real possibilities. Anticipating them and developing the appropriate management and governance for both internal information systems and those of business partners, contractors and other third parties prior to being involved in litigation, are key to avoiding what can often be very costly difficulties if litigation does arise.

Data Breaches and Liability

The potential for data breaches[23] has become an increasing concern for any organization that maintains valuable information of any kind, from personal financial information to trade secrets. As they become more common, we can lose sight of the fact that large-scale data breaches are a relatively new phenomenon. And, because case decisions do not begin appearing until at least a few years after an issue gains legal traction, case decisions involving breaches are likewise quite new, and were rare until about 2012, a scant six years before this writing. As a result, the decided cases share some characteristics worth noting:

- any decided cases concern preliminary legal maneuvering – motions to dismiss, motions to certify class actions and so on; and
- Particularly for earlier decisions, there may not be a great deal of breach-specific precedent to go on.

A further issue that limits analysis is the reality that large-scale data breach cases usually settle before trial, thereby depriving legal researchers of definitive rulings on many points of interest.

Breach cases themselves often present other novel legal situations for several reasons:

- The types of data lost or stolen varies widely from breach to breach;
- The data volumes lost, and the resulting number of individuals that may be impacted, is immense, with a breach sometimes affecting hundreds of millions of individuals;
- The relationships between the party whose systems were breached and the persons whose data was compromised is quite diverse; and
- The damage to any individual may be uncertain or speculative.

Consider *Leibovic v. United Shore Mortg.*,[24] a class action case involving a data breach in which personal information provided to a mortgage broker for purposes of obtaining a mortgage was stolen. The information was collected and stored electronically by a third-party service provider on behalf of the mortgage company.

The service provider moved to dismiss the complaint, arguing that they owed no duty of care to the plaintiffs. The arguments made by the parties required the court to consider the nature and legal status of the defendant Xerox Mortgage Services, Inc. (XMS)'s custody of the data, to determine if at least the plaintiffs' claims could survive an initial motion to dismiss. The plaintiffs argued the following legal theories of liability:

- Breach of contract: Although the plaintiffs had no contractual relationship with XMS, the mortgage broker did, and that contract obligated XMS to use reasonable commercial care in collecting and managing the data. Plaintiffs argued that they were third-party beneficiaries of that contract; XMS argued that they were not. Citing prior cases (and a split of opinion in the appellate courts), the Court concluded that the plaintiffs could state a claim for breach of contract, reasoning that contrary cases involved contracts that explicitly excluded third-party beneficiary claims. In this case, the contract was silent on that point, thereby introducing at least a contemplation of third-party beneficiaries on the part of the contracting parties. Based on that reasoning, the Court also allowed claims for negligence and "negligent performance of an undertaking" to go forward.
- Bailment (the transfer of property to another for safekeeping): Plaintiffs argued that possession of the information was a bailment, and that XMS breached its duties to safely maintain the information and to either return or account for the information at the end of the bailment. The Court rejected this claim, reasoning that the plaintiffs provided no factual basis for the argument that they had an expectation that the information would be returned or accounted for at the end of the transaction for which they provided it.
- Unjust enrichment:[25] The Court observed that in order to prevail on a claim of unjust enrichment the plaintiffs must show: (1) the receipt of a benefit by XMS from them;

> and (2) an inequity resulting to them because of the retention of the benefit by XMS. And, previous cases required that there be direct contact between the two parties as well. In this case, there was no direct contact between the parties to the claim and, as such, the claim failed on that basis alone. In addition, the plaintiffs would have had a difficult time proving the two elements of the claim as well.

This opinion is a preliminary ruling in a case that is still active, and only decided whether the plaintiff's claims were strong enough to proceed to trial. But it provides insight into the new and unsettled nature of the legal landscape in respect of data breaches:

- The plaintiffs' rights and available redress were contingent upon the specifics of the language *of a contract they were not a party to*;
- The plaintiffs' rights and available redress were likewise contingent upon the Court's decision on which of two states' case law was applicable; and
- The plaintiffs' rights and available redress were also contingent upon the Court's decision as to which of two competing lines of cases (with different and mutually exclusive holdings) it would choose to follow.

The underlying facts the Court considered are very common:

- The transaction between the individual and the business;
- The third-party vendor in possession of personal information collected for the business as part of that transaction;
- No consent – and perhaps no knowledge – by the consumer that the third party was in possession of the information; and
- A controlling contract for which the individuals were not a party and whose terms and conditions were unknown to the individuals.

These factors, and the fact that they are commonplace, places many parties in many situations on uncertain legal footing. Given the right set of circumstances, these plaintiffs might have found themselves with no right of action at all against the third party whose system was breached (although they would still possibly have a right of action against the business that was their counterpart in the transaction). Given another set of circumstances, the vendor would have found

itself faced with stronger claims by the plaintiffs. So for all parties, the case demonstrates that awareness of the legal underpinnings of data collection is critical to understanding what rights and liabilities may be implicated by a data breach.

Another case illustrating the unsettled state of the law is *In re Target Corp. Customer Data Breach Litig*.[26] This too was a class action suit over a data breach involving customer financial data, and, again, Target sought to have some or all the claims dismissed. And as with *Leibovic v. United Shore Mortg.,* the Court's ruling was dependent upon the specifics of state law and some specific facts being alleged. Thus:

- Suit could be brought as a class action only for some states, because in many states class actions are precluded by consumer protection statutes;
- Claims that Target failed to notify consumers of the data breach were likewise precluded in many states because breach notification statutes in those states vested enforcement authority exclusively in a state official.

In reviewing these and other claims, arguments and counter-arguments, the Court analyzed dozens of state statutes, often without the benefit of much prior case law to guide it.[27] This is illustrative of this class of cases – they are a relatively new phenomenon, often with a lack of prior authority to guide the courts.

