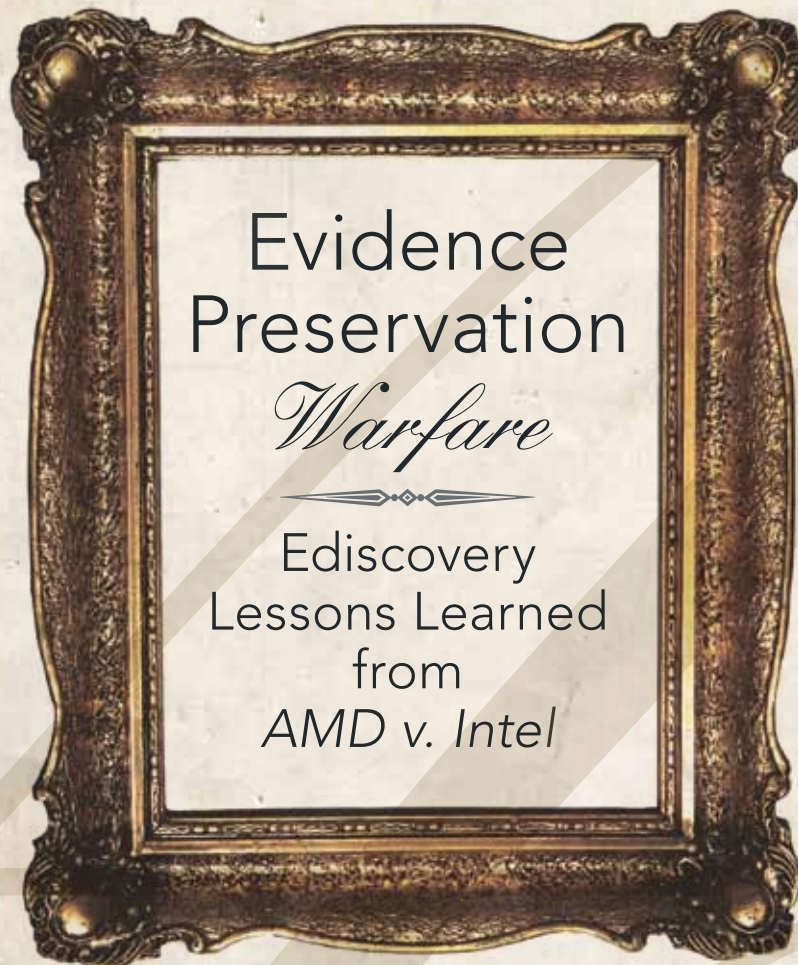




*Intel*



# Evidence Preservation

## *Warfare*

Ediscovery  
Lessons Learned  
from  
*AMD v. Intel*

BY ELIZABETH OZMUN,  
DAVID HERRON AND JAMES PEARL

Advanced Micro Devices, Inc. (AMD) and Intel Corporation (Intel) are the only major purveyors of x86 microprocessors, the “brains” of almost every computer in the world. Intel dwarfs AMD in size and market share in this industry, on which the productivity of virtually all business relies. In the early 2000s, AMD and Intel exchanged repeated allegations and denials about unlawful Intel monopolistic activities. Then in March 2005, the Japan Fair Trade Commission ruled that Intel had violated Japan’s antitrust laws. Four months later in June 2005, AMD sued Intel in federal court in Delaware, asserting civil claims under US antitrust laws.

What followed was massive, world-wide litigation that took five years to conclude. No one keeps precise records yet on this topic, but this case also likely became the largest ediscovery case in US civil litigation history: The equivalent of as many as 400 million pages of electronic documents changed hands, which, if printed out and laid end-to-end, would have stretched around the globe — *almost three times*; the parties collected terabytes of additional electronic data from every imaginable source in the United States and abroad to assess it for relevance; hundreds of employee-custodians from both companies were placed under long-term litigation holds; scores of contract attorneys spent years parsing through the collected data mass; and the evidentiary gems culled from this review were used in more than 300 depositions consuming more than 2,200 hours.

### What you should know about evidence preservation

The evidence preservation, collection and production challenges posed by *AMD v. Intel* were daunting, even unprecedented. Both sides grappled with the challenges and despite good-faith efforts by all, neither side was perfect. In retrospect, therefore, it is hardly surprising that this case spawned evidence preservation issues — and claims and counter-claims of evidence spoliation — that produced (some might say, devolved into) satellite, case-within-a-case litigation of the Brobdingnagian<sup>1</sup> scale. During it, a vast array of cutting-edge evidence preservation issues took turns under the bright lights of the ediscovery stage. Facing an evidence spoliation adverse inference jury instruction, on top of billions of dollars of potential antitrust damages, the stakes were chillingly high for Intel. Ultimately, the evidence preservation warfare that erupted was intense, withering and woefully expensive for both sides.

AMD and Intel settled their dispute in November 2009, less than five months before trial and just a matter of weeks before the decision on the AMD's then-pending motion asserting Intel's spoliation of evidence, and on Intel's competing "sanctions" motion.<sup>2</sup> The parties ultimately asked to dismiss these motions in recognition of the enormous scope and size of their document retention and productions, the inherent difficulties those undertakings imposed, and each side's good faith effort to remediate any losses that might have ensued. Of course, *AMD v. Intel* was not the first case to confront evidence preservation issues and will most certainly not be the last. Indeed,



ELIZABETH OZMUN is vice president, litigation and employment law at Advanced Micro Devices, Inc., where she oversees all worldwide AMD litigation and employment law issues. Ozmun managed the *AMD v. Intel* litigation, and spearheaded AMD's internal ediscovery effort and preservation program in that case.



