Stop Taking the Heat

Six Steps to Avoid the e-Discovery Inferno

Written By Keri Farrell, Product Manager and Kyle Hetherington, e-Discovery Consultant, Dell, Inc.

Abstract

The process of finding, identifying, holding, searching, reviewing, producing and presenting electronic data to be used as evidence in a legal or investigative matter is called electronic discovery, or simply e-discovery. Today, the overwhelming majority of e-discovery is performed against email systems and data. Failure to retain relevant email data puts organizations at risk of significant legal liability, but retaining unnecessary data also incurs significant costs, not only in storing the data but also in processing and review by paralegals and attorneys who charge by the hour. Organizations need processes to help them retain the appropriate data, and to produce it quickly when required by legal proceedings.

In short, organizations need to implement a good information management program. This white paper explains the best practices for such a program and how to choose the right software tools to help implement the program.

Organizations must to be prepared to respond to lit igation or investigations with a multi-pronged approach.

Introduction

In today's fast-paced, high-tech environment, the printed word is fading fast. Pen and ink are quickly being replaced with electronically stored information (ESI), including emails, instant messages, blog posts and other electronic documents. This data is stored not only on servers but also on desktops and personal devices small enough to fit in your pocket.

This explosion of electronic communications has opened new and creative ways of conducting business, but it has also created new challenges in the way litigation and investigations are conducted. Since communications and other records relevant to any legal matter are often found in electronic format, the methods for collecting, processing and reviewing potentially relevant evidence has changed. The process of finding, identifying, holding, searching, reviewing, producing and presenting electronic data to be used as evidence in a legal or investigative matter is called electronic discovery, or simply e-discovery.

The scope of an e-discovery effort can include any form of ESI, but the overwhelming majority of e-discovery is performed against email systems and data. In fact, email data has quickly become the de facto standard for prima facie evidence and affirmative defense in litigation or investigative matters. Unfortunately, searching against email systems often results in enormous amounts of data, which must then be processed and reviewed for relevance, typically by paralegals and attorneys who charge by the hour. Therefore, email processing and review is typically the most costly part of an e-discovery project.

To reduce these costs, organizations must be prepared to respond to litigation or investigations with a multi-pronged approach that includes comprehensive information management and a litigation response plan with defensible preservation and collection procedures. These procedures should be well-documented, as well as continually maintained and monitored.

This white paper identifies best practices in e-discovery and provides tips for selecting the right software solutions to complement an overall strategy that includes defining internal processes and involving business stakeholders, counsel and IT. To illustrate how important best practices are, the paper begins with a story of an unplanned and ill-prepared e-discovery effort, loosely structured like Dante's Divine Comedy—with "circles of hell" updated to reflect the modern workplace.

A divine e-discovery comedy

Suppose an attorney suddenly informed you of pending litigation against your organization and asked you to prevent the deletion or modification of any data that might be important to the litigation, including any files, documents, emails, database records and virtually any electronically stored information that may have been read, written, modified or stored on any device or media. Could you do it? Would you even know where to start?

Unfortunately, most organizations do not know how to respond when faced with litigation. Many users often turn to their IT organization or resident computer expert for quick answers. Without a plan, ill-prepared organizations will lack the necessary operational controls, so they either retain more data than is necessary or fail to preserve the necessary data, and then react by altering existing data retention processes. It is critical to introduce litigation hold as an exception process with its own unique set of requirements. Let's take a look at how a scenario such as this might play out, using our Divine Comedy theme.

The journey begins

The setting and cast of characters

Dark Wood

Dark Wood Company, the unwitting victim in this fictional story, is a medium-sized company with a highly-educated and growing work force. Dark Wood values its people and gives them access to the latest technologies to share their ideas, communicate with clients and collaborate with each other. Like most companies, Dark Wood has dedicated systems and detailed processes for its official business records (contracts, HR, payroll, etc.) to ensure compliance with the company's information governance policies.