In many cases, even though the individual may not have suffered immediate harm from a data breach, the risk of future identify theft and other prospective injuries are regarded by courts as an injury sufficient to bring suit,[28] even though the defendants typically claim that potential future damages are insufficient to give standing.[29] Courts have also recognized that the loss of value of personally identifiable information (PII)[30] is an injury sufficient to give standing to sue.[31] This is not universally true, however. Some courts have held that such prospective injuries do not give rise to a state cause of action.[32]

A Comparison to the European Union

A data breach that occurs in the United States stands in substantial contrast to that of the European Union and other countries. Substantive law in the European Union provides

unequivocally that personal data is the property of the individual to whom it relates,[33] regardless of the relationship between that person and the custodian, and provides for joint and several liability[34] between the custodian and the party with whom the individual contracted or was in negotiations with.[35]

Conclusion

These and other cases illustrate the undeveloped and often contradictory state of the law as it concerns personal data in the possession of third-party providers and processors:

- The relationship between the individual and the processor is often undefined, leaving the courts to define it on a case-by-case basis. When it is defined, it is often dependent on the law of whatever state the judge determines to be controlling, making predictability challenging;
- The precise status and ownership of the data is likewise unsettled and uncertain, and dependent upon the vagaries of state law (much of which pre-dates and does not contemplate data breaches) and the case-by-case determinations of judges, again making proactive strategies based on predictability of outcomes difficult;
- Final conclusions are rare, since the cases invariably settle before trial, creating additional uncertainty; and
- As a result of all this ambiguity and uncertainty, the liabilities and available remedies of the parties are likewise uncertain.

In view of the continued and increasing use of third parties to collect, process and manage personal information on behalf of businesses, data breaches and liability are likely to become increasingly prominent and frequent, and a rationalization of the law to provide uniform and predictable outcomes is likely to take a number of years as case law develops and contradictions are resolved. In such cases, well-drafted contracts between all concerned parties from consumers through third-party data processors, and defining roles, rights and responsibilities, may alleviate some of this uncertainty and in the process reduce the cost and complexity of any disputes that may arise.

In a similar manner, data processors are well advised to consider the difference between United States law and European Union law. Data collection is often international in scope, and a strategy based on United States law is likely to fail when tested against European Union law.

Discovery[36] and Spoliation

Typically, a data breach involves a large-scale intrusion into a computer system. The state of that system and many of its components and artifacts is therefore highly relevant to a lawsuit alleging any negligence or breach of duty of care. In *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*,[37] the Court considered whether a party commits spoliation[38] by failing to preserve the entire system in its as-breached state (or a forensic mirror image of it). Although noting that doing so might indeed be useful, the Court denied a spoliation motion, reasoning that: (1) requiring such preservation is a rare remedy based on specific facts, and (2) to prevail on a spoliation claim the party seeking the sanction must establish "that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."[39] The Court concluded that mere failure to preserve the system in its breached state, and conclusory statements that some things that might have been useful had not been preserved, was insufficient to support a spoliation claim.

This outcome illustrates the changing attitude of the courts toward electronic data systems in the past 20 years. In the early days of electronic systems, it was routine to require companies in litigation to preserve or mirror entire systems, even if it involved an enormous expense to the litigant.

Other more recent cases – not necessarily concerning data breaches - are likewise illustrative of courts' increasing sophistication concerning electronic data systems and the nature of spoliation in them. *Victor Stanley, Inc. v. Creative Pipe, Inc*.[40] is representative. Here, the Court entered default judgment against the defendant in an intellectual property theft suit based on extensive spoliation of evidence by the defendant. As in *Auctioneers, Inc. v. EquipmentFacts,* the Court declined to order preservation of the entire system. However, discovery was conducted through normal means, over an extended period of several years. During this period, the defendant

engaged in a protracted, but poorly executed, campaign to delete an assortment of emails and other electronic data from various systems and repositories, including a business computer system, laptop computers, an email system, social media accounts, third-party email and other places. Only after repeated proven instances of spoliation on the part of the defendant was a mirror made.

In entering sanctions, the Court engaged in an extensive and knowledgeable discussion of electronically stored information, including:

- Discussion of email systems, procedures and deletion;
- Backup tape rotation;
- Disk defragmentation; and
- Drive wiping software.

The Court noted the continuing cost and complexity of electronic discovery, and the continuing lack of uniform national standards concerning it, stating:

> The lack of a national standard, or even a consensus among courts in different jurisdictions about what standards should govern preservation/spoliation issues, appears to have exacerbated this problem. It is not an exaggeration to say that many lawyers, as well as institutional, organizational, or governmental litigants, view preservation obligations as one of the greatest contributors to the cost of litigation being disproportionately expensive in cases where electronically stored information (ESI) will play an evidentiary role.[41]

The Court in *Victor Stanley, Inc. v. Creative Pipe* noted that different federal circuits have different standards with respect to a duty to preserve evidence, particularly ESI. Thus:

- In the Second and Fourth Circuits, documents are considered to be under a party's control when that party has the right, authority or practical ability to obtain the documents from a non-party to the action;[42]
- In the First, Fourth and Sixth Circuits, the preservation duty applies not only when the evidence is in the party's control; there is also a duty to notify the opposing party of evidence in the hands of third parties;[43]

- In the Third, Fifth and Ninth Circuits, a preservation duty exists only when the party controls the evidence, without extending that duty to evidence controlled by third parties.[44]

These competing standards create a challenge for large organizations, as the court in *Victor Stanley* observed. Having different e-discovery and preservation policies in different parts of the country is an impractical proposition, but at the same time, applying the most restrictive policies nationwide is costly. There appears to be no near-term solution for this issue.

Likewise, courts differ widely in interpreting the duty to impose and enforce a legal hold. Thus, while it is generally recognized that, once a preservation duty has arisen, an organization must suspend its records retention and disposition policy,[45] some courts consider that a legal hold – particularly a blanket hold – might not always be necessary depending on the circumstances, and that reasonableness is still a consideration.[46] And while some courts consider failure to implement a written legal hold as gross negligence with its attendant legal consequences,[47] other courts have concluded that failure to implement a legal hold is relevant conduct for the court's consideration, but is not sanctionable conduct.[48]

And, while courts have concluded that a party need not retain all backup copies or duplicates of relevant documents,[49] the split in authority among the circuit courts and in legal thinking continues to leave uncertainty as to whether all parties throughout the country can rely upon this doctrine.[50] Of course, whatever decisions a party makes, it will not know if they are correct until months later, when a court rules on them. And as with many issues, the relevant legal standard by which conduct is judged is vague and depends on determinations of "reasonableness" of conduct, whatever that may mean.[51]

Discovery in Distributed Systems

As data systems become more dispersed and diffuse, these issues have taken on increasing complexity. Nowhere is this more evident than in the proliferation of mobile devices, including laptops, cellular telephones and tablet devices in the business environment. Consider *In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig.,* a pharmaceutical product liability suit.[52] In

this case the defendant was sanctioned for discovery abuses, including, among other things, failure to produce text messages from employee mobile phones. In some cases, the messages were subject to automated deletion configurations in the system that were never changed. In other cases, there was a policy in place that affirmatively required employees to delete text messages. This, too, was not timely suspended.