DAVID HERRON is a partner in the Los Angeles office of O'Melveny & Myers LLP and is chair of the firm's Electronic Discovery and Document Retention Practice. He focuses on ediscovery-related litigation and counseling. Herron can be contacted at [dherron@omm.com](mailto:dherron@omm.com).



JAMES PEARL is a partner in the Century City office of O'Melveny & Myers LLP and a member of the firm's Business Trial and Litigation and Antitrust and Competition Practices. He focuses on antitrust, accounting, entertainment and general business litigation. Pearl can be contacted at [jpearl@omm.com](mailto:jpearl@omm.com).

case law is now replete with claims of purported preservation failures involving electronic evidence. It doesn't take a cynic to suspect that not all of these assertions are tethered to a genuine belief of actual preservation breakdown. Counsel for some litigants, it seems, will pounce on any perceived or even non-existent preservation deficiencies to run up costs or achieve another undue litigation advantage.

Anyone who has tried to design, implement and monitor an ironclad evidence program knows well that successfully achieving this goal can be challenging and expensive. The risk of possible failure is high and potentially case-altering. The costs of defending against charges of evidence preservation impropriety — that is, the cost of "discovery into discovery" — can be

phenomenal. Yet the law unquestionably places the burden of compliance squarely on corporate in-house counsel and their outside lawyers. And these tough economic times have squeezed litigation budgets microscopically thin, thus putting a premium on cost-effective, defensible evidence preservation measures that won't break the bank. Implementing an evidence preservation program correctly from the outset of litigation matters more now than ever before. We examine some of the evidence preservation issues that arose in litigation, and which corporate counsel may confront in almost any case. We don't pretend to have all the answers. But the trail of lessons learned in *AMD v. Intel* might offer guideposts to the wary and useful practice points for the in-house ediscovery practitioner.

### A brief history of *AMD v. Intel*

**The red telephone:** Those of a certain vintage will recall the Cold War-era "red telephone" that directly tied the White House and the Kremlin and was designed to avoid nuclear mishap. Every piece of big-case litigation has its red telephone equivalent, established between lead trial counsel of the warring factions. Although it is almost always email these days, the litigation red telephone is used only sparingly and, even then, only when situation-critical.

In February 2007, Intel's outside counsel, Robert Cooper of Gibson, Dunn & Crutcher, sent an email to AMD's lead trial lawyer, Chuck Diamond of O'Melveny & Myers. Intel had detected non-compliance with evidence preservation directives by a then-unknown, but apparently large, group of document custodians. The problems largely cen-

# THE RIGHT TECHNOLOGY FOR THE WRONG MARKET?



Innovation in itself is no guarantee of success. You need a market that's prepared to accept that innovation. At Foley Hoag, we can help you fit your technology to its proper market. We offer more than clear and sound legal advice. We offer strategic thinking that helps you realize every advantage. Learn more at [foleyhoag.com](http://foleyhoag.com).

BOSTON | WASHINGTON | EMERGING ENTERPRISE CENTER | [FOLEYHOAG.COM](http://FOLEYHOAG.COM)

*Attorney advertising. Prior results do not guarantee a similar outcome.*

tered on email retention and, as Intel would later disclose publicly, were exacerbated by the fact that Intel had neither disabled the “auto-delete” function on its email servers, nor implemented from case outset a thoroughly-comprehensive back-up tape retention system as a backstop against email loss. Days after there was more news: Intel had determined that, 20 months into the case, several hundred custodians (more than 375, as it turned out) had never received litigation hold notices. The issues were unfolding and dynamic, and the potential for evidence loss appeared real.

**Intel’s remediation plan:** Within months, Intel submitted a court-ordered “remediation plan” that outlined in general terms the apparent scope of data loss and what Intel intended to do about it. In the plan, Intel asserted that in the end, “nothing of any genuine significance will prove to have been lost.” AMD was skeptical. Intel had in fact preserved a “snapshot” of backup tapes made days after litigation began, and in November 2005 — five months after the case started — had begun to migrate some custodian email accounts to dedicated servers that were being backed up weekly. But the combination of Intel’s auto-delete function that purged certain email in as few as 24 hours, litigation hold notices of questionable comprehensiveness and Intel’s admitted overwriting of some backup tapes, prompted AMD suspicion of irremediable Intel evidence retention failures. Intel’s proposed solution was an expensive one. To its credit, Intel decided to gather all available backup tapes (essentially, the initial “snapshot” of its Exchange environment and weeklies of its dedicated email server); harvest additional data from as many as 1,000 Intel document custodians who were under litigation hold (not all of whom were required by the court’s document production order to actually produce documents); and create a vast “mush pot” of terabytes of electronic data that would be searched to find documents that a producing custodian should have kept but did not. This took more than a year to accomplish and, according to Intel’s public filings, some \$20 million to execute — although the true financial impact was surely much higher.