When a disgruntled client threatened to sue the company for millions over a breach of contract involving some accounting concerns, Dark Wood was confident that it would be vindicated.

The vestibule

Dark Wood's legal team knows the company doesn't have any official policies regarding email retention. So the lead counsel asks the accounting records manager to ensure that any relevant emails are retained. The records manager, confident in the mission, sets our e-discovery journey into motion.

The upper rings

Circles 1 and 2: Limbo and Desire

Knowing that there are no existing policies governing the retention of email data, the records manager decides that the best approach is to issue a memorandum titled "Hold Order" to all department heads informing them of the possible litigation and their responsibility to ensure that all records relevant to the matter are kept. To reinforce the importance of this directive, the memo also states that failing to comply with the order may result in immediate termination. The records manager is pleased with his work. Because he is confident that everyone will do as requested, he doesn't bother to follow up.

After more than a year, the anticipated litigation finally materializes and e-discovery begins. The legal team expects to be able to hand over any potentially responsive ESI to the opposing party in two weeks. Since the scope of the request is limited to just email and involves only a handful of people (custodians) in Dark Wood's accounting department, two weeks seems reasonable.

A team of five internal IT gurus is tasked with collecting the emails. A list of names is provided by the legal team and a lab server is chosen as the staging area to store the data. Full access is granted to each member of the collections team so they can write data as they collect it. It takes the team a couple of weeks to research the identities, user accounts, email accounts, email servers, file server shares and desktops in use by each of the custodians named for collection. As it turns out, some had recently married and changed their names. Others had moved to new office locations and their data was now spread across multiple servers. Others had received new desktops and their old systems had been either disposed of or given to other employees; no one remembers which systems were reused, whether the old files were deleted or if the systems were flattened and rebuilt.

Nonetheless, the collections team manages to complete a collection for one of the custodians and pauses to brief the legal team before proceeding to the next custodian in the list. The collection of data taken from the custodian's email server, file server and desktop includes over 400 .pst files totaling 500 GB, and more than 600,000 emails.

"Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita."

Dante Alighieri
Midway in our life's journey, I went astray from the straight road and woke to find myself alone in a dark wood (Ciardi 28).

"Lasciate ogne speranza, voi ch'intrate."

Dante Alighieri
Leave all hope behind all ye who enter here (Johnston 13).

> “In su l’estremità d’un’alta ripa che facevan gran pietre rotte in cerchio venimmo sopra più crudele stipa.”
>
> *Dante Alighieri*
> *On a steep precipice’s upper edge, In circle form’d by huge disjointed stones, We came upon a mass of deeper woe (Johnston 60).*

The legal team, stunned and in complete disbelief, asks, “Why so much?”

Circles 3 and 4: Gluttony and Abundance

The custodian explains the memorandum from the records manager that instructed everyone to save all email in accordance with a litigation hold. The accounting heads, desiring to ensure compliance with the memorandum and to save their jobs, took immediate and swift action. They instructed their staff to begin saving copies of all of their emails. The accounting staff began by saving .pst files onto their desktops and laptops, and when their drives filled up, they began printing their emails and storing the printouts in filing cabinets.

After printing over 200,000 emails, the accounting staffers exhausted the useable cabinet space. They contacted their desktop support technician, who instructed them to back up their email to the file server, and each person in the accounting department did so, every day, for the last year.

Circle 5: Anger

The accounting team is proud of its thoroughness. However, the legal team is angered and overwhelmed. “Where else is email being retained?” they ask. Disappointed by the legal team’s reaction, the accounting team resigns itself to the long hours that will be required to investigate the answer to this question.

The lower rings

Circles 6 and 7: Heresy and Disorder

The investigation yields some unexpected discoveries.

Because the file servers were never intended to be used in this way, they were full after a few months. When server administrators informed custodians that they needed to clean out personal disk space on the server, the custodians resorted to archiving their email data to personal USB memory sticks, zip drives and shared locations on other servers. Some had even sent copies of email to their personal accounts.

