E-discovery Developments:

Rewriting the Rules on Records Management

A host of legal rulings over the past decade mean companies must think before they press "delete."

Adam Cohen
Senior Managing Director,
FTI Technology

Adam Cohen is a nationally recognized expert in electronic discovery and electronic information management policy issues. He advises on planning and implementation issues associated with every phase of electronic discovery in litigations and investigations as well as electronic information management policies and practices.
adam.cohen@fticonsulting.com

Shocking as it may be to senior management, the mundane task of keeping records has become a flashpoint, as legal authorities react to the age of information.

A legal or regulatory investigation, lawsuit or a government audit has a voracious appetite for records. Records often show what people did and what they were thinking when they did it.

But the quantity of records in any enterprise is swelling thanks to the incessant growth of computer processing and storage capacity, increasing modes and usage of digital communications and the proliferation of multimedia applications. According to a 2008 study by International Data Corporation, around 1,200 exabytes (1.2 trillion gigabytes) of digital data will be created this year. But managing all those records is challenging. It is easy to lose them or render them practically unfindable.

In a surprising way, the rise of electronic records is changing the law. Legal authorities are increasingly suspicious, even frustrated, when an enterprise (private or public sector) fails to keep good e-records. For the authorities, the attitude is that all those computer records are critical for accountability and dispute resolution, and therefore they should be kept available for electronic discovery. Further, if records have been buried or destroyed, authorities are prone to sense wrongful intent.

Milestones in the Law of E-discovery

A series of incremental decisions have added up to a major change in companies' responsibilities regarding data.

NOVEMBER 1998
Netscape forced in e-discovery to recover deleted emails from backup tapes.

NOVEMBER 2001
U.S. court sanctions government for its nonparty litigation consultant's destruction of expert draft reports. *Trigon Ins. Co. v. United States*

JUNE 2002
Arthur Andersen criminally convicted for destroying Enron records, including emails.

FEBUARY 2004
U.S. court fines tobacco company $2.75 million, and forbids 11 key executives from testifying at trial, as punishment for adopting early email destruction as usual business practice. *United States v. Philip Morris USA Inc.*

MARCH 2004
Securities and Exchange Commission fines Bank of America Securities $10 million for tardy disclosure of emails under official investigation.

JULY 2004
U.S. court emphasizes responsibility of lawyers to ensure clients find and preserve relevant emails in a lawsuit. *Zubulake v. USB Warburg*

MAY 2005
In a fraud suit, bungled discovery of emails sets stage for $1.45 billion jury award against investment bank. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley*

JULY 2005
In a business-to-business lawsuit, Canadian court orders discovery of records on home PCs and personal cell phones of employees and their families. *CIBC World Markets Inc. v. Genuity Capital Markets*

1998 2001 2002 2003 2004 2005

Illustrations: iStock

As more legal rulings declare that e-records must be retained and organized, corporations and government agencies are in a quandary. Trying to keep everything forever is absurd. Traditional record retention practices, which were developed when paper dominated, now seem out of date, but there is little consensus on what practices to follow instead.

Meanwhile, though courts are not the most tech-savvy institutions, neither are they clueless. The court system is learning fast about topics such as digital forensics and backup tapes. Leading judges such as U.S. Judge Shira Scheindlin are issuing thoughtful opinions on the growing responsibility of counsel to locate and preserve e-evidence as soon as a lawsuit is anticipated – and those opinions quickly become famous via the Internet.

Two other ideas are gaining currency among judges. One is that the discovery of electronic records should be a cooperative process, where litigants are expected to be candid and forthcoming, even in an adversarial court system like the U.S. Another is that records should be found and revealed in phases, such that the easier-to-find records (e.g. more recent emails) are divulged promptly, and other records are resurrected later, but only if the progress of the lawsuit justifies the effort.

Although U.S. courts have been at the vanguard of e-discovery, the phenomenon is global, as the timeline below shows.