The imposition of sanctions involved the construing of Rule 37(f) of the Federal Rules of Civil Procedure. That rule provides a safe harbor for loss of information due to the routine operation of an information system. The defendants argued that, although sanctions might be warranted in the case of failure to turn off an auto-delete function in an email system, sanctions for a similar failure in a text message system were unwarranted. The crux of their argument appeared to be that texting was a less important means of business communication; that production of text messages was excessively burdensome; and that, since there was a policy in place prohibiting the use of texting for substantive business purposes, any deletion of texts was essentially harmless. They also apparently made a blanket assertion, unsupported by rationale, that production of text messages was not required.

The Court rejected these arguments, observed that neither rules nor cases make a distinction between text messages and other forms of ESI, and that parties do not have the option to choose what evidence is appropriate for production. Texting was used for business purposes; therefore, it was relevant to the litigation and ought to have been preserved and produced.

The defendants also argued that some texting was done on personal phones of employees and could not be produced for that reason. In rejecting that argument as well, the Court ordered that any employee that refused to turn over texts from a personal device would be subject to a show cause order and would be required to appear in court personally to show why he or she should not be held in contempt of court.[53]

A similar series of arguments and a similar result were obtained in *Stinson v. City of New York*.[54] In this case, the City of New York was sued by a class of plaintiffs who alleged they had been issued summonses by the police without probable cause. The plaintiffs sought production of a

wide variety of communications, including memoranda, emails and text messages. The City failed to institute a legal hold until three years after the suit was filed, and then offered a series of arguments for failure to preserve or produce relevant documents:

- The City had a records retention policy that authorized the destruction of relevant documents after a comparatively short time;
- Because the City was the defendant in numerous lawsuits, imposing a legal hold for each would effectively result in a perpetual legal hold for all records, and that therefore the City ought not to be under a duty to impose a legal hold at all;
- The City had an email policy that limited the size of email inboxes, requiring employees to delete old email when the box became full;
- The City had no obligation to preserve text messages on employees' personal devices; and
- The police department did not use email for important communications.

The Court rejected all of these arguments, noting among other things, that the practices at issue in this case were also the subject matter of a separate lawsuit that was ongoing at the time this lawsuit was filed.[55] The Court concluded that there was no basis for concluding that the City acted in bad faith. However, the Court concluded that the City's actions amounted to gross negligence:

- The existence of a records retention schedule made the destruction of documents foreseeable;
- The existence of size limits on email inboxes likewise made the destruction of emails foreseeable;
- Regardless of any duty or lack thereof regarding employees' personal devices, the police department issued devices to some personnel, and had a duty to preserve ESI on those devices; and
- Failure to implement a legal hold within a reasonable time, resulting in destruction of relevant evidence, was a breach of the City's preservation obligations.

The Court then imposed the sanction of an adverse inference on the City.[56]

In *Sec. Alarm Fin. Enters., L.P. v. Alarm Prot. Tech.*,[57] the plaintiff likewise asserted the routine operation of a records retention schedule as a basis for avoiding sanctions for destruction of telephone call recordings relevant to issues at trial. The plaintiff argued that a legal hold had been issued, but that although it did not encompass the recordings, the hold constituted a reasonable effort to preserve evidence, and the destruction was therefore not sanctionable. The Court disagreed, first observing that, "It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances."[58] But the Court then concluded that a legal hold that did not encompass the recordings, which were central to the case, was not a reasonable effort to preserve evidence. A series of sanctions was then imposed.

Small v. Univ. Med. Ctr. of S. Nevada[59] resulted in sanctions from a number of issues that could easily have been the result of simple poor records management practice, and not of intentional misconduct by the defendant. They included:

- Failure to disclose the existence of and preserve documents stored in share drives;
- Failure to institute some preservation procedure for employee desktop computers on which information could be saved that was not saved to the central document management system;
- Failure to include laptop computers in preservation and discovery;
- Failure to preserve and produce information on departmental websites and cloud-based repositories;
- Failure to preserve and produce information from departmental sites on a company intranet;
- Failure to preserve and produce relevant email from employee mobile phones;
- Failure to preserve and produce information from a blackberry server and its associated devices; and
- Failure to adequately supervise a legal hold.

In many of these cases, automated processes were not suspended even after a duty to preserve arose, which allowed information to be deleted through routine and automated processes. Other instances may simply have been the result of inadequate search of a complex and highly

distributed data system with many repositories on many platforms, and with apparently no institutional knowledge about what contents might reside in the many nodes of this system. Nonetheless, as a result of these failures, the special master recommended the entry of default judgment against the defendant.

Another problematic area is the frequent replacement of devices. In *Shaffer v. Gaither,*[60] the plaintiff failed to preserve relevant text messages from a cell phone because it was damaged, and her insurance contract on the phone required her to turn in the damaged phone in order to receive a replacement. The Court concluded that, although a sanction was not yet warranted because the information from the texts was available from other sources, the plaintiff nonetheless had a duty to preserve the texts on the phone prior to turning it in for replacement.

Destruction of Personally Owned Information

A much different situation arose in *Rajaee v. Design Tech Homes*.[61] Here, the plaintiff worked for a home construction company and used a personal mobile phone for an assortment of his employer's business. He worked in this business for a number of years prior to this and had accumulated an assortment of business contacts and other valuable information related to his work, which was stored on the phone along with a quantity of personal information. When he was terminated, the employer remotely wiped the phone and restored it to its factory settings, destroying not only information related to his job, but also his personal and pre-existing business information. Along with a number of claims based in state law, he sued under the provisions of the Electronic Communications Privacy Act,[62] which provides that anyone who ""intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."[63] Citing *Garza v. City of Laredo*, the Court concluded that a mobile telephone is not a communications facility, and that this claim should be dismissed.

Plaintiff also asserted claims under the Computer Fraud and Abuse Act,[64] claiming economic losses in excess of $5,000, a necessary prerequisite to suit under the Act, based upon the loss of business contacts and personal data.

The defendants countered, and the court agreed that a "loss" under the terms of this act was limited to actual costs incurred in investigating and remediating the acts at issue, and to loss of service. Based upon this, the court dismissed this claim also.