The server backup team, upon reading the memo, modified the tape backup schedule from weekly to daily to ensure a complete server image on a nightly basis. The tape rotation schedule and reuse of tapes was suspended and Dark Wood began shipping its email and file server backup tapes to an offsite storage facility for safekeeping.

Circle 8: Trickery

The internal capacity management team responsible for supporting the email and file servers routinely migrated data off the servers when disks became full. They would later delete previously migrated data if the owners did not request that it be restored after about a month. The team’s rationalization was there were plenty of backups on tape if a user really needed access to the data.

The final circle: Cocytus

Circle 9: Betrayal

Through generous and repeated backups, data copies and enthusiastic storage management practices of online and offline systems, media and even printing of hardcopy, these very creative and ambitious people at Dark Wood had gone to extreme lengths to ensure compliance with their preservation obligations. Unfortunately, they did so without an understanding of why or how they were to hold onto this data, and in their haste they proceeded to create a nightmarish scenario for the collections team. They had doomed that team to failure in its effort to locate, identify, collect and process this data into meaningful and useable formats for the attorneys to review.

The original two weeks turned into several weeks. Each member of the five-person collection team worked around the clock, extracting emails from backup tapes, servers, desktops and laptops, as well as collating and scanning paper printouts. The accounting and IT operations staff, as well as management, attacked them for monopolizing the systems, staff, office resources and tape restoration infrastructure. And the company's legal department condemned them for failing to deliver the information on schedule and for the numerous surprises and delays they've encountered along the way.

But Dark Wood's hell, paved with good intentions, had only just begun. The millions of documents obtained had to be processed for duplicates and loaded into a system for litigation review. This process took weeks and cost hundreds of thousands of dollars due to the many technical challenges caused by the multiple formats and inconsistent methods used to store and collect the data.

Dark Wood's attorneys may be required to defend the efficacy of the e-discovery, and its tale of woe is not likely to evoke confidence that due diligence and prudence were ever present.

The moral of the story

You should now understand why it is necessary to be prepared for litigation with good hold processes and collection procedures. You don't want people inventing processes for preserving or collecting data for litigation "on the fly"; without processes to handle preservation and collection, decisions made under pressure of litigation may seem reasonable at the time, but could prove to be disastrous. Dark Wood incurred many costs due to inefficient resource usage and failure to heed archival and storage best practices. There were also significant costs associated with business interruption and by the inefficient collection and processing of ESI. Dark Wood will incur even greater expense as it loads huge amounts of data into a system to be used for litigation review.

The most devastating costs, however, are those Dark Wood may incur as a result of its inadequate litigation hold strategy. In the story, emails were deleted, purged or otherwise lost after the preservation requirements were communicated. This fact is not to be taken lightly, as courts have little patience for spoliation of evidence when handling ESI during legal proceedings. Serious sanctions are imposed when a party fails to take the appropriate measures to preserve responsive ESI or delays in responding to e-discovery production requests. Acts of "good faith" after the fact to comply with e-discovery obligations may reduce the extent of sanctions, but the courts today are demonstrating less and less tolerance for ignorance.

For example, in a recent opinion, Keithley v. Homestore.com, Inc., 2008 WL 3833384 (N.D.Cal. Aug. 12, 2008), the court awarded sanctions to remedy the defendant's e-discovery misconduct. Defendants were on notice that documents relevant to this case should have been maintained pursuant to a litigation hold. See, e.g., Phoenix Four, Inc. v. Strategic Resources Corp., 2006 WL 1409413, *5-6 (S.D. N.Y. 2006) (stating that lack of a litigation hold can constitute gross negligence and can justify monetary sanctions). Yet according to testimony, Defendants engaged in a large scale transfer of source code to a new source code control system without taking adequate precautions to safely maintain the older information, which was plainly relevant to this litigation and should have been the subject of a litigation hold, leading to destruction of some source code in 2004. The facts—specifically that Defendants have no written document retention policy nor was there a specific litigation hold put in place, that at least some evidence was destroyed when the Development Computer failed, that Defendants made material misrepresentations to the Court and Plaintiffs regarding the existence of reports, and that Defendants have produced an avalanche of responsive documents and electronically stored information only after the Court informed the parties that sanctions were appropriate—show a level of reckless