**AMD’s evidence preservation discovery:** The court monitored AMD’s discovery into Intel’s preservation failures and, at the parties’ urging, divided it into two phases. The first phase was deemed “Remediation Discovery,” and was intended to allow AMD to make a first-blush assessment of Intel’s apparent data loss, to respond preliminarily to Intel’s out-of-the-box assertion that no evidence of any value had been lost, and to comment on Intel’s proposed remediation plan. In response to that plan, AMD agreed that, in the circumstances, Intel had proposed to remediate its loss by the only reasonable means then available to it. Still, AMD asserted then — and later in its evidence spolia-

tion motion — that Intel in fact had expunged forever vast (albeit then-unknown) quantities of unique emails material to the litigation.

The second phase of court-sanctioned inquiry was called “Culpability Discovery,” and was intended to allow AMD to plumb Intel’s responsibility, and liability, for its evidence preservation failures. Intel said that its retention problems were the result of “human error,” the product of in-house counsel’s lapses in oversight and execution caused by the crush of other litigation activities. This assertion — and the fact that Intel’s in-house counsel helped design and implement Intel’s preservation program — made relevant what in-house counsel did and didn’t do, and when and why. This placed the attorney-client privilege and attorney work product at risk. Over the course of almost two years, Intel produced documents, yielded up its in-house counsel and IT personnel for depositions, and produced its external ediscovery vendors for both off-the-record interviews and video-taped depositions.

**Intel strikes back:** Even before it filed its own proposed remediation plan, Intel launched a searching inquiry into AMD’s preservation program. The preservation discovery that followed was as thorough and invasive as the court would permit. While the court dismissed some of Intel’s discovery as Intel simply “fishing for errors,” Intel successfully procured extensive AMD disclosures about its preservation program, document productions, numerous “informal” technical interviews with AMD IT staff and ediscovery vendors, and several depositions.

Intel’s preservation counter-attack settled on two central theories: First, Intel argued that although AMD had implemented company-wide preservation efforts four months before the case was filed, AMD had “reasonably anticipated litigation” even earlier and, thus, had not initiated preservation early enough; and, second, that select AMD custodians had themselves not saved all potentially relevant email in the time before AMD implemented an automatic email retention solution known as “journaling” in November 2005, some five months after the case was filed.

**Unknown outcomes:** In an attempt to resolve each other’s myriad evidence preservation complaints, both Intel and AMD made “remedial” document productions designed to cure actual or perceived preservation errors. But when the smoke of the long, costly and daunting preservation discovery battle cleared, neither side was satisfied; each filed a motion seeking evidence spoliation sanctions against the other. No one will ever know, however, how these motions would have turned out since the parties settled before the court had a chance to decide them. But we are left with some important lessons learned about defensible evidence preservation protocols and preservation pitfalls to be avoided.

## ACC Extras on... Evidence Preservation

### ACC Docket

- *Why My Human Document Reviewer Is Better than Your Algorithm (May 2010)*. Stop relying on document search technology and temporary agencies and take back control of ediscovery. Not only will this eight-step process reduce your costs, but as your review team becomes better informed, your litigation strategy will become more effective too. [www.acc.com/humandocrw\\_may10](http://www.acc.com/humandocrw_may10)
- *Effective Management of Litigation Holds and Ediscovery (May 2009)*. Two years after amendments to the FRCP became part of the discovery process, in-house counsel have adjusted. Read the answers and applicable best practices to these lingering questions relevant to your company's legal hold process. [www.acc.com/docket/lithld&edis\\_may09](http://www.acc.com/docket/lithld&edis_may09)
- *E-Data and Discovery: Protecting Your Company From Avoidable Risk: The Simple Steps That Every Executive Should Know (Jan. 2007)*. Lack of understanding about data management systems can stand in the way of improving communication between in-house lawyers and IT, before and after receipt of document requests. Prepare your organization and avoid potential pitfalls when you respond to an electronic data request. [www.acc.com/docket/edata&disc\\_jan07](http://www.acc.com/docket/edata&disc_jan07)

### ACC Alliance

- ACC Alliance partner IntraLinks offers corporate legal departments an effective way to manage the exchange and storage of their company's confidential and sensitive information. Exclusive discounts are available. Visit [www.acc.com/alliance](http://www.acc.com/alliance) for more information.

### Article

- *Ediscovery Compliance as Domestic and Foreign Litigation Grows (April 2009)*. Mary Mack, Corporate Technology Counsel for Fios, Inc., discusses the financial crisis, and impact of litigation on businesses outside the financial

sector — focusing on investigation and electronic discovery. [www.acc.com/edisc-compl&lit\\_apr09](http://www.acc.com/edisc-compl&lit_apr09)