This case, like many of the data loss cases cited in the sections above, is illustrative of the relative absence of remedies available to an individual in the case of loss of data. Controlling law, both statutory and case decisions, provides narrowly tailored causes of action in most cases, often leaving the individual with few or no remedies at law.

Conclusion

Management of electronic information – and with it, e-discovery – is an increasingly complex process. Information can be stored in a wide variety of places, formats and devices, and with many custodians, not all of them necessarily under the direct control of the party that is in court. All of these places and devices are potentially available for discovery, but many pitfalls await the careless or unwary. Sound system architecture, data maps, sound discovery strategies and well-drafted and rigorously implemented legal holds are all necessary to avoid those pitfalls. As the cases above illustrate, the legal landscape upon which an organization's actions will be judged is complex, and the outcome from a decision that has not been thoroughly thought through is uncertain.

Records and Information Management Policies

Records Retention Schedules

It has long been the case that courts accept the existence and validity of a records retention schedule and its associated implementation procedures as a legitimate tool for information management.[65] However, courts also have a long history of examining both the motives for implementing a records retention schedule and the details of its implementation. Similarly, recent cases have considered email and other records and information management policies, and, increasingly, how these policies are applied and constrained by the technology systems within which they must operate.

In *Micron v. Rambus,*[66] the Court considered the motives behind the adoption of a records retention schedule and activities associated with its implementation. The facts before the Court were relatively straightforward:

- Defendant Rambus had previously been involved in an industry consortium developing an open standard for chip circuitry;
- Rambus was actively engaged in development of a litigation strategy that involved suing other companies for patent infringement of computer chip circuitry; and
- Concurrently, Rambus was developing a records retention/disposition program, and actively engaging in cleanout days and other disposition activities.

Considered in the abstract, Rambus' document disposition activities were benign, industry-standard practices.[67] However, in conjunction with the above, Rambus:

- Held a series of board meetings featuring PowerPoint presentations discussing a "Nuclear Winter" litigation strategy; and
- The same presentations discussed document destruction activities, apparently discussed at the same time, by the board.

The timing of events – presentations about the "Nuclear Winter" contiguous with discussions of records destruction, and the development of the "nuclear winter strategy concurrently with the implementation of an aggressive records disposition program," allowed the Court to infer that the records disposition was a strategy by Rambus to destroy records in anticipation of litigation, and, as a result, the Court declared that the patents in question were unenforceable against the plaintiff. The same facts were used by Rambus' opponents with considerable success in a series of lawsuits over the same patents.[68]

Email and Backup Policies

In *In re Actos® (Pioglitazone) Prods. Liab. Litig.*,[69] the Court considered two distinct sets of questions regarding records retention: (1) The nature, effect and interaction of a series of records management policies; and (2) The ability of the party to implement them within its technology system.

Defendant Takeda Pharmaceuticals (Takeda) had in effect a number of standard records management policies and procedures, including backup tape policies, email management policies and a records retention policy. In a product liability lawsuit, Takeda claimed to have implemented a legal hold very early in litigation, and to have refreshed it periodically throughout the litigation. However, testimony in deposition and trial by Takeda's own employees, as well as extended discovery, elicited the following:

- Notwithstanding the existence of the legal hold, documents and records highly germane to the issues were deleted by employees per the regular records retention policy and in violation of the terms of the legal hold;
- Respecting backup tapes, Takeda took conflicting positions, both in policies and in trial testimony, as to whether backup and disaster recovery tapes were expected to be used as a document repository for purposes of litigation discovery;[70]
- Takeda's information technology systems were incapable of implementing the policies in any event; and
- Takeda compounded the above by hiding and obfuscating instances where it realized that errors and omissions had occurred, both by hiding facts and filing misleading legal pleadings.

In imposing a series of sanctions, including allowing an adverse inference instruction to the jury,[71] the judge rejected arguments by Takeda that its errors and omissions were made in good faith, and that the very large mass of documents produced was sufficient evidence of that good faith.

Application of Policies When a Legal Hold is Required

In *Larson v. Bank One Corp.*,[72] the Court considered the defendant's duty to preserve documents when the defendant asserted a document retention policy as a defense against production of documents. In this case, many key documents were simply not there, and the defendant claimed they were legitimately destroyed pursuant to a records retention schedule. However:

- Bank One's internal email indicated that neither of the two records retention schedules asserted as a defense had been properly adopted;

- The document retention policies[73] did not adequately address or apply a legal hold as of the date that the court concluded that Bank One was on notice of litigation; and
- There was little or no evidence that the relevant policies and procedures had been disseminated to employees.

The Court concluded that although Bank One had been engaged in "extraordinarily poor judgment" and "gross negligence," Bank One's conduct was not willful, intentional destruction of evidence. Therefore, the Court declined to enter a default judgment, but did recommend precluding Bank One from challenging the plaintiff's expert testimony on the subject matter related to the destroyed documents. In discussing Bank One's duty to preserve, the Court stated:

> As a large corporation, Bank One can only discharge its duty by: 1) creating a "comprehensive" document retention policy that will ensure that relevant documents are retained, and 2) disseminating that policy to its employees (citation omitted).[74]

Privilege and Undue Burden

When a party produces a records retention schedule, it cannot assert any sort of privilege or undue burden with respect to the production of records. In *Sharma v. BMW of N. Am. LLC,*[75] the defendants asserted irrelevance, delay by the plaintiffs and undue burden in resisting production of a records retention schedule. The Court rejected that assertion, noting that the records retention schedule itself would assist in determining the universe of relevant documents available to them, and that:

> The document retention policies they seek are contained within a modest number of pages, and in light of this, the burden or expense of producing this information is likely minimal, while the benefit of such information would be substantial.[76]

And, not only is an organization's current records retention schedule relevant, but past versions of it are likewise useful. In *Progressive Cas. Ins. Co. v. FDIC,*[77] the Court concluded that since the actions in question predated Progressive's current records retention schedule, past versions of it were relevant to help resolve possible issues of spoliation. On the other hand, at least one court has concluded that legal hold notices themselves are attorney-client communications and attorney work product, and are therefore privileged.[78]

Destruction of Records When a Hold is in Place

Document destruction pursuant to a records retention schedule, including after institution of a legal hold, is likewise often a topic of dispute. Destruction of records, even considerable quantities of them, after institution of a legal hold is not necessarily a sanctionable act, notwithstanding the *Rambus* decision. In *Medeva Pharma Suisse A.G. v. Roxane Labs., Inc,.*[79] the defendant destroyed considerable quantities of records after institution of a legal hold, including through means such as bulk office cleanout days and similar processes. The Court rejected spoliation claims by the plaintiff, noting that:

- The defendant's records retention schedule required preservation of the documents in question for very long periods of time, from 20 to 30 years;
- The defendant produced vast quantities of relevant documents; and
- Plaintiff's claims about destruction of documents were in many cases speculative, since they could establish only that a document did not exist, not that it had been destroyed.