> "Ben se' crudel,
> se tu già non ti
> duoli pensando
> ciò che 'l mio cor
> s'annunziava; e se
> non piangi, di che
> pianger suoli?"
>
> *Dante Alighieri*
> *Cruel thou art if thine eye be dry, Thinking on that which my sick heart foretold; And if thou weepest not, when dost thou weep? (Johnston 191).*

disregard for their discovery obligation and for candor and accuracy before the Court sufficient to warrant severe monetary and evidentiary sanctions.

In this case, the monetary sanctions awarded the plaintiff as a result of e-discovery misconduct may top $1 million, and the instruction to the jury regarding the duration of alleged infringement will unquestionably hamper the defendant's posture.

Since the basis behind developing a strategy to either defend or prosecute a claim is inherently about who did what and when, the information provided by e-discovery creates the foundation for a successful response to litigation. Having a litigation hold process that quickly communicates and provides actionable steps for custodians to take is crucial. The dynamic nature of litigation means that any changes to the preservation process must be clearly communicated to all stakeholders and thoroughly documented.

Business value, statutory and regulatory requirements must drive the definition and ongoing maintenance of your information management policies.

Best practices to avoid the e-discovery inferno

Establish an information management program

Being prepared to respond responsibly and efficiently to an e-discovery request goes beyond just preserving evidence; it begins with good information management. To borrow a mantra from Peter Lynch, a popular Wall Street investor: "Know what you own." Just as investors should know their portfolios in detail, organizations need to know what information they own, including all electronic data. They need to know where data is stored, who has access and control of it, its value, and, if there is no value, why it is being kept. They also need to determine its retention schedule. A data map and management policy that defines clearly all of these attributes and establishes a foundation for ongoing governance is paramount to being prepared for an e-discovery request.

Companies with no information management programs—or programs that do not sufficiently address the full life-cycle of electronic data—end up creating mountains of legacy data and media. Most of this data has no real business value, is free from any statutory or regulatory retention requirements, and is not subject to any legal preservation obligations.

Helpful tips for proactive e-discovery that complement best practices

Tip #1: Be prepared

Failing to prepare for the eventuality of litigation contributes to a lack of awareness throughout a company and limits the ability to meet litigation preservation obligations. This can be disastrous when litigation does occur

Tip #2: Know what you own

One man's trash is another man's money pit!

E-discovery can result in enormous amounts of data that must be processed and reviewed by paralegals and attorneys who charge by the hour. This is often the most costly part of an e-discovery project, and poor stewards of data exacerbate the costs. Raise awareness among your staff members and monitor their data habits. Ensure that data that doesn't provide business value—or that isn't subject to legal, compliance retention or preservation requirements—is disposed of quickly and properly

Tip #3: Involve the right people

A comprehensive information governance program needs to include ongoing participation of business leaders, IT operations and technology specialists, and legal and compliance authorities

What to include

Business value, statutory and regulatory requirements must drive the definition and ongoing maintenance of your information management policies. Since the content and context of information will vary among the numerous classes of electronic data, as will the relative value to each business area within your company, the program should account for this variation by ensuring complete representation by the business.

The program should contain a policy document that defines the various classes of data and their specific retention needs. It should answer the following questions for each class of data:

- Where and how is the data being stored? (e.g., WORM-compliant storage)
- Why is it being retained? (e.g., for business, regulatory or statutory compliance reasons)
- How long must it be retained?
- When should the data be destroyed?

Tip #4: Check and re-check.

Before beginning any new data disposal efforts, be absolutely certain that you hold and secure all data that may be potentially useful to any threatened, pending or active litigation or investigative matter, and be certain you have valid procedures for adding or removing holds as changes occur. The cost of overlooking this tip can be catastrophic

Tip #5: Don't panic

Decisions made in a panic are often poorly considered, so they can increase your liability and result in unanticipated e-discovery costs.

