

Module 13: Production and Presentation of Electronically Stored Information

Learning Outcomes

Upon completion of Module 13, students will be able to:

- Justify the format that has been selected for production of electronic evidence as part of an e-discovery process.
- Compare and contrast the various technologies and approaches for producing electronic evidence.
- Assess the contents of a comprehensive report on the activities undertaken as part of an e-discovery process.
- Recommend some approaches for helping an expert to prepare for being deposed or testifying in court.
- Identify software, vendors, forms, templates and other resources that can be helpful in an e-discovery process.
- Summarize the important points in Module 13 and the reading assignment.

Please read Chapter 7 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed.

Please also read the following, included as part of Module 13.

- Chapter Eleven in *Electronic Discovery for Small Cases* introduces us to a simple solution we can use for producing ESI, called dtSearch Publish - http://www.dtsearch.com/plf_publish_2.html
- Discovery Project Management Template
- E-Discovery Production Steps – from *Using Computers in the Law Office*, 7th ed.
- Search & Collection, Corporate In-House E-Discovery Workflow – from Exterro
- Yesterday's Technology, Today's Problem – from *ABA Journal*

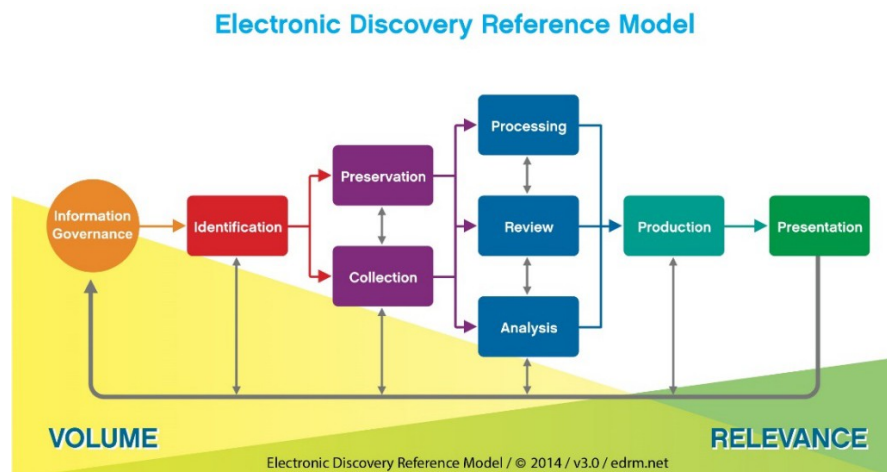
By Sunday, November 24 by noon, please respond to the questions for Discussion Forum #7 (covers Modules 12 and 13):

- What are some of the benefits and challenges with predictive coding, as illuminated in the webinars from ILTA? Find a recent case through K&L Gates or Exterro that discusses predictive coding or technology-assisted (TAR) or computer-assisted review.

Provide the citation to the case and a brief summary of the court's view about the use of this technology.

- Which of the steps in e-discovery (using the EDRM) do you find most interesting or compelling? How can technology assist with this step? How does this technology reduce the potential risks of this step in an e-discovery process?
- Of all of the software tools that we have covered in the reading assignments for Modules 12-13, which do you find the most intriguing or helpful? What is the particular focus of this software (which step or steps within e-discovery)? What are its strengths and weaknesses?
- What strategies do you use for preparing for public speaking activities? How have you improved your skills or confidence in public speaking? Have you had to testify in court or give a deposition or assist someone else with these activities? If so, please describe.
- Please **REPLY** to another student who participated in the questions for Discussion Forum #7. What strategies does this student use to prepare for public speaking activities and how has he/she improved his/her skills and confidence? What other suggestions would you provide to this student?
- Any other surprising or interesting points from Module 12, Module 13 or the reading assignment.

Please read the following mini-lecture.