### Quick References

- *Electronic Discovery Action Plan (March 2007)*. An electronic discovery action plan should be reviewed on a case-by-case basis and tailored for individual clients' needs, but the following general guidelines can be applied in nearly any situation. [www.acc.com/quickref/ed-actionpln\\_mar07](http://www.acc.com/quickref/ed-actionpln_mar07)
- *Top Ten Tips for Corporate Counsel In Dealing with the New FRCP on Ediscovery (Nov. 2006)*. In December 2006, the amendments to the FRCP forced deep changes in how corporations approach litigation. They require more discussions and planning for the preservation, collection and production of electronic evidence much earlier during litigation. [www.acc.com/quickref/10tips-frcp\\_nov06](http://www.acc.com/quickref/10tips-frcp_nov06)
- *Electronic Discovery: Hype, Sleeping Monster, or Roaring Tiger? (Sept. 2006)*. This material includes steps for how to control the collection, review and production of information during electronic discovery, to preserve client confidences and not waive privileged information. [www.acc.com/quickref/edis-hype\\_sep06](http://www.acc.com/quickref/edis-hype_sep06)
- *Ten Tips on Handling Electronic Discovery (Oct. 2003)*. Review the 10 dos and don'ts of ediscovery. [www.acc.com/quickref/10edtips\\_oct03](http://www.acc.com/quickref/10edtips_oct03)
- *Discovery in the Digital Age (Jan. 2007)*. View this guide addressing the evolving legal duties of in-house counsel regarding discovery and computers. It includes overview of the duty to preserve, relationship with opponents, controlling costs, and admissibility and authentication. [www.acc.com/quickrefer/disc\\_digitalage\\_jan07](http://www.acc.com/quickrefer/disc_digitalage_jan07)

ACC has more material on this subject on our website. Visit [www.acc.com](http://www.acc.com), where you can browse our resources by practice area or use our search to find documents by keyword.

### Practical ediscovery considerations

**Craft defensible litigation hold instructions.** This is not novel advice, but let's acknowledge what sometimes happens in practice: When a lawsuit is filed or anticipated, in-house counsel typically dusts off a litigation hold template or precedent, makes a few changes to fit the new case (or simply instructs custodians to "save everything"), and delivers hold instructions to the usual suspects. Time is of the essence, so all of this is done quickly, without a lot

of analysis about how now might be different than before. The result is that you may direct people to save too much or too little; the "usual suspects" may not be everyone who reasonably should be placed under litigation hold. Further, the spam delivery of instructions that are either unintelligible, too legalistic or too much trouble to adhere to, may be ignored.

Treat hold instructions with the reverence they deserve. First, you must make intelligent effort to assess the claims

# Proportionality: WHY WAIT?

**A**dvocates for corporate legal departments have proposed changes to the rules governing civil procedure. Yet, there is an existing and overlooked approach to reduce electronic discovery costs available now.

It is well-documented that e-discovery consumes increasing percentages of overall civil litigation costs. Judges and legal professionals are exploring various initiatives to address the problem, and several recent conferences and rulings have taken up the theme of proportionality. Proportionality shifts attention from the general problem of high-volume, prohibitively expensive productions to a more focused analysis of whether discovery costs are proportionate to the value and the importance of the case in question. The American College of Trial Lawyers Task Force on Discovery declared that, “Proportionality should be the most important principle applied to all discovery.”<sup>1</sup>

Federal Rule 26(b)(2)(C)(iii), the existing procedural rule that addresses proportionality, is remarkably lucid and robust:

*On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that . . . the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.*

Considerable attention has been paid to the many factors contributing to the growing “burden or expense” of e-discovery, yet it is striking in retrospect how quiet the judiciary has been, until recently, about the concept of proportionality as it appears in the Federal Rules. The rule unambiguously states the court must balance the scope of proposed discovery against case-specific variables such as the amount of damages and fees in question, the risks to the parties, the magnitude of the legal issues at



MARY MACK, Esq.  
Technology Counsel  
Fios, Inc.  
mmack@fiosinc.com

stake and the relative importance of electronic evidence in arriving at a resolution.

Proportionality has often been forgotten in the past; however, it now appears that the judiciary is undergoing an important

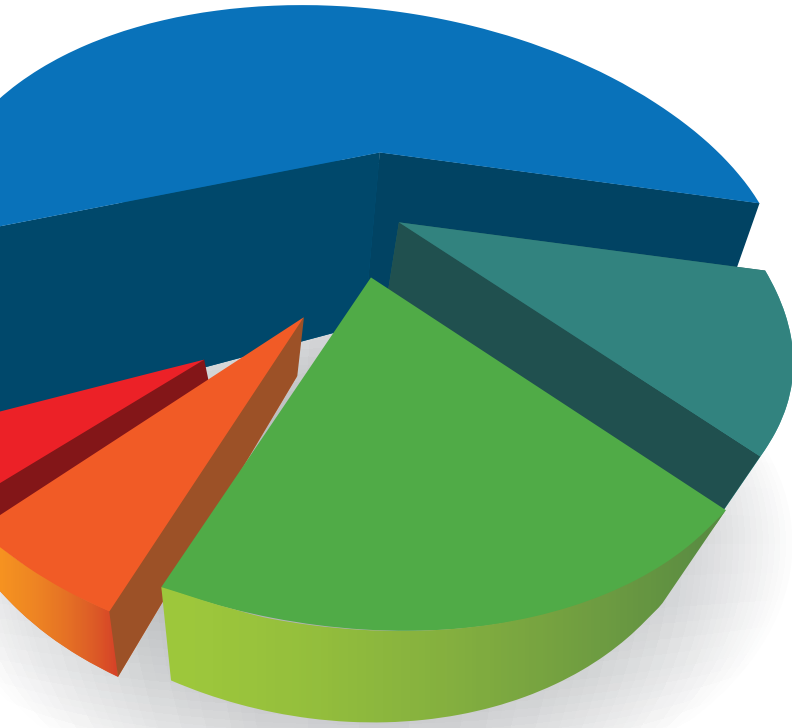
cultural shift. Before, judges may have been waiting for properly formed motions to invoke the proportionality requirement in considering broad discovery requests. That is no longer the case, as Federal District Court Judge Lee Rosenthal demonstrated in *Rimkus*, where she makes explicit reference to the rule and cites proportionality as the decisive factor in determining what is “acceptable” and “reasonable” in “preservation and discovery conduct.”