Tip #6: Establish email policy

Email is the most widely sought ESI in litigation. Establish a policy that defines appropriate usage and retention rules as well as procedures to fulfill litigation hold obligations against email. Wherever possible, use technology to automate compliance monitoring and enforcement of your email policy.

Whom to involve

A common mistake made when crafting an information governance and records management policy is failing to involve and gain acceptance from all business areas when evaluating the value of the information. Otherwise, your information policy will be incomplete, hinder the business and ultimately fail.

An effective program should involve business leaders with knowledge about the data and its value, records management personnel who will administer the program and technology experts and IT operations personnel who have direct impact on information management. In addition, legal and compliance specialists should participate to ensure qualified representation of statutory or regulatory retention and litigation preservation requirements.

Best practices

Best practices for a good information management program include the following:

- Creation and ongoing upkeep of a complete data map with a full accounting of all repositories, media and systems owned and controlled by the company.
- Retention of data subject to any legal or contractual obligations for the appropriate length of time in the appropriate manner.
- Retention of data with legitimate business value. Failure to retain and maintain access to useful data incurs litigation risk. On the other hand, retaining data that is not subject to any legal or contractual retention requirements can also be a liability, from both a monetary and litigation risk perspective.
- Authenticated access to data by people and systems. People or systems access to data needs to include proper authentication measures to ensure all data access is predictable, controlled and auditable.
- Tested and validated litigation hold procedures to ensure that any potentially

An effective program should involve business leaders with knowledge about the data and its value, records management personnel who will administer the program and technology experts and IT operations personnel who have direct impact on information management.

responsive information is not deleted, overwritten or otherwise modified when a litigation or investigation occurs or is anticipated.

- Tested and validated procedures for the ongoing disposal of remaining data that is not subject to any of the preceding statements.

Choosing the right software solutions

The right software tools can drive down the cost of e-discovery. Choosing the right tools requires understanding where your email data is stored.

Determining where email is stored

The right software tools can drive down the cost of e-discovery. Choosing the right tools requires understanding where your email data is stored. If you don't have an email archiving solution, your email is likely stored in the following places:

Email stored on backups

Historical emails are typically stored in offline backups on tape, disk or image. Companies are often required to search backed up email data and export it for evidential review. A good solution will make this process quick and simple in order to support the stringent timeframes of the e-discovery process.

Email stored on production Exchange server

Current emails are often stored on the Exchange server. Although newer versions of Exchange have the ability to search for emails, it is still difficult to search for and export specific emails. Moreover, single-instance storage was removed in Exchange 2010, so it takes longer to search through the results because you need to weed through duplicate messages.

Email stored in personal storage files

PST files have been a long standing problem for most organizations. PST files are stored in many locations, such as users' desktops, laptops, file servers and external drives. They are a nightmare to manage and an even bigger nightmare from which to discover email. It is a good idea to move PST files into a central location for easy discovery. PST files can be moved and single instanced into an email archiving solution, which will make them more discoverable.

Choosing an email archiving solution

Email archiving solutions are a great way to manage your email. Be sure to look for the following functionality:

- Email retention periods – A good email archiving solution will automatically keep what you want and remove what you don't want.
- Legal hold – As we saw earlier, it is not ideal or realistic to depend on users to archive email pertinent to a lawsuit. Emails are missed and there is no central location to store all the emails for a long period of time. A good email archiving solution will not only have a legal hold option for all or a particular set of users but it will single instance that data down to the attachment level. That way, you are able to retain more data longer, and when it comes time for e-discovery, legal staff is not overwhelmed by duplicate and irrelevant content.

Dell Solutions

Dell offers two solutions that can help: Archive Manager and Recovery Manager for Exchange.