What does the future hold? First, the interest of legal authorities in electronic records will only grow. Second, as businesses continue to embrace social networks such as Twitter and rich media such as video conferences, the quantity of e-data will continue to skyrocket.

At the same time, the cost of storing and searching records will continue to fall. Technologies such as cloud computing promise to make enterprise archiving more effective for internal control and for responding to e-discovery. It's not all good news, though. The pressure on corporations and governments to improve the way they preserve data is only going to increase.

From authorities, one message rings clear: they tolerate early record destruction less today than in the past. For management, this message means the enterprise must re-examine its policies on which records to keep and how long to keep them. Although no single solution fits every enterprise, simply to stick with historical practices is dangerous. Those who do not up their game should expect to be penalized (see the implications in the Philip Morris case on our timeline).

What's more, among enterprises that hold records, an old idea is losing favor. The idea that records are dangerous – and should be purged quickly – holds less merit. Plentiful, computer-searchable records are a valuable asset, which can help management maintain control and be marshaled to defend against bogus allegations.

Many enterprises are retaining more records, especially emails, for longer time periods. These records can constitute a valuable day-to-day journal of activity. Retained records present the opportunity to demonstrate that a corporation is a good organization, employing good people, trying to do their best. Sure, people will make unfortunate utterances in email. But in an enterprise of largely well-intentioned people, there should be a negligible number of smoking guns.

2006

DECEMBER 2006
U.S. Federal Rules of Civil Procedure amended to cope with difficulty e-discovery poses for modern litigation.

2007

MARCH 2007
In an employment case, a mirror image of defendant's personal computer was ordered because contact may have been made with current and prospective clients. *Equity Analytics, LLC v. Lundin*

JANUARY 2008
U.S. court sanctions lawyers for cooperating with corporate client that withheld email from discovery demand. *Qualcomm Inc. v. Broadcom Corp*

MAY 2007
U.S. court concluded that unauthenticated emails were not admissible into evidence and set out the requirements needed to properly admit electronically stored information. *Lorraine v. Markel*

JUNE 2007
In a disability case, failure to suspend the "auto-delete" function for emails two years into the case results in an order to produce backup tapes. *Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Authority*

2008

DECEMBER 2008
Ohio Supreme Court orders Seneca County to use extraordinary forensics measures to recover deleted emails so they can be produced under Freedom of Information Act request. *State ex rel. Toledo Blade Co. v. Seneca County Board of Commissioners*

MARCH 2009
Suspecting bad faith, U.S. court sanctions company for destroying e-records for some years before lawsuit was actually filed or specifically threatened. *Phillip M. Adams & Associates v. Dell Inc.*

OCTOBER 2008
UK court orders Cable & Wireless to retrieve deleted email from backup tapes. *Digicel et al. v. Cable & Wireless*

2009

SEPTEMBER 2009
U.S. court fines in-house lawyer at Seminole County (Florida) Sheriff's Department for feeble effort to ensure preservation of lawsuit evidence in email and on laptops. *Swofford v. Eslinger*

JANUARY 2009
Former CEO of Collins & Aikman persuades U.S. Department of Justice to drop prosecution after he assembles 15 million day-to-day company records, especially email, to dramatize the complexity and weakness of the case against him.

OCTOBER 2009
Supreme Court of Arizona finds that embedded metadata is subject to disclosure under Arizona's public records law, joining a Washington State Court of Appeal decision issued approximately a year earlier. *Lake v. City of Phoenix; O'Neill v. City of Shoreline*

MAY 2009
Singapore High Court effectively grants judgment in favor of defendant because plaintiff company failed, at outset of lawsuit, to suspend normal policy of destroying email in six months. *K Solutions Pte Ltd v. National University of Singapore*

2010

JANUARY 2010
East Anglia University (UK) embarrassed by revelation that climate scientists apparently deleted emails to prevent disclosure under Freedom of Information requests.

JANUARY 2010
U.S. court sanctions pension fund for failing to preserve emails as soon as it started to prepare to sue hedge funds. *The Pension Committee of the University of Montreal Pension Plan et al. v. Bank of America Securities*

