

security as well as the protocols and methodologies for the recovery and production of electronic data.

2. I hold a Bachelors of Science degree in Criminal Justice and a Masters in Business Administration. Since devoting myself to forensic discovery, I have served as a Speaker for the American Society of Industrial Security, Federation of Insurance and Corporate Counsels, Association of Certified Fraud Examiners, International Association of Financial Crimes Investigators and various Bar Associations in California, Arizona and Texas. I am a member of the High Technology Crime Investigators Association (HTCIA), ARMA (Record Management) International, the Computer Security Institute (CSI), ASIS International, Association of Certified Fraud Examiners and the International Association of Financial Crimes Investigators (IAFCI). I hold certifications as a Certified Protection Professional (CPP) and a Certified Fraud Examiner (CFE). I have written numerous articles on computer forensics, computer security and electronic discovery.

Corporate Document Preservation Policies

3. On any given day, hundreds of thousands of emails and electronic documents are created at companies like the OEMs, distributors and retailers from whom AMD intends to take discovery. Like boxes filling up a warehouse, email and electronic data consume ever-increasing amounts of space on the memory devices of corporate computers and servers – both of which have limited storage capacity. Instead of endlessly purchasing more and more capacity, virtually all major U.S. and foreign businesses have adopted some form of document destruction and retention policies. Pursuant to these policies, older and inactive files are deleted on a systematic or scheduled basis in order to ensure that adequate storage capacity is available for newer, more active files.

4. The destruction of data is, therefore, a central feature of any company's document retention and destruction policy. With respect to electronic documents and

communications, such as emails, instant messages, memoranda, PowerPoint presentations, and spreadsheets, data is continually being preserved for a certain period of time and then purged in order to make room for new data that is created. This creation and deletion cycle happens at virtually every major company. With the exponential growth in the pace of electronic communications and the relentless reproduction rate of electronic data, no company can afford to save everything. From company to company, the cycle of deletions may vary in timing. Eventually, however, all data that is not designated for preservation will be deleted. This destruction can be prevented if the company takes the following steps detailed in the remainder of this Declaration.

Suspending the Automatic Destruction of Evidence

5. The first step in preserving documents relevant to litigation is ensuring that the proper custodians of information are identified. With knowledge of the proper custodians, the company can narrow its document preservation efforts only to the data that is essential to the case. Here, as a result of its factual investigation, AMD has been able to identify a set of the most important document custodians at each company. AMD has asked the company to supplement that list with any direct reports or persons above the custodian in the chain of command.

6. Once the custodians are identified, the company should suspend the systematic destruction of that custodian's documents that occurs in the ordinary course. For instance, most companies enforce policies that target informal, intra-corporate communications such as email or instant messages when they achieve a specified age, *i.e.*, thirty, sixty, or ninety days old. Companies employ this policy to manage the massive data that is created on a daily basis from electronic communications. Without active steps taken to preserve this data, it is likely to be subject to the automatic deletions described above. This step is relatively inexpensive and only requires a couple hours of an information technology technician at the company to alter the deletion schedule for that specific individual.

7. In addition, manual (*i.e.*, user activated) deletions of relevant documents and data must also be suspended. To accomplish this, the company need only send out a notice to the individual custodians informing them of their legal obligation to maintain documents relevant to this litigation and request a return confirmation that each custodian understands her obligation. With the most important custodians already having been identified by AMD, the company need only send an email or hard copy memorandum to the identified custodians and await return confirmation. The cost of such a notice is negligible.

8. To preserve other historical data and documents on the individual's computer, a company should duplicate or "mirror" the hard drive of each custodian. For most companies, this can be done by an information technology technician accessing the files via the company's network or through the laptop or desktop of that custodian, and transferring a mirror image of all the documents and data from that employee to another hard drive. Portable hard drive storage devices used to store this type of information tend to cost in the neighborhood of \$150. If the company does it internally, it will cost approximately \$300 per custodian. To hire a third party vendor to accomplish the entire task of mirroring the hard drive and copying it to a portable storage device would cost approximately \$500 per custodian.

The Importance of Backup Tapes

9. The above mentioned steps should preserve the relevant documents that exist on a custodian's hard drive. Another universe of relevant documents exists, however, on what are referred to as backup tapes. It is often on these backup tapes where the most relevant evidence can be found.