Archive Manager

Archive Manager is email archiving software that captures, retains, preserves and searches for email. Archive Manager captures a single instance of each email message, applies granular retention and disposition policies and offers powerful search to quickly retrieve data to satisfy legal requests. Archive Manager ensures that email will be available when needed, without creating a storage or performance burden on your servers.

In addition, with Archive Manager you can quickly produce evidence for audits, investigations and litigation. Its tamperproof email repository keeps only relevant email. Content can be tagged and categorized to accelerate the discovery process, and granular permissions enable authorized users to retrieve items from particular mailboxes, or across the entire archive. Retention policies can be created using complex queries or message tags. These policies can be applied to a mailbox, mail store, group, organization unit or the entire archive. Furthermore, a legal hold state can be applied to Archive Manager which prevents any messages from being deleted.

For more information, visit: quest.com/archive-manager.

Recovery Manager for Exchange

Recovery Manager for Exchange makes discovering and recovering business-critical Exchange data fast and easy. It helps you meet SLAs as well as fulfill your email discovery obligations for legal inquiries or internal investigations. You can restore individual, message-level items from regular Exchange backups, un-mounted .edb information stores and Lotus Domino .nsf files without setting up a dedicated recovery server. And you can selectively retrieve only the data that is needed rather than all data from a server, database or file.

Recovery Manager for Exchange helps accelerate discovery by finding and retrieving message-level data from PSTs, mailboxes, public folders, single or multiple stores or Lotus Domino. You can search based on sender, recipient, date, attachment type, subject, message keyword or attachment keyword and compare the contents of an online mailbox with a backup mailbox to identify any differences. More than 85 percent of corporate email data is found within attachments, and discovering this data is crucial to any operational or compliance-driven recovery effort. It helps to reduce recovery costs by eliminating the need for brick-level backups and used in combination with most other backup and CDP solutions, alleviating the need to maintain costly recovery environments.

For more information, visit: quest.com/recovery-manager-for-exchange.

Conclusion

A good information governance program and sound e-discovery strategy provides a foundation for identifying where, why and how potentially relevant ESI exists. You can avoid a journey to the e-discovery netherworld and ensure predictable, repeatable and defensible preservation of ESI by:

- Creating and maintaining a comprehensive

Archive Manager captures a single instance of each email message, applies granular retention and disposition policies and offers powerful search to quickly retrieve data to satisfy legal requests.

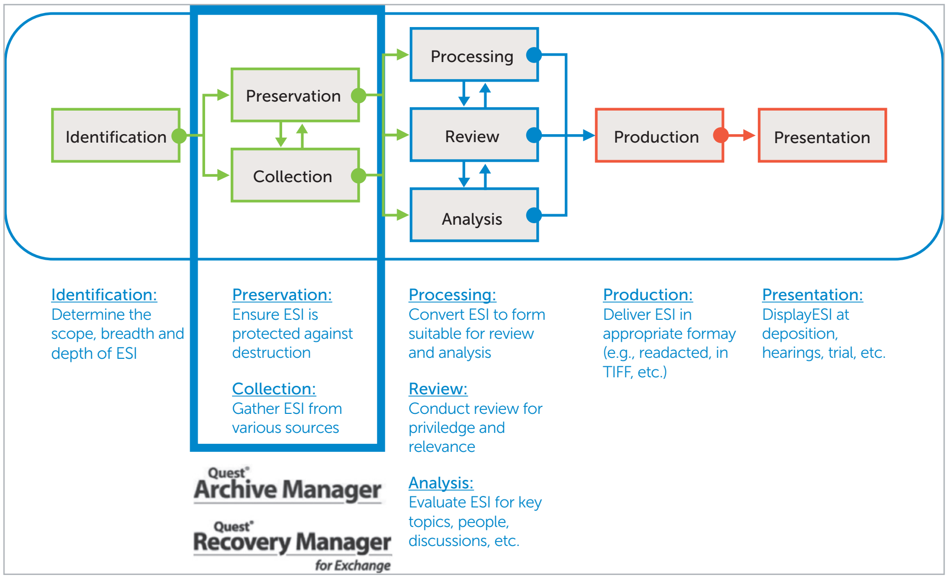
Identification
Preservation
Collection
Processing
Review
Analysis
Production
Presentation
Identification:
Determine the scope, breadth and depth of ESI
Preservation:
Ensure ESI is protected against destruction
Collection:
Gather ESI from various sources
Processing:
Convert ESI to form suitable for review and analysis
Review:
Conduct review for priviledge and relevance
Analysis:
Evaluate ESI for key topics, people, discussions, etc.
Production:
Deliver ESI in appropriate formay (e.g., readacted, in TIFF, etc.)
Presentation:
DisplayESI at deposition, hearings, trial, etc.
Quest® Archive Manager
Quest® Recovery Manager for Exchange