With Module 13, we move into the production and presentation steps in an electronic discovery process, bringing us to the end of the EDRM. It is helpful to visualize these steps using the EDRM, which we were introduced to earlier in the semester. Recall that Module 9 was devoted to information governance/litigation readiness, Module 10 covered collection of electronically stored information and Module 11 examined how to preserve electronically stored information. Module 12 covered processing, which includes analysis and review. By this point, the volume of electronic evidence that we have to produce to the opposing party and what we want to present as part of our case in court has decreased markedly and we should only be dealing with evidence that is truly relevant.

Chapter Eleven in *Electronic Discovery for Small Cases* introduces us to a simple solution we can use for producing ESI, called dtSearch Publish.

Chapter 7 in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. is quite short and I hope that no one minds a less robust reading assignment for Module 13! As the author indicates on page 255, in Chapter 7, he will discuss the reasons and methods for sharing the data that we have so carefully collected, preserved and managed. There may be different approaches and procedures that will be appropriate to the specific needs of the situation. These approaches and procedures will include the format in which the data are produced, the content, the timing of release, the actual physical media and the delivery of the electronic evidence (see Figure 7.1).

As indicated on page 255, “[o]ne of the first considerations in sharing the data you have collected will be in what format you want to produce the data.” The author contrasts the approach to delivering information to friends and relatives versus to the IRS or other taxing authority as part of an audit, wherein the taxing authority is likely to provide specific instructions about format and metadata. However, this course is about e-discovery and thus the information about how to produce data for litigation on pages 257-258 is of greatest interest. As anticipated in the FRCP, the “meet and confer” conference should have provided an opportunity for the lawyers not only to indicate the electronic and physical evidence they wanted to receive, but also the format for that evidence. In nearly every case, parties will want the electronic evidence in native format with metadata intact. As we have already learned, special challenges may arise when we are working with older and obsolete media and with data that has been created and stored through a proprietary database. The author observes that it can be a daunting task to obtain relevant electronically stored information that will stand up to evidentiary requirements, so it is especially important to be aware of the issues at the beginning of the case. As the author suggests on page 258, it may be to everyone’s advantage to create different data formats in order to ensure that the evidence is consistent, not compromised in any way and can be used most effectively and easily by all parties. Fortunately, as the e-discovery industry matures, there are more products from vendors that facilitate the production of electronic evidence.

As stated on page 259, “[t]he actual physical or logical medium used to transfer produced electronic data will depend on both the goals of the producing parties and any agreements made between them.” As shown in Figure 7.3, electronic evidence can be copied onto many types of physical media, such as DVDs, CDs or USB drives, as long as the copying is done in a forensically sound manner that ensures the integrity of the evidence. The author offers a process for ensuring forensically sound copying on page 259.

- Create and document at least two different hashes of the data before and after copying.
- Maintain a chain of custody, documenting where the data were originally, who was the custodian, who copied the data, when, and for what purpose.
- Document the tools used to copy the data, including their version numbers.

Appendix II includes some sample logging and chain of custody documents. If data is transferred

using email or an online service, the author suggests ensuring the integrity of the data by using hashes and maintaining good logs for all activities involved in copying the data. If email is chosen as the means of transferring data, the data should be classified and we should consider encrypting email and documents. Encrypting documents can be accomplished with common tools, such as those that are listed in Appendix III. If you decide to use an online service, the author recommends that the provisions described on page 260 be included in the contract with the service provider. He asserts that these provisions are paramount to ensuring that the data is there when we need it and that the integrity of the data is assured. As he observes on page 260, the most important considerations will always to be ensure the integrity and availability of the data.

Another aspect of the production step in an e-discovery process is the need to create reports that are understandable, concise and complete (see Figure 7.4). Of course, the first step is to keep excellent records of everything you do with respect to the data in question, including a records retention policy. (Recall Prof. Berry-Tayman's article from Module 9 about law firms being the weak link in a client's information governance/e-discovery process.) This should include a record or log that illustrates compliance with this policy, such as where and how the data are preserved and the process for archiving and/or destroying the data according to documented and audited schedules. Recall from previous Modules and recent cases that the court will look at an organization's practices, not its policies.