Violation of Recordkeeping Laws

The question of regulatory compliance and records retention schedules is likewise a question that has arisen in recent years. In theory, a records retention schedule is supposed to state retention periods that comply with all applicable laws. But the number of potentially applicable laws could run into hundreds or thousands, and many are ambiguous or very general, leading to uncertainty. What if a law is missed and a retention period is not compliant with it as a result?

The Court in *Ramirez-Cruz v. Chipotle Servs*.[80] considered this question in the context of a spoliation motion. The defendant had destroyed certain employment records in conformance with its records retention schedule, but apparently in violation of certain federal regulations. In rejecting a request for spoliation sanctions, the Court concluded that there must be a finding of bad faith when documents are destroyed prior to litigation pursuant to a routine document retention policy. Good-faith routine destruction, even though inadvertently in violation of a law, is not enough to justify a spoliation sanction. Other courts in recent cases, including *EEOC. v Jetstream Ground Servs*.[81] and *Stevenson v. Union Pac. R.R.*[82] have reached similar conclusions.

Conversely, in *United States EEOC v. GMRI, Inc.,*[83] the defendant's records retention schedule required it to keep job applicant-related material for *longer* than the statutory minimums. Regardless, some paper records were destroyed due to confusion over the geographic scope of an EEOC investigation into the company. Nonetheless, the Court declined to impose sanctions on the defendant, and instead chose to let the parties argue to the jury about the relevance and contents of the missing documents, reasoning that:

- The EEOC's lack of clarity as to the scope of the investigation contributed to the issue;
- It was at least as likely as not that the missing documents would have helped, rather than hurt, the defendant;
- Existing documents and other evidence allowed the EEOC's case to proceed; and
- There was no evidence that the documents were destroyed in bad faith.

Incomplete Application of the Policy within the Organization

A different situation – one found in many organizations – occurred in *Scentsy, Inc. v. B.R. Chase*.[84] Here, a records retention policy and an email policy were in force at Scentsy, but were not applied to email and documents stored on the hard drives of individual computers and deleted only as and when the person whose computer it was saw fit. Compounding the issue was a very informal and poorly supervised legal hold instituted by Scentsy, and the crash of a computer hard drive which was not backed up and which potentially contained many relevant documents. Based on facts presented in depositions, the Court concluded that:

- The hard drive crashed well before litigation was reasonably anticipated;
- Since the retention policy did not apply to individual drives, there was very little likelihood that any relevant documents had been destroyed; and
- Many documents would in any event have been legitimately destroyed pursuant to the records retention schedule well before litigation was anticipated.

However, based upon the slight chance that some documents on individual drives might have been destroyed after litigation was foreseeable, the Court allowed depositions on this topic to determine if such destruction had actually occurred. The Court declined to authorize a forensic examination of all relevant machines as excessively burdensome and costly in the context of the case.

Conclusion

Courts are increasingly accepting of routine records management practices, including routine destruction of records, purging of email systems and other data destruction activities. This contrasts dramatically with the situation 20 or 30 years ago, when unsophisticated courts viewed any records or data disposition activity – even routine, automated operation of electronic systems – with great suspicion, often imposing draconian restrictions such as freezing entire systems, as well as severe sanctions for even inadvertent destruction or deletion of documents.

In like manner, courts have generally come to be relatively accepting and tolerant of inadvertent records and data destruction even when a legal hold was or should have been in place. Rather than the former relatively routine practice of imposing severe sanctions regardless of the facts or of the impact on the case, courts increasingly look to evidence of bad faith and intentional destruction to conceal evidence. And, when imposing sanctions, they are far more likely than formerly to try to balance the sanctions with the actual harm done.

Although courts have become more sophisticated in their approaches to information management issues, they do not provide blanket acceptance of anything that an organization may propound as good information management practices. Courts are increasingly examining records retention schedules and information governance policies and considering not only the objective reasonableness of those policies, but also examining how those policies are put into practice. Organizations should therefore consider the following:

- Are its policies drafted in a way that allows them to be applied with reasonable consistency throughout the organization and its information systems?
- Does it conduct training and awareness activities to ensure that personnel understand and comply with the policies?
- Does it have an effective system for timely creating and disseminating legal holds, including processes for applying them in distributed systems?

Attention to these three basic concepts is likely to prove highly valuable in the event of litigation. Good faith efforts to comply with legal duties, combined with objectively reasonable and achievable policies, are likely to go a long way with a court, even when results are imperfect.

Final Thoughts

If there is a common theme running through all the cases we have just reviewed, it is the uncertainty of the legal landscape within which records and information management resides in the 21st century. The uncertainty arises in two places:

The first is the reality of inadequate and outdated legal doctrine. Legal doctrines are old and evolve slowly. In contrast, information technologies and practices are advancing at a lightning pace. Legal doctrine and the processes by which it evolves – legislation and case decision – are by their very nature conservative and slow moving. Both courts and legislatures continue to grapple with these issues, and the law does indeed evolve to better address these issues. And as this process continues, both courts and legislatures themselves evolve, developing increased awareness and sophistication, so the laws and doctrines they promulgate will improve over time and provide more realistic and effective guidance. But there is little chance that they will ever fully catch up to the advancements in the information field. The facts on the ground simply move too swiftly.

This means that parties faced with compliance or litigation issues will inevitably face some uncertainty in planning and executing management strategies. It likewise means that courts facing these issues will face a similar uncertainty, and they still continue to respond as we have seen above, sometimes kicking the can down the road, sometimes crafting a very fact-specific remedy, and occasionally crafting a meaningful forward-looking doctrine that courts and litigants in the future will find of value.