Figure 1. Dell tools help collect and preserve relevant email data, as a critical step in all five phases of e-discovery.

data map with a full accounting of all data repositories, media and data systems owned and controlled by the company.

- Retaining data subject to any legal or contractual obligations for the appropriate length of time in the appropriate manner.
- Retaining all data with legitimate business value, and only that data.
- Ensuring authenticated access to data by people and systems. People or systems access to data needs to include proper authentication measures to ensure all data access is predictable and controlled and auditable.
- Establishing and testing litigation hold procedures to ensure that any potentially responsive information is not deleted, overwritten or otherwise modified when a litigation or investigation occurs or is anticipated.
- Establishing and testing procedures for the ongoing disposal of remaining data that is not subject to any of the preceding statements.

The cost of being a good data steward is easily justified by the savings in the efficient utilization of IT resources, but the real savings are avoiding the costs you will incur if you don't establish a solid collection and litigation hold strategy.

Heed these best practices well, or risk burning in the e-discovery inferno!

Works cited

Alighieri, Dante. The Inferno. Translated by John Ciardi. New York: Penguin Books, Ltd., 1982.

Alighieri, Dante. A Translation of Dante's Inferno. Translated by David Johnston. Oxford University: Printed at the "Chronicle" Office, 1867. Digitized April 13, 2007.
Accessed at http://books.google.com/books?id=ZY0HAAAAQAAJ.

About the authors

Keri Farrell is a product manager at Dell, where she is responsible for global e-discovery and recovery strategy for messaging and unified communications systems. Keri has worked in IT for 12 years and specializes in Microsoft Exchange and legal discovery pertaining to email systems. Prior to joining Dell, Keri got substantial hands-on industry experience at Microsoft, Iron Mountain, Boston Scientific and Safety 1st. At Microsoft, Keri served on the Exchange PSS team focusing on database recovery technologies. With Iron Mountain, she assisted Fortune 500 companies archiving to the Iron Mountain Digital Archive, and played a key role in developing policies and solutions for high-volume recovery from tape backup, email record definitions and journaling configuration.

Keri has authored numerous technical publications on legal discovery, recovery, archiving and enterprise data protection. Currently based in the Boston area, Keri holds a bachelor's degree in business administration with a concentration in computer information systems from Bryant University in Smithfield, Rhode Island.

Kyle Hetherington is an independent e-discovery consultant with more than 20 years of experience in global enterprise IT operations in financial services, enabling him to gain specialized knowledge and experience in e-discovery and litigation technology. Kyle previously worked for John Hancock, State Street Research and Management and Fidelity Investments. As a senior manager of Fidelity Investment's Electronic Communications Retention, Response and e-Discovery Services Team, Kyle led an e-discovery practice comprised of case project managers and evidence collection analysts responsible for performing identification, collection, preservation, culling, litigations review hosting and production of evidence for litigation, regulatory agency inquiry and investigation.

Kyle earned a Bachelor of Arts degree in business administration with a concentration in management information systems from Saint Leo University in Saint Leo, Florida, and is a member of the Delta Epsilon Sigma National Scholastic Honor Society.

For More Information

© 2013 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. (“Dell”).

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.