Technology on Trial: Prosecutors Leave an E-Trail

John Bringardner

could have been a scene from Fox TV's Cops, as John Rigas, the frail, 77-year-old founder of Adelphia Communications Corp., was led out of his Park Avenue apartment in handcuffs the morning of July 24, 2002. The media was out in full force, capturing images of the fallen leader who would face charges that he turned the multi-national cable company into his personal piggy bank.

Indeed, two years later, on July 8, 2004, a federal jury in Manhattan found Rigas guilty on 18 of 23 counts, including concealing $2.3 billion in loans and stealing more than $100 million from the now-bankrupt company, based in Coudersport, Pa.

Rigas now faces up to 20 years in prison, but a technical snag in the investigation could have jeopardized the conviction. And that glitch offers us an important lesson on how to properly handle electronic documents.

A court opinion, rendered by U.S. district judge Leonard Sand on Sept. 22, 2003, discusses the manner in which the U.S. Attorney's Office collected evidence from hard drives provided by Adelphia. When the drives were returned to Adelphia, defense attorneys discovered work product left by the government on two of the drives, and petitioned the court for the right to use that information.

Compromised Hard Drives

In United States of America v. John J. Rigas, Timothy J. Rigas, Michael J. Rigas, and Michael C. Mulcahey [02 Cr. 1236(LBS)], the defendants were charged with conspiracy, bank fraud, wire fraud, and securities fraud in connection with the management and control

of Adelphia. As part of its investigation, the government issued Grand Jury subpoenas to Adelphia requesting documents covering a wide range of issues.

In August 2002, Adelphia responded by producing, among other things, exact copies of 26 computer hard drives, created by accounting firm PricewaterhouseCoopers, which had been retained by Adelphia. The original hard drives remained with Adelphia in "pristine condition," explained assistant U.S. attorney Christopher Clark.

Doar, a court technology and litigation support firm based in Lynbrook, N.Y., was asked to make copies of the Adelphia hard drives used by the United States Attorneys' Office, on behalf of the defense team.

When defense counsel examined the drives they discovered that two of the them contained work product from Margaret Lee, a U.S.A.O. paralegal. Unbeknownst to her at the time, Lee's computer had copied files from its own network onto the Adelphia hard drives, according to court documents.

Defense counsel then petitioned the court to keep the work product.

Proper Protocol

Adelphia asked Paul Neale, vice president and general manager of Doar, to testify before Judge Sand about the proper protocol that should have been followed in the duplication of the Adelphia hard drives.

"The accepted industry standard regarding handling original electronic evidence is, 'Do not handle original electronic evidence,' " Neale explained during an interview with LTN.

"The nature of electronic files in and of themselves makes them dynamic and subject to change just by opening the file. Therefore, you should always review electronic documents from a working copy of the hard drive/back up tape/storage device/etc."

Court documents report that paralegal Lee had conducted a cursory review of the drive to confirm that it could be accessed. That document was located within a folder labeled "MLee" on the hard drive from the computer used by James Brown, Adelphia's former vice president for finance.

Upon the discovery of the Lee files, Doar's Neale notified Peter Fleming, defense counsel for John Rigas. Fleming then called U.S. assistant attorney Clark, and advised him that no one on the defense team had read the chronology or any other U.S.A.O. documents on the hard drive, according to court documents.

James Miller, a U.S.A.O. computer specialist, discovered that Lee's entire computer network account was copied onto two of the 26 hard drives, court documents showed.

It turned out that Lee's computer had copied Grand Jury material, confidential law enforcement information, as well as her own work product relating not only to the Adelphia matter, but to a number of other cases.

Miller also discovered that a directory with Lee's user name was present on a second Adelphia drive, but no files had been copied into that directory.

How it Happened

Each U.S.A.O. computer terminal contains a hard drive, divided into two "virtual" drives (the "C" and the "D" drives). According to court records, the "D" drive is used for, among other things, storing a backup copy of files saved within the U.S.A.O. network account of the computer's "designated user."

The backup copy was generated using Peersync software, from Hauppage, N.Y.'s Peer Software Inc. It creates a backup after a designated user logs on to the network.

When Miller installed one of the Adelphia hard drives into the U.S.A.O. computer, he unknowingly triggered a change in the way that computer's existing hard drive was partitioned, according to court documents.

As a result, the Adelphia drive became the "D" drive and Peersync replicated the files of the designated user (Margaret Lee) on to that Adelphia drive rather than the computer's own existing hard drive.

Rigas' defense team petitioned the court to keep the government's files, arguing that the government waived its work product privilege when it voluntarily permitted defense counsel to copy the hard drives that contained their employee's work product.

Doar's Neale testified that the situation could have been prevented had the government not connected the Adelphia hard drives to its network.

Adding fuel to the fire, explained Neale in the LTN interview, was that he had warned the government about exactly this issue. Neale said he had initiated conversations with the government's IT staff, to advise them on accepted industry standards in handling the duplication of the drives, in order to prevent just such a mishap.

"The government not only ignored industry standards and common sense, they ignored an explicit warning from me that their process was flawed," Neale told LTN.

Paul Marsala, president of Peer Software, declined to comment on the litigation, but explained that the software is designed to be invisible to the end user, "who typically doesn't even know it's running. Everything is completely configurable, there's nothing hardwired in the product. It is all dependent upon how it's applied."

Ultimately, Judge Sand denied the defense application, arguing that the government had "taken reasonable precautions to protect the hard drives' integrity."

Though Neale claimed that it was a "clearly forseeable risk," he also testified that he had never witnessed such an occurrence in all his years of experience with technology-based litigation services.

The U.S.A.O.'s Clark told LTN that because there still existed "sealed, original drives that no one had ever touched, there were originals someone could resort to," there was never any spoliation.

"However," Neale says, "[because] the government was the producing party, those hard drives were the government's 'originals' and should have been handled as such. You wouldn't make notes, redact, highlight original documents and then produce them; you create a working set to use for those purposes."

Lessons Learned

The U.S.A.O. attorneys relied on their IT personnel that the hard drives could be viewed without risk of altertion. Attorneys must be aware that metadata embedded in documents isn't the only hidden danger - electronic data discovery presents other issues that also must not be overlooked. Had the judge ruled otherwise, that hidden data would have provided the defense with a clear outline of the prosecution's tactics.

Disponível em:< http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=3650> Acesso em.: 20 set. 2007.