Judge Waxse, author of several ground-breaking decisions in e-discovery disputes, was surprised when he recently re-read the rule and realized it set forth an explicit requirement—“the court must”—rather than a mere recommendation. Waxse now refers to the proportionality provision in the Federal Rules as, “. . . probably the most underused, valuable rule we have. . . Judges on their own are supposed to consider this. . . We don’t need to change the rule; we need to start using the rule.”<sup>2</sup>

## What does this mean for corporate legal departments?

The new emphasis on proportionality has a number of practical implications for e-discovery. Both the number and the scope of discovery requests are likely to be subject to more limits and to closer judicial scrutiny, thereby reducing costs. Adversarial conduct in the discovery process will be increasingly discouraged, as will the wielding of far-reaching requests as a blunt-force weapon to compel early settlement. Broad, boilerplate requests and universal checklists will no longer pass muster. Instead, meaningful cooperation between counsel will be paramount; and litigants will need to produce accurate, detailed, case-specific, court-consumable documentation as the best means to demonstrate the appropriate level of proportionality.

In effect, both parties to a case involving large volumes



of electronic data will need to undertake a detailed cost-benefit analysis early in the litigation process. Parties should specify the anticipated impact of proposed discovery (in terms of factors like cost, time, risk and disruption of day-to-day business), and then be prepared to weigh these burdens against the overall value of the case, the significance of its core legal issues and the anticipated benefits of the requested evidence for its resolution.

Another likely outcome of evoking the proportionality rule is that litigants will be urged to focus initial discovery efforts on the data that appears to be most relevant to

**“Proportionality...  
probably the  
most underused,  
valuable rule  
we have.”**

— *Federal Magistrate  
Judge David Waxse*

the issues and least burdensome to produce. Phased productions, in which the scope of each successive effort is narrower and more closely targeted to the key legal issues of the case, will be more common. Defensible data sampling and search techniques using tools designed specifically for e-discovery will become increasingly important.

E-discovery partners, like Fios, understand these cost drivers intimately. And a quality vendor won't hesitate to apply the most precise methods and technologies available to assist in projecting early on what scope of inquiry is reasonable and is proportional to the value of the case. (See case study sidebar.)

So the next time the plaintiff attempts to force early settlement with a broad discovery request, don't wait, use proportionality and a trusted e-discovery partner to ensure rationality prevails.

### Case Study

A large corporation discovered one of its executives did something unethical and potentially illegal. The executive was dismissed; authorities were notified. The company was sued in U.S. District Court by a customer in connection with the dismissed executive's actions in the handling of a product line. The plaintiff requested that the defendants produce electronic evidence related to all similar matters involving related products at the company. Defendant's counsel, with the assistance of Fios, countered that producing evidence relating to multiple similar product incidents was disproportionate to the value of the case, which concerned a single customer and a single product line.

Fios, handling e-discovery processing, hosted review and productions for the defendant, sampled a subset of the data directly related to the plaintiff's complaint. Means, medians and averages pertaining to data volumes were used to project volumes—and costs—associated with expanding discovery to additional matters. Fios also generated culling reports, showing drastic reduction in responsiveness when evidence was collected from other custodians. Finally, a random sample of non-hits from the culling process revealed no relevant data was omitted. All information was included in a formal declaration presented to the court by counsel to demonstrate that **requested discovery was disproportionate to the case.**

To explore more resources, including Fios' proportionality webcast with Judge Waxse, footnote references 1 & 2, or to set up a meeting with Mary Mack, visit [www.fiosinc.com/ACC2010](http://www.fiosinc.com/ACC2010).

Fios' e-discovery experts can help.  
Contact us at: **877.700.3467**



or issues in the litigation, actual or potential, in order to identify with reasonable particularity the documents to be retained. Define too broadly, and you buy yourself a real expense when you later have to collect and review a mass of documents irrelevant to any issue; define too narrowly, and the other side will squawk — you may also deprive yourself of evidence needed for your company’s case. This isn’t always simple, but it deserves due attention at the busy advent of litigation. Second, you should draft litigation hold instructions in normal-person language. Sure, it will be difficult, but your employees aren’t lawyers and legalese is easily misunderstood, if not ignored. Third, for attention-grabbing reasons, consider having hold instructions delivered by a high-ranking or well-respected member of management, since they are more likely to procure

**If in doubt, disclose; if you truly believe your custodian’s assertions of good faith compliance and doubts can reasonably be resolved against disclosure, stand firm and defend.**

custodian attention and compliance. Fourth, avoid the urge to shy away from potential preservation challenges; instead, highlight them and offer useful help. If, for example, the company has — as Intel did — a fully-operating auto-delete function that it doesn’t intend to disable, experience teaches that it is best to specifically tell employees about it and instruct them on how they should deal with it. Likewise, consider providing custodians the name of a lawyer and an IT professional who have been pre-designated to provide “white glove” preservation assistance when necessary and appropriate.