The second area of uncertainty is the actions of the parties themselves, and here, information and legal professionals have a real opportunity to avoid at least some of the pitfalls we have seen. A common thread running through many of these cases is that the parties entered into an information sharing arrangement with no real understanding amongst them about rights and responsibilities, ownership and control. In many cases, it appears that these matters were given little or no thought at all until things went wrong. And as a result, the legal relationship between the parties and third-party beneficiaries, as evidenced by the contracts and other legal

arrangements amongst them, were silent. Combined with the absence of clear and clearly applicable law, the parties often found themselves in a legal vacuum, or subject to obscure and ill-defined case decisions that left them in a place far from where they had contemplated.

This is the place where information and legal professionals can assist themselves. Information sharing arrangements should be subject to policies and procedures, and when appropriate, contractual obligations that define roles, responsibilities, obligations and consequences. Policies and contracts are private law, and when properly constructed, are as enforceable as public law in the form of statutes and regulations. In many – perhaps most – of the cases above, had the parties entered into a thoughtful and comprehensive agreement about information ownership, custody, control and protection, it is likely the case would never have gone to court, or if it had, it would have been resolved quickly and expeditiously.

That is the practical teaching of these cases: legal uncertainty need not mean practical and transactional uncertainty. You can indeed take the law into your own hands if you do so thoughtfully; and that self-made law can provide the certainty that public law currently cannot.

Endnotes

[1] *PhoneDog v. Kravitz*, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. 2011).
[2] *In re CTLI, LLC,* 528 B.R. 359, Case No. 14-33564 Chapter 11 (S.D. Texas 2015).
[3] See, e.g., *Eagle v. Morgan et al*, 11-4303 (E.D. Pa. 2011), where the employer took control of a Linkedin Account from a discharged employee.
[4] See, e.g., *United States v. Councilman*, 418 F.3d 67, 80-81 (1st Cir. 2005).
[5] 8 U.S.C. §§ 2701–2712 (1986).
[6] *Garcia v. City of Laredo*, 702 F.3d 788 (5th Cir. Dec. 12, 2012).
[7] See also*, In re iPhone Application Litig*., 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012), *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 2:11-cv-01073, 2012 WL 3862209, (S. D. Ohio Sept. 5, 2012).
[8]2013 U.S. Dist. LEXIS 26887 (D. Colo. Feb. 27, 2013).
[9]116 Fair Empl. Prac. Cas. (BNA) 743, 2012 U.S. Dist. LEXIS 160285, *4–5 (D. Colo. Nov. 7, 2012).
[10] *Ronnie Van Zant, Inc. v. Pyle*, 270 F. Supp. 3d 656, 2017 U.S. Dist. LEXIS 138039, 98 Fed. R. Serv. 3d (Callaghan) 719, 2017 WL 3721777.
[11] *Golden Trade v. Lee Apparel Co.*, 143 F.R.D. 514, 1992 U.S. Dist. LEXIS 12215.
[12] *Hatfill v. New York Times,* 242 F.R.D. 353 E. Dist. Va. 2006.
[13] *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364, 2007 WL 2080419.
[14] See, e.g., *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518-19 (9th Cir. 1993); *Apple Computer, Inc. v. Formula International, Inc.*, 594 F. Supp. 617, 622 (C.D. Cal. 1984).
[15] But see, *Ice Corp. v. Hamilton Sundstrand Corp.,* 245 F.R.D. 513, 2007 U.S. Dist. LEXIS 62261 (production by the party is not required if the requesting party can obtain the documents from another source).
[16] *Burka v. United States HHS*, 87 F.3d 508, 1996 U.S. App. LEXIS 15759, 318 U.S. App. D.C. 274, 34 Fed. R. Serv. 3d (Callaghan) 1347. *Tax Analysts v. Dep't of Justice*, 269 U.S. App. D.C. 315, 845 F.2d 1060, 1069 (D.C. Cir. 1988).
[17] *Burka,* 87 F.3d 508 at 515.
[18] *Tiffany (NJ) LLC v. Qi Andrew,* 276 F.R.D. 143, 2011 U.S. Dist. LEXIS 80677.
[19] Comity is the legal doctrine whereby one jurisdiction elects to give effect to the laws of another jurisdiction, not because it is required to do so, but as a matter of comity between the jusisdictions.
[20] For which see, e.g., *In re Maxwell Commc'n Corp*., 93 F.3d 1036, 1049 (2d Cir. 1996); see also *Strauss v. Credit Lyonnais, S.A.*, No. CV-06-0702 (CPS), 2006 U.S. Dist. LEXIS 72649, 2006 WL 2862704 at *18 (E.D.N.Y. Oct. 5, 2006); *Container Leasing Int'l, LLC v. Navicon,* S.A., No. CIV303V00101 (AWT), 2006 U.S. Dist. LEXIS 17547, 2006 WL 861012 at *6 (D. Conn. Mar. 31, 2006); *Alfadda v. Fenn,* 149 F.R.D. 28, 34 (S.D.N.Y. 1993).
[21] *Gucci America, Inc. v. Curveal Fashion*, 2010 U.S. Dist. LEXIS 20834, 2010 WL 808639.
[22] See, e.g., *Landry v. Swire Oilfield Servs., L.L.C.*, 323 F.R.D. 360, 2018 U.S. Dist. LEXIS 885, 99 Fed. R. Serv. 3d (Callaghan) 1191, 2018 WL 279749 (extensive discussion of the evolution of discovery and the role of ESI (electronically stored information) in the discovery process); *S2 Automation LLC v. Micron Tech., Inc.,* 2012 U.S. Dist. LEXIS 120097, 2012 WL 3656454 ("Courts will also find that documents are within a party's control when it has the practical ability to obtain the documents, particularly when the opposing party does not have the same practical ability to do so."); *Tomlinson v. El Paso Corp*., 245 F.R.D. 474, 2007 U.S. Dist. LEXIS 64783, 42 Employee Benefits Cas. (BNA) 1429 (data collected or maintained by a third party for a party is in the party's custody and control when the party has a legal duty to collect and maintain the information and the third party is maintaining it on their behalf).
[23] A data breach is an entry into a data system that results in the loss, unauthorized copying or unauthorized exposure of non-public data. A data breach is distinct from other data security incidents in that not all data security incidents result in the loss, unauthorized copying or unauthorized exposure of non-public data.
[24] *Leibovic v. United Shore Mortg.,* 2016 U.S. Dist. LEXIS 149584.
[25] Unjust enrichment is the receiving of a benefit to which you are not entitled, or for which you have not paid proper compensation.
[26] *In re Target Corp. Customer Data Sec. Breach Litig.,* 66 F. Supp. 3d 1154 (D. Minn, 2014).
[27] See, *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig*., 613 F. Supp. 2d 108, 2009 U.S. Dist. LEXIS 41300 (A jury could conclude that data security was an implied contract term of a grocery purchase; under Maine law, there is no implied warranty of fitness for a credit card payment system; under Maine law there is no duty to notify consumers of a data breach).