10. To protect against the unintentional loss of data, corporations make copies of their data onto backup tapes. Here is how the process of backup tapes works: Each company is likely to have a master set of backup tapes which contain a full image of the entire system ("full backup"). Companies typically run a full backup on a weekly or

monthly basis. In addition, companies also will have a set of incremental backup tapes which save new information on a regular basis since the last full backup tapes were made. An incremental backup is like a daily snapshot of what is currently on the system. Thus, an email that may have been deleted by a custodian prior to the suspension of the automatic deletion function as well as documents that have changed over time are likely to exist in their original form on these backup tapes. Backup tapes have, therefore, become a critical component of what is searched when companies produce relevant evidence.

11. Backup tapes, however, are not maintained indefinitely. These full and incremental backup tapes are stored in a facility for thirty, sixty, or ninety days, depending on the company's policy, at which point they are "recycled." When tapes are recycled, they are re-used, new data is placed on them, and the old data is lost forever. The most effective means of preserving this data is to "sequester" or set aside the backup tapes containing the data of the relevant custodians. Searching the backup tapes to determine which contain data of the relevant custodians is the most expensive part of the process, but even this could be accomplished for \$150 per custodian. The company would then need to remove these backup tapes from the rotation of tapes used. As a result, the company might have to purchase additional backup tapes. However, these are relatively inexpensive – depending on media type, five replacement tapes might cost between \$250 and \$600.

12. On a going forward basis, the company can redirect the data of the relevant custodian to one backup tape. This would require less than five hours of a technician's time. Such a directed backup effort would avoid the cost of sequestering unnecessarily any backup tapes.

13. Finally, because the issues in this case will turn on the terms of sales and negotiations between the third parties and Intel, the specific software used to track sales transactions also must be preserved. I am familiar with this software because I use it in

my business. Many of these companies employ proprietary sales databases or third party vendors such as "Salesforce.com" to house their sales data – from contact information to minutes of sales meetings to actual sales records. Such information detailing the dates, times and content of sales negotiations also needs to be preserved from systematic destruction. Preservation of this information will require a full copy to be made, a suspension of the recycling of the backup tapes associated with this software, or an additional fee paid to the third party vendor to retain such data. None of these steps should cost more than a few hundred dollars per month of data.

14. While the total costs of these preservation measures are not negligible, they are costs that third parties incur regularly in the discovery process as the amount and importance of electronic data has grown. For multinational companies as large as the ones listed here, such preservation efforts are not a substantial burden. Instead, these technology companies are likely to have large staffs of information technology professionals. Securing the data of 10-30 document custodians for three - six months should not cost in excess of \$10,000 - \$30,000 even in the most complicated case. It should be noted that most of these costs will be incurred whether the company preserves documents in response to this subpoena or not. Eventually in this litigation, these companies will have to access this data and produce it when it is requested.

15. Failing to take these prophylactic steps, however, will almost assuredly lead to higher costs. Documents deleted from network and desktop computers before being copied to back-up storage (or lost when back-up tapes are overwritten) more than likely are permanently destroyed. In some cases, however, these documents can be recovered by computer forensics experts who specialize in document recovery, and if the documents are deemed sufficiently important, an expert is summoned. The document recovery expert must then attempt to collect and restore data from "unstructured" or unrecognizable areas of the media. This requires converting files that have become unstructured back into active files. These electronic data recovery efforts are usually

vastly more expensive than what it would have cost to prevent their destruction. Moreover, if the documents are unrecoverable, the cost to the affected litigant is immeasurable.

I declare under the penalty of perjury of the laws of the United States and the State of Arizona that the foregoing is true and correct.

Executed this 1st day of July, 2005 at Phoenix, Arizona.

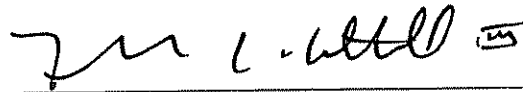


KELLY J. KUCHTA

CERTIFICATE OF SERVICE

I hereby certify that on July 1, 2005, I electronically filed the foregoing with the Clerk of Court using CM/ECF and served the foregoing on the following counsel via Federal Express:

Darren B. Bernhard, Esquire
Howrey LLP
1299 Pennsylvania Avenue, N.W.
Washington, D.C. 20004-2402



Frederick L. Cottrell, III (#2555)
cottrell@rlf.com