Finally and importantly, draft your litigation hold notice expecting that it will be disclosed. Cases are mixed on whether these communications are privileged or attorney work product. In *AMD v. Intel*, the parties exchanged litigation hold instructions with the agreement that doing so would not constitute a broader waiver of work product or privilege. Both sides realized that preserving a privilege claim for a widely-distributed document, the content

of which is increasingly viewed as non-confidential — or not even as legal advice — is tough. It’s especially difficult if your judge views it as containing simply “facts” about preservation efforts that the other side deserves to know. In fact, counsel may wish to disclose these notices in order to demonstrate preservation compliance.

**Commit to preservation program design and implementation.** A lot of attention-grabbing tasks rear up when litigation does, and some in-house counsel (since they are human) tend to handle the familiar before dealing with the new and difficult — like those annoying evidence preservation issues. Who can blame them? Learning the scope and nuances of the company’s often-complex IT infrastructure and what data is stored where and by what means can be daunting to the uninitiated. Yet successful preservation programs are those that are initiated promptly, designed with the input of experienced professionals and implemented with care.

This need not be unduly overwhelming. Company IT professionals are a vital resource, and designating at least one as the legal department liaison to assist in preservation program design and implementation can be helpful. You will have to learn their language (a sometimes tall task) and cannot permit unintelligible IT-speak to be uttered without cross-examination. Ediscovery vendors can also help. Many have deep experience and while their technical advice is not a sufficient surrogate for the legal advice you must give, it can prove a useful guide. A warning: Ediscovery vendors and consultants come in all shapes and sizes, and some sell elixir of questionable curative quality; professed expertise unaccompanied by real-world experience will get you nothing but a bill to pay. As such, you might want to turn to your trusted IT personnel and experienced outside counsel to assist in ediscovery vendor vetting and selection. Remember that technical prowess, while helpful, is only of marginal help to designing, defending or prosecuting evidence preservation issues.

Ultimately, of course, it is the duty of in-house counsel to design a defensible preservation program that is well-implemented and scrupulously monitored. Do so cautiously, carefully, according to well-defined, defensible protocols, and document what you have done. If the challenge to your program comes — many months or even years into the litigation — you will want to be able to resort to records that defend your prior choices.

**Monitor, monitor, monitor.** The now famous *Zubulake* series of ediscovery decisions and the recent *Pension Committee of the Univ. of Montreal Pension Plan, et al., v. Banc of America Securities, LLC, et al.* decision by the same judge, place a non-delegable duty on in-house counsel to monitor and enforce both custodian preservation and data collection efforts. In short, you need to ensure that

executives and employees understand their obligations and are making appropriate efforts to comply. Merely sending a good hold notice when the case starts is not enough. You should consider establishing a schedule for periodic delivery of written preservation reminders throughout litigation. Also consider other effective means of cultivating a preservation-oriented employee mindset by such activities as brief custodian preservation interviews; presentations at group meetings (such as sales conferences and the like); one-off conversations or written communications with the most important or potentially-problematic custodians; or legal department training programs and presentations that emphasize proper preservation behavior without boring the audience to tears. Thoughtful implementation — well documented for potential later use — can be surprisingly inexpensive and burden-free. It beats the alternative of having to explain under oath why monitoring was too much trouble to undertake.

**Take reasonable steps to strategically protect privilege.** Protecting privilege in the ediscovery era isn't child's play. No one disputes that the law obligates in-house counsel to design, implement and monitor preservation, data collection and production. When inquiry, or an inquisition, is made into the effectiveness of these activities, counsel's acts, omissions, communications and thought processes come at least arguably into play. You may be tasked with defending what you did or didn't do by disclosing it, thus jeopardizing truly privileged matters. Even the wary can stumble. In the *AMD v. Intel* case, for instance, the court held that Intel had waived privilege as to certain aspects of an outside counsel-led investigation it conducted into custodian preservation failures, in part because of its remediation plan's assertion that nothing of genuine significance had been destroyed. The court therefore ordered the disclosure of attorney interview notes. The court also found that AMD had waived privilege by filing an attorney declaration that specified preservation steps it had taken. The point is that the potential for waiving privilege and work product makes for dangerous ediscovery shoals that even a seasoned navigator may not be able to avoid.

Summarizing in this article all the proper protocols for privilege protection that a party should take would surely be unsuccessful. But we suggest that in-house counsel should be cognizant up front that some fact-based attorney communications — those that attorneys would refer to as “non-core” — not only are subject to discovery but perhaps should be voluntarily disclosed, at least under an agreement that disclosure would not operate as a broader or subject matter waiver of privilege. An opposing party hungry for preservation information might be inclined to acquiesce in this agreement,

especially if it operates reciprocally. In short, what an attorney does, as a factual matter, to ensure compliance with ediscovery obligations, even if potentially privileged, should be viewed cautiously as something you may want or have to disclose. Generating a paper trail of preservation activities requires care to separate the non-core, fact-based communications that might later be produced or relied upon to show preservation compliance, from “core” communications containing attorney thought processes and legal conclusions, which should in all events be vigilantly protected.

