

Type: Article, Reproduced with the permission of Jario and Legal
Author: Chris Brighthouse, CEO Jario
Date originally appeared: 20th September 2003

How did PCs become such rich targets for Electronic Discovery?

Most IT directors are aware of many of the tracks left behind by users in the daily use of a computer system, even if the majority of users are not. Whether we're aware of them or not, why does software leave so many tracks behind?

The answer to this question typically comes from the software vendor, and the software vendor with the most influence on our systems is of course Microsoft. Let's look at some of the key components of a typical Legal IT system and consider the reasons for their design.

Starting with the operating system, files form the core building blocks, stored on file systems. The critical characteristics of a file system are integrity and performance. To enhance integrity, systems such as RAID have developed which maintain multiple copies of a file simultaneously so that even if a disk fails a copy can be retrieved. For performance reasons, even on single disk systems files are merely marked as deleted, rather than being wiped from the disk, so it is often possible to reconstruct the files from their indexes provided they have not been overwritten. It was not a driving goal of Microsoft or other vendors to allow files to be recovered even after being deleted, but this is the case nevertheless.

Office applications such as Word, Excel, WordPerfect and others all now have comprehensive undo and change tracking facilities to allow the user to undo mistakes and spot document updates. Collaboration facilities now mean that changes must be recorded per user, adding further hidden information to the file. The addition of Meta-data for title and subject allowed users to have a title longer than a DOS 8.3 filename and also to reflect the meta-data automatically throughout the document through macro calls so that only the meta-data needed to be changed and the change would be reflected throughout the document. Meta data has now become a way to tag all sorts of application or process specific data onto files to facilitate automated processing. Meta data now contains useful information about a document, including version and historical information to the extent that there is a growing market in tools to remove meta data from documents before it gets into the wrong hands, therefore crippling the applications that depend on it and creating Meta-data wars between applications in different companies.

Email systems contain automatically generated headers and receipts showing the path they have taken through the internet. This was not implemented as a “big brother” feature, but to ensure delivery and allow delivery problems to be diagnosed. Analysing email trails has now become a major tool of electronic discovery companies.

It is clear, that as computers have become more and more embedded into everything we do they are a natural target for detectives at the scene of the crime trying to unravel the truth about a particular case. These are often skilled consultants with an in-depth knowledge of all the “accidental” ways applications and users leave tracks.

It is also clear that increasingly companies are expected to run their computer systems responsibly. Hence we buy Meta-strippers and carefully document record retention policies and deploy document management systems to maintain our information assets. So now the boot is on the other foot. In order to maintain control and visibility of the activities on the company network, companies must either lock down systems and prevent copying to external devices, emailing through hotmail, or instant messaging systems, and force users to use network drives rather than the ubiquitous 40Gig C: drives most of us now have. This approach has not worked – Microsoft and the powerful Personal Computer have prevented it – we need to work offline and maintain our own information at some time or other, and frankly, this can't be prevented by implementing more applications.

Does this mean that companies now have to employ their own internal document discovery systems to track deleted files, search for incriminating information on a regular basis and review every email or document that enters and leaves the company? It would appear that the answer is fast becoming a resounding “yes”.

Isn't it therefore logical that a system should be devised that works transparently, understanding file systems, applications, documents, DMS systems and online applications and provides complete visibility of the activity on the network? This would not prevent users from working, but would enforce accountability, something that most of us are used to via employment contracts covering all other areas of company activity.

Jario is such a system, working invisibly to the user (like a virus checker) but providing users and managers alike with sensible alert messages and trend information to allow us all to stop worrying and get on with the jobs we're paid to do - using company systems to do the job they were

bought for. You won't need a squad of forensic detectives to know what's going on, and you'll be ready if they do come knocking on your door.

END.