Next, we will carefully log any and all activities undertaken to locate, collect and preserve any potentially relevant electronic evidence. The author provides a list of the documentation needed on page 262. If electronic devices or systems have been analyzed, you should log every step of the investigative process, including time, date, tools and results. (This will be part of the report that a digital forensics expert will provide.) The author describes an easy way to do this in Windows using "notepad" on page 262. We may need to gather system or database event logs, ingress and egress records, application logs, metadata and other detailed information that is related to the data. From here, we will prepare a report that is appropriate to the audience, avoiding as much technical jargon as possible. The resources in Appendix I may be helpful as will reviewing the previous chapters of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. The author advises us to check spelling and grammar and review the report to make sure it is clear and covers all of the important information.

On page 264, the author asserts that one of the most challenging and rewarding activities that might present itself to someone who becomes an expert in electronic evidence is the opportunity to share this knowledge as part of litigation (see Figure 7.5). This may range from assisting lawyers or management in understanding the electronic evidence that has been handled during an e-discovery process and all of the details and issues that are part of this process. However, experts may be required to participate in depositions or to testify in court.

The author offers additional suggestions on pages 265-266, including:

- Make sure that you understand your audience.

- Have all of your information nicely organized and ready.
- Be concise.
- Ensure that you will be able to answer any questions by meeting with the lawyer beforehand.
- Only answer the questions that you are asked – see page 265. This is a common problem with witnesses, but which should be avoided for the reasons discussed by the author.
- It is better to indicate that you don't know an answer or have provided all the information you have than try to provide an answer about something you are not sure of.
- Take the time to review all of your data and go over possible issues with the lawyer beforehand.
- Consider a mock deposition or trial. (There are jury research companies that will provide this kind of service.)

As indicated on page 266, there are specific rules and protocols for expert witnesses and evidence. (Recall the supplemental materials included with previous Modules.) Other advice from the author is to be honest, prepared, respectful, polite and appropriately dressed and to speak clearly. As he notes, the more prepared you are ahead of time, the less nervous you will be in the actual presentation, deposition or testimony.

Appendix II in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. provides a number of helpful forms and guides:

- Chain of custody form – see page 273.
- Confidentiality Agreement – see pages 274-275.
- A pre-acquisition planning meeting form – see pages 276-277.
- A final investigation report – see pages 278-279.
- A sample log file (from Notepad) – see page 280.
- An investigation request – see page 281-282.
- A sample statement form – see pages 283-289.

Please be sure to review the list of links and references in Appendix I and the links to technical software solutions in Appendix III.

Next Steps

With Module 14, we will consider one of the hottest topics in e-discovery, which is e-discovery of social media.

Please let me know if you have questions about Module 13 or the reading assignment.

SHARING IS GOOD

Dissemination and Reporting

7.1 Introduction

In this final chapter, we will discuss the reasons and the methods for sharing the data we have so carefully acquired, preserved, and managed. There are several reasons that we will consider, and each may engender different approaches or procedures appropriate to the specific needs of those situations.

These approaches will include the format in which the data are produced, the content, the timing of release, and the actual physical media and process for delivering the electronic information (Figure 7.1). We also discuss reporting protocols and suggest some ideas to ensure that the reports you create are clear and concise.

Finally, we end this chapter with some tips for participating in depositions or as an expert witness.

7.2 Format Issues: Original or Usable?

One of the first considerations in sharing the data you have collected will be in what format you want to produce the data.

Think about it in terms of your reasons for producing the data in the first place, and this should guide you in your formatting decisions (Figure 7.2). For instance, one reason for producing data is for dissemination to colleagues, relatives, or friends who simply have a nonadversarial interest in the information. In that case, there is little likelihood of their using the data or its metadata in any way that would be harmful to your interests. There will also be no legal or regulatory rules compelling you to ensure the integrity of the data.