**Beware of the pesky issue of auto-delete.** An “auto-delete” function operates to purge emails that are stored for certain time periods in an active mailbox. AMD had no auto-delete function while Intel's auto-delete purged inbox email in 30 days, sent items within 7 days, and deleted items within 24 hours. Without a backstop against loss (such as backup tapes or automatic journaling), an auto-delete function can permanently expunge vital data. Intel's decision not to disable auto-delete was, in fact, a central Intel choice that AMD contended led to massive data loss.

In this day and age, leaving auto-delete running in the face of a clear preservation duty entails risk and can easily be second-guessed by your opposition. Indeed, as noted in the recent *Pension Committee* case referred to before, some courts consider the failure to disable auto-delete as evidence of “gross negligence,” — a designation that may be visited with severe sanctions. Without a machine-based backstop against loss — (e.g., journaling, vaulting or dedicated email servers subject to timely, retained backups) — exclusive reliance on custodian “self-selection” of materials while leaving email subject to automatic deletion, risks loss you may have to explain, remediate or pay for by way of sanctions.

Some of the main problems with disabling auto-delete are how to store, manage, and — after the litigation is over — dispose the huge volumes of email that accumulate as a result. Your average IT professional is likely to balk at simply “shutting auto-delete off,” given the potential performance hit on email systems this may cause, and because solutions for handling the increased volume of email impose costs and technical challenges. Yet solutions exist for appropriate cases. Both parties in *AMD v. Intel* adopted automatic journaling as a retention mechanism that mooted the auto-delete risk (AMD six months after the case began in November 2005, and Intel shortly after it disclosed its preservation errors in early 2007). The cost of these email-capturing solutions has decreased over the years, and ediscovery and IT professionals can advise about other defensible retention means. Our view is that developing case law and standards governing email retention will increasingly induce corporations, especially larger ones,

to implement these mechanisms in appropriate cases that involve prospective preservation obligations.

**Deal with the rogue custodian.** Here is a not entirely unusual situation: You have done everything you should to procure a custodian's compliance with preservation duties. You've issued a timely litigation hold notice; sent reminders; talked by telephone with the custodian about preservation; and even met with him and secured his affirmation of compliance. Yet despite all this, when the data "harvest" and review is completed, major gaps in his data corpus exist, suggesting either a collection error or, worse, custodian non-compliance or intentional deletion of relevant data. The fear is that the custodian has gone "rogue" on you and, despite his representations of adherence to instructions, simply deleted what he should have retained, purposely or through lay-person inadvertence.

The rogue custodian presents a troubling conundrum. The preservation duty of the corporate litigant is, of course, to take reasonable steps to save potentially relevant data. In the hypothetical above, you would have done that and therefore satisfied the corporation's legal duty. Or did you? You are aware that the custodian's produced data set is deficient; you suspect non-compliance and case law is sufficiently clear to impose upon you and outside counsel a duty to apprise the opposing party and the court of certain losses of relevant data. If you disclose the apparent loss, however, you buy yourself preservation discovery, a discovery motion or possibly even sanctions. If you don't disclose, a sophisticated opponent may uncover the apparent deficiency and claim you haven't "come clean" with the court. It's a Catch 22.

The answer, as with many preservation issues, is dependent on the circumstances. You must first examine alternatives to spoliation as the possible explanation for apparent loss, such as collection failures, a missed delivery of data to the vendor, corrupt electronic files, or a data processing error. When those causes are ruled out — and after you've again interviewed the custodian to get to the bottom of his preservation habits and omissions — a judgment must be made. Ethical mandates and the duty of candor owed the court may well compel you to make a disclosure against interest that leads to self-inflicted pain, but satisfies your obligations as an officer of the court; let the preservation chips fall where they may. On the other hand, you may well conclude that your company's rogue custodian reasonably, although narrowly, interpreted preservation instructions, and that hopefully, whatever he lost is contained in the files of other custodians' collections; there has been no loss or harm.

Maintaining credibility with the court is a commodity of great price and value, and adherence to and discharge of legal duties is something we all accept as vitally necessary

to a properly-functioning legal system. If in doubt, disclose; if you truly believe your custodian's assertions of good faith compliance and doubts can reasonably be resolved against disclosure, stand firm and defend. Either choice may cost you — and you may rue your rogue custodian — but the alternatives to self-disclosure may be slim or none.

**Don't leave real data loss undetected.** Whether you or the other side has lost data may remain a secret unless you proactively try to detect and resolve it. Given the high stakes of an adverse inference and the potentially-huge monetary penalty Intel faced in *AMD v. Intel*, as each side fly-specked the other's document productions, looking for data loss in an expensive preservation holy war is incommensurate with normal litigation protocol and, perhaps, good sense. That is no model for how things should be done (though it certainly seemed justified at the time). However, counsel's desire to protect their corporate client against claims of preservation failure may compel implementation of reasonable audit steps to detect their own data losses.

In *AMD v. Intel*, for example, both parties focused in large part on custodians' electronic "file counts." The analyses generally compared the number of files kept monthly by document custodians themselves when they had no automatic preservation backstop against loss (like journaling), against monthly file counts when machines saved everything for them. It was, in short, a comparison of preservation efforts afflicted by human frailty (since even the most conscientious custodian won't save everything) against the perfection of machine-based, automatic preservation of all email sent or received. Where the disparities between the "self-preservation" and automatic preservation file counts were too high (e.g., the amount of email increased between the two periods by 50 percent, 100 percent or even by many multiples beyond that), the parties asserted insufficient preservation. While this is only one aspect of some rather sophisticated analytics each side deployed to assert non-preservation by the other, it proved a major arrow in the quiver of asserted evidence preservation failures.