[28] See, e.g., *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.,* 2017 U.S. Dist. LEXIS 140212.
[29] *Remijas v. Neiman Marcus Grp*., LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur.").
[30] Personally Identifiable Information is any data about an individual human being that relates to them in a manner to traceable back to them. It includes demographic information, medical information, financial information, biometric information anything else about the or their lives.
[31] See, e.g., *In re Anthem, Inc. Data Breach Litigation* ("Anthem II"), 2016 U.S. Dist. LEXIS 70594, 2016 WL 3029783 (N.D. Cal. May 27, 2016); *In re Facebook Privacy Litigation,* 572 F. App'x 494 (9th Cir. 2014); *Svenson v. Google, Inc*., 2015 U.S. Dist. LEXIS 43902, 2015 WL 1503429 (N.D. Cal. Apr. 1, 2015).
[32] *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* 903 F. Supp. 2d 942, 2012 U.S. Dist. LEXIS 146971, 2012 WL 4849054; *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig*., 45 F. Supp. 3d 14, 2014 U.S. Dist. LEXIS 64125 (Neither prospective future damages from theft of PII nor actual costs such as the costs of remediation measures such as credit monitoring were sufficient to give standing.).
[33] See *European Union General Data Privacy Regulation* (Regulation (EU) 2016/679) (EU-GDPR), Arts. 12-15.
[34] Joint and several liability is a form of legal responsibility whereby, if more than one party is liable for injuries to another, each party is liable for 100% of the damages. So if one or more of the liable parties cannot contribute their share, the others are responsible for it.
[35] See EU-GDPR Arts. 24-31.
[36] Discovery is the process in a lawsuit whereby the parties are obligated to search their records systems and other places for purposes of giving the opposing party access to records, information and other artifacts that may be relevant to the case.
[37] *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 2013 U.S. Dist. LEXIS 69734, 2013 WL 2151779.
[38] Spoliation is the intentional or negligent concealment, alteration or destruction of potential evidence to prevent an opponent in a legal action from gaining access to it.
[39] *Id* at 4.
[40] *Victor Stanley, Inc. v. Creative Pipe, Inc.,* 269 F.R.D. 497, 2010 U.S. Dist. LEXIS 93644 (D. Maryland 2010).
[41] *Id*. at 517.
[42] *In re NTL, Inc. Sec. Litig.,* 244 F.R.D. 179, 195 (S.D.N.Y. 2007), *Goodman v. Praxair Servs*., 632 F. Supp. 2d 494, 2009 U.S. Dist. LEXIS 58263 (D. Maryland 2009), *Alter v. Rocky Point Sch. Dist*., No. 13 Civ. 1100, 2014 U.S. Dist. LEXIS 141020, 2014 WL 4966119 (E.D.N.Y. Sept. 30, 2014).
[43] *Silvestri v. GMC* , 271 F.3d 583 (4th Cir. 2001); *Velez v. Marriott PR Mgmt., Inc.*, 590 F. Supp. 2d 235 (D.P.R. 2008); *Jain v. Memphis Shelby County Airport Auth*., No. 08-2119-STA-dkv, 2010 U.S. Dist. LEXIS 16842, 2010 WL 711328, at *2 (W.D. Tenn. Feb. 25, 2010).
[44] *Bensel v. Allied Pilots Ass'n*, 263 F.R.D. 150, 152 (D.N.J. 2009); *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S. D. Texas 2010); *Melendres v. Arpaio*, 2010 U.S. Dist. LEXIS 20311, 2010 WL 582189 D. Arizona 2010), *Cotton v. Costco Wholesale Corp*., No. 12-2731, 2013 U.S. Dist. LEXIS 103369, 2013 WL 3819974 (D. Kan. July 24, 2013).
[45] *Goodman v. Praxair Servs.* , supra, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212.
[46] *Jones v. Bremen High Sch. Dist.* 228, 2010 U.S. Dist. LEXIS 51312.
[47] *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec.,* LLC, 685 F. Supp. 2d 456.
[48] *Haynes v. Dart,* No. 08 C 4834, 2010 U.S. Dist. LEXIS 1901, 2010 WL 140387(N.D. Ill. Jan. 11, 2010).
[49] See, *Zubulake v. UBS Warburg LLC,* supra, *Consol. Edison Co. of N.Y., Inc. v. United States*, 90 Fed. Cl. 228, 256 (Fed. Cl. 2009).
[50] See, Grimm et al, *37 U. Balt. L. Rev*. at 410 ("The general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and metadata.")
[51] See, *Jones v. Bremen High Sch. Dist., supra, Danis v. USN Commc'ns, Inc.,* No. 98 C 7482, 2000 U.S. Dist. LEXIS 16900, 2000 WL 1694325 (N.D. Ill. 2000) (A party's actions must be "'reasonably calculated to ensure that relevant materials will be preserved,' such as giving out specific criteria on what should or should not be saved for litigation.").
[52] *In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig.,* 2013 U.S. Dist. LEXIS 173674, 2013 WL 6486921.
[53] *Id. at 62*. See also, *Hosch v. Bae Sys. Info. Solutions, Inc.,* 2014 U.S. Dist. LEXIS 57398, 2014 WL 1681694 (party sanctioned for wiping mobile devices prior to making them available to opposing party for discovery).