If that is the case, you might simply create copies of the pictures, documents, spreadsheets, and so forth, and send them via standard

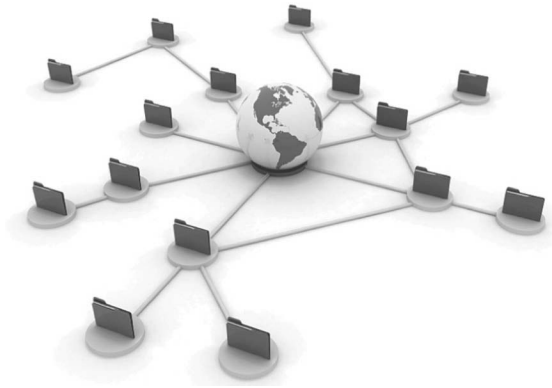


Figure 7.1 Consider the procedures that you will put into place for disseminating the evidence you collected.



Figure 7.2 The format of the evidence you produce should be decided early on.

e-mail, mail them on a DVD, or store them online on a file sharing tool. You have no responsibility to ensure the data are secure and uncompromised. You do not need to be concerned about what metadata are attached to the data as it is very unlikely that any of those people will even know or care about its existence.

Another reason for producing data could be for a tax audit required by the Internal Revenue Service (IRS) or other taxing authority. You might consider this a somewhat more adversarial situation, and you are legally required to produce any and all relevant records and to be able to prove their integrity. It is unlikely that the IRS would require specific metadata, but if questions arise about the integrity of your records, you could be required to prove the legitimacy of those records. That proof is likely to be enhanced by your ability to refer to metadata and to your careful data handling processes. If this is the case, you will most likely be creating copies of documents, spreadsheets, and so forth, with accompanying metadata or other means of proving their integrity as we discussed earlier (e.g., hashing).

The IRS or other legal auditing authority will be specific about the format in which they expect your documentation to be delivered. It will be to your advantage to not only comply with those requests, but to do all you can to ensure good procedures and data management, including chain of custody and data security practices. That will allow you to address any issues of data integrity with well-documented management practices.

Another likely scenario is the need to produce data for a legal matter. For the most part, as we discussed in Chapter 1, a meeting will be conducted between the parties to discuss the data that will be produced. In that meeting, your legal counsel will make decisions with the other side about specific electronic and physical evidence required to adjudicate the case. The sides will agree in what format they want the evidence produced.

In some cases, they will decide that they want the data produced in its original format, including all metadata. Or they might decide that graphic copies such as TIFF files are appropriate. If that is what they decide, they might also ask for graphic copies of metadata for each file, or they might not require metadata.

Depending on the specific types of data, producing them in original format can have advantages and disadvantages. For instance, if the

original data were in a Microsoft Word file, that is relatively common and most organizations will have the applications and tools to be able to read both the document and its attached metadata. Therefore, as long as you are careful not to compromise the document when you transfer it in that Word document format, it will be a simple and relatively secure production of the electronic evidence.

However, if the original data were stored as a Lotus 123 spreadsheet created many years ago, it may be very difficult, first to preserve any metadata when you produce the copy, and second for the recipient to open it with current existing tools. The recipient might also have a hard time being able to access the metadata without specialized tools.

This becomes even more difficult when the original form of the data is in a proprietary database. Database applications can be expensive, and data stored therein might be difficult or impossible to extract or even to view. Without having the correct version of the database software (including required licensing), specific information about the design of the original database, and expertise to re-create the original database architecture, it might be impossible to actually view data in the original context.

All that said, it can be a daunting task to be able to actually gain relevant electronic evidence that will stand up to evidentiary requirements in court. The most important thing that you and your legal counsel can do is to be aware of these issues up front and be specific when requesting data from the other parties during your pretrial meetings.