A safe protocol to avoid these kinds of alarming file count gaps might include auditing the completeness of your data collection. Auditing can take place at many steps in the process and take many forms, including auditing data when processing it in an ediscovery tool; auditing during and after document review; and auditing just before production (e.g., by tabulating the number of relevant files about to be produced for each month of the production period) to see if file count variations month-to-month reflect gaps or disparities that suggest anomalies. If auditing reveals error of sufficient import, fix it. Of course, there is cost in all of this, and some steps might be foregone in

favor of less-expensive alternatives. Abjectly ignoring collection, processing and production analytics, however, can be like playing a preservation roulette wheel, especially if your opponent is sophisticated or just ornery.

The same goes for data received. Most electronic review tools and vendors of any real worth can execute relatively low-cost analytics on produced collections that may provide essential insight into whether your opponent has a preservation problem — or is stiffing you.

**Think strategically about proving evidence spoliation.** Generally speaking, sanctions for evidence spoliation require proof that:

- the spoiling party had control over the evidence and an obligation to preserve it at the time it was lost or destroyed;
- the spoiling party acted with a culpable state of mind; and
- the lost or destroyed evidence was not only relevant to the innocent party's claims or defenses, but also that party suffered real prejudice as a result of not having it.


That third set of proof points can be challenging. How can you possibly say that what has been permanently expunged is relevant if you've been deprived of the opportunity to see it? And showing that you have been prejudiced because the lost evidence was probative on essential merits issues requires an even greater analytic stretch. The new *Pension Committee* case provides a shifting burden of proof and presumption-of-prejudice regime which, if adopted more broadly, will ease the burden of proving the relevance of and prejudice resulting from lost data (and, we fear, increasingly induce the ill-motivated litigant to pursue questionable spoliation cases that impose burden and expense on even a compliant party acting in good faith).

There are other means of showing the relevance and importance of destroyed electronic data that you've never seen. For example, if a third party has produced documents in the case, compare "hot" (i.e., important and probative) email sent between the party and your opponent to determine whether your opponent's production contains the same email file. If not, something's fishy. As discussed before, file counts also can be at least suggestive of spoliation; where total files produced in month one are wholly disparate from the preceding and following months, for example, the producing party may have something to explain. Alternatively, if the production of one custodian similarly situated in duties and position to another custodian is woefully shy of the volume his colleague produced, a legitimate question of preservation impropriety may be raised. Likewise, an email sent by custodian A that is found only in the produced data set of custodian B shows that A didn't keep what B thought (and, as evidenced by production, the

corporate litigant thought) was relevant to the case. The significant accumulation and tabulation of these relevant and, hopefully, "smoking gun" electronic documents found only in other custodians' files can be a strong indicator that something is amiss — and suggestive that it was not only the already-produced file that was purged by the offending, non-compliant custodian.

These analytics can cost you, and ediscovery vendors or experts worth their salt may be vital to generating the proof needed to persuade a court to issue a spoliation sanction. Of course, these tools in the hands of an opponent bent on proving loss could generate messy — or at least expensive — preservation discovery that could become a distracting sideshow of limited or non-existent validity. But if the other side erred in ways that suggest bad faith or deprivation of vital evidence, employing them to the good end of insisting on discovery compliance is both justified and, perhaps, a necessary part of discharging your duty zealously to represent your client.

### Central lesson learned

The foundation of proper preservation and modern ediscovery compliance is founded on in-house counsel's dedication and commitment to doing it right. In ediscovery, thinking, planning, strategy, priorities and timing are more important than just hard work, and are essential to designing, implementing and defending an effective and compliant evidence preservation program. Costs come, usually early and sometimes often. But evidence preservation efforts initiated promptly, crafted thoughtfully, and implemented with care can make that investment pay off. Those efforts will avoid risk and minimize expensive preservation discovery battles — or an award of sanctions — later in the case. 

*The opinions expressed in this article do not necessarily reflect the views of O'Melveny or its clients, and should not be relied upon as legal advice.*

Have a comment on this article? Email [editorinchief@acc.com](mailto:editorinchief@acc.com).

#### NOTES

- 1 Jonathan Swift, *Gulliver's Travels* (1726).
- 2 Despite a relationship that for three decades has been "difficult, challenging and often acrimonious," the former combatants "wip[ed] the slate clean" of past grievances, and expressed a mutual desire to coexist in a "constructive manner" and to resolve future grievances "amicably, if possible" through their settlement of the case. (Settlement Agreement, Recitals, ¶ D.)

Reprinted with permission of the authors and the Association of Corporate Counsel as it originally appeared: "Evidence Preservation Warfare: Ediscovery Lessons Learned from AMD v. Intel," *ACC Docket* 28, no. 7 (September 2010): 66-77. © 2010 the Association of Corporate Counsel. All rights reserved. If you are interested in joining ACC, please go to [www.acc.com](http://www.acc.com), call 202.293.4103, ext. 360, or email [membership@acc.com](mailto:membership@acc.com).