[54] *Stinson v. City of New York,* 2016 U.S. Dist. LEXIS 868, 2016 WL 54684.
[55] *Floyd v. City of New York*, 283 F.R.D. 153, 164-66 (S.D.N.Y. 2012).
[56] But see *Newmark Realty Capital, Inc. v. BGC Partners, Inc.,* 2018 U.S. Dist. LEXIS 69936 (pursuant to a stipulation of the parties, the discovery order provided that "absent a showing of good cause, voicemails, mobile phones, and tablets are deemed not reasonably accessible and need not be searched or collected from in response to a discovery request."). *Merial Ltd. v. Velcera, Inc.*, 2012 U.S. Dist. LEXIS 105006 (M.D. Georgia).
[57] *Sec. Alarm Fin. Enters., L.P. v. Alarm Prot. Tech., LLC*, 2016 U.S. Dist. LEXIS 168311 (D. Alaska 2016).
[58] *Id*. at 9.
[59]*Small v. Univ. Med. Ctr. of S. Nev*., 2014 U.S. Dist. LEXIS 114406 (Dist. Nevada 2014).
[60] *Shaffer v. Gaither,* 2016 U.S. Dist. LEXIS 118225 (W.D. North Carolina (2016).
[61] *Rajaee v. Design Tech Homes, Ltd.,* 2014 U.S. Dist. LEXIS 159180.
[62] 18 U.S.C. 2701.
[63] Id. at 18 USC §2701(a)(1).
[64] 18 U.S.C. § 1030.
[65] See e.g., *Reish v. Pennsylvania State University*, 2011 U.S. Dist. LEXIS 55170, 2011 WL2015350(M.D. Pa. 2011) ("Defendants have made a substantial showing that no spoliation has occurred here, and that the document destruction that Reish claims took place either never occurred or was a function of routine document destruction policies."); *Fortune v. Bitner,* 2006 WL 839346 (M.D.Pa. 2006) ("No adverse inference can be drawn, therefore, from the mere fact of [a party's] inability to produce the records, absent evidence that they were intentionally concealed or destroyed").
[66] *Micron v. Rambus*, 255 F.R.D. (Dist. Delaware 2009).
[67] By way of full disclosure, this author was engaged by Rambus as an expert witness on records management in this and several related lawsuits.
[68] See, *Hynix Semiconductor, Inc. v. Rambus Inc.*, 591 F. Supp. 2d 1038 (N.D. California 2006), *Rambus, Inc. v. Infineon Techs.* AG, 220 F.R.D. 264, 2004 U.S. Dist. LEXIS 4577 (E. D. Virginia 2004), *Samsung Elecs. Co. v. Rambus Inc.*, 439 F. Supp. 2d 524, 2006 U.S. Dist. LEXIS 50007 (E.D. Virginia (2006), *Micron Technology, Inc. v. Rambus Inc.*, 645 F.3d 1311 (Fed. Cir. 2011).
[69] *In re Actos® (Pioglitazone) Prods. Liab. Litig.,* 2014 U.S. Dist. LEXIS 86101 (W.D. Louisiana (2014).
[70] Stating in policies that backup tapes were not to be relied upon for litigation discovery, but in testimony stating that its intent all along was to use them for just that purpose.
[71] In this case, an instruction that the jury could, *if it chose to*, find the destroyed and missing documents would have been adverse to Takeda.
[72] *Larson v. Bank One Corp*., 2005 U.S. Dist. LEXIS 42131 (N.D. Illinois 2005).
[73] Presumably, not only the records retention schedule, but also its supporting policies and procedures.
[74] *Larson* at *35.
[75] *Sharma v. BMW of N. Am. Llc*, 2016 U.S. Dist. LEXIS 34101, 2016 WL 1019668 (N.D. California 2016)
[76] *Id.* at *11. See also *Newman v. Borders, Inc.,* 257 F.R.D. 1 (D. D.C. 2009) ("That a party's document retention policies, including its policies as to electronically stored information, may be a fit subject of discovery cannot be gainsaid.").
[77] *Progressive Cas. Ins. Co. v. FDIC*, 298 F.R.D. 417 N.D. Iowa (2014).
[78] *PersonalWeb Techs., LLC v. Google Inc.,* 2014 U.S. Dist. LEXIS 116140 (N.D. California 2014).
[79] *Medeva Pharma Suisse A.G. v. Roxane Labs., Inc.,* 2011 U.S. Dist. LEXIS 8417 (D. New Jersey 2011).
[80] *Ramirez-Cruz v. Chipotle Servs.,* LLC, 2017 U.S. Dist. LEXIS 128149 (D. Minnesota 2017).
[81] *EEOC. v Jetstream Ground Servs.,* 2016 U.S. Dist. LEXIS 154109, 2016 WL 8201623 (D. Colo. Nov. 3, 2016).
[82] *Stevenson v. Union Pac. R.R*., 354 F.3d 739 (8th Cir. 2004).
[83] *United States EEOC v. GMRI, Inc.,* 2017 U.S. Dist. LEXIS 181011 S.D. Florida (2017).
[84] *Scentsy, Inc. v. B.R. Chase, L.L.C.,* 2012 U.S. Dist. LEXIS 143633 (D. Idaho 2012).

About the Author

John Montaña J.D., FIIM, FAI, is a principal of Montaña & Associates, an information governance consulting firm based in Denver Colorado. In this capacity he advises corporations, law firms and non-profit organizations on best practices and legal compliance in information systems of all types, including paper-based systems, unstructured document and data repositories and structured data systems.

His work has included analysis and advice on a wide variety of governance, compliance and management issues, including records retention scheduling, advice on the legality of various information storage media, regulatory compliance, litigation and discovery, risk mitigation and other matters likely to impact information governance and management considerations; as well as analysis, critique and modification of practices, policies and procedures, and retention schedules developed by others and start-to-finish development of records retention schedules and records management policies and procedures. He is widely recognized as one of the foremost records management experts in the US and abroad.

Mr. Montaña has published four books on records management issues, as well as dozens of articles for magazines and professional journals, and is an active seminar speaker on records management topics. He holds a Juris Doctor from the University of Denver.

The Foundation is a leading organization that enhances the practical and scholarly knowledge of information management by funding and promoting research, scholarship, and educational opportunities for information management professionals. The Foundation is a non-profit corporation with 501(c)3 tax exempt status in the United States.

Mission

Our mission is to fund and promote research, scholarship, and educational opportunities for the information management profession.

Purpose of Research

Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The Foundation's purpose is to answer that need by providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

Thank you to sponsor

The Foundation thanks the ARMA Metro New York City Chapter for the financial contributions made to support this research project.

If you wish to fund any future research projects, please contact admin@armaedfoundation.org or visit the Foundation website www.armaedfoundation.org.

Additional Foundation financial and program information can be found at:

The National Database of Non-profit Organizations
http://www.guidestar.org/organizations/31-1556655/arma-international-educational-foundation.aspx