Being aware of these issues as they relate to your own data will also help to inform you and your legal counsel as to your capabilities for producing relevant electronic evidence in either its original format or in some other format that might be requested.

At times, it may be to everyone's advantage to create different data formats in order to ensure that the evidence is consistent, uncompromised in any way, and most effectively and easily used by all sides. The sides might decide to have all evidence stored in a database online so that it is accessible by all concerned. There are some new online services that offer that possibility.

In the end, it is most important to consider the goals of everyone involved for the production of the data and find the most efficient and effective method to accomplish those goals.

7.3 Mediums for Transfer

The actual physical or logical medium used to transfer produced electronic data will depend on both the goals of the producing parties and any agreements made between them. In many cases, electronic evidence can be copied onto physical media such as DVDs, CDs, tape, or USB devices such as hard drives or flash drives. As long as this copying is done in a forensically sound manner that ensures the integrity of the data, that should be sufficient for most situations (Figure 7.3).

The ways you can ensure a forensically sound copying of data to these media are as follows:

- Create and document at least two different hashes of the data before and after copying (see Chapter 5 for more details).
- Maintain a chain of custody, documenting where the data were originally, who was the custodian, who copied the data, when, and for what purpose.
- Document the tools used to copy the data including their version numbers.

Appendix II includes some sample logging and chain of custody documents.

In other cases, the parties involved might decide on transferring the data using e-mail or an online service. In these cases, you can ensure the integrity of the data by using hashes and maintaining good



Figure 7.3 The type of media on which you store or deliver the evidence will depend on many factors.

logging of all activities involved in copying the data. This should be agreed upon up front between all of the parties.

If you decide to use e-mail as a means of transferring data, you should consider the classification of the information. If it is sensitive in any way, you should look at the possibility of encrypting the e-mail transmissions or possibly encrypting the documents. Most e-mail applications have the capacity to encrypt their contents, or there are third-party add-ins that will allow you to do so. Encrypting the documents or other evidence can also be accomplished with commonplace tools, several of which are referenced in Appendix III.

Should you decide to use an online service, you should ensure that the service provider contract includes the following:

- Information security policies that address the confidentiality of your data, its availability, and its integrity
- Backgrounding of its employees who will have access to your data
- Well-defined procedures for access to the data
- Defined and practiced authentication protocols to ensure data are accessed only by those with the correct and current rights
- Disaster recovery and business continuity policies and practices that are both well documented and auditable
- 24/7/365 access to support and priority assistance
- Effective and timely notification procedures in case any issues affect the confidentiality, integrity, or availability of your data
- Data management, access, retention, and archiving procedures that meet your requirements

These contractual requirements are important in any service that you use online, but when you decide that this is how you are going to disseminate legally relevant electronic evidence, they become paramount to ensuring your data are there when you need them, and that the integrity of the data is unsullied.

Whatever medium makes the most sense to achieve the goals of sharing your data with another party, the most important consideration will always be ensuring the integrity and availability of the data to all concerned. As you consider which solution makes the most sense, always keep this in mind.

7.4 Creating Readable Reports

As the person in your organization who has taken on the task of learning about electronic evidence, or just due to your interest in better managing your own data, you may be in the position to create reports in this regard. These might include data management and retention reports, audit information, or evidence investigation and acquisition reports.

One of the most important things you can do for the sake of your audience is to create reports that are understandable, concise, and complete (Figure 7.4).

The first step in ensuring that your report is complete and contains all of the relevant information is to keep excellent records of everything you do in relation to the data in question. The foundation of that record keeping and of your eventual ability to document your actions will always be a good records retention policy. That policy means little or nothing if it was not properly disseminated and carefully followed by you or your organization.

Beginning with your records management policy, you should have some record or log that illustrates your or your organization's compliance. It should document how you follow the correct records management procedures, where and how the data are preserved, and your process for archiving or destroying the data according to your documented and audited schedules.

Next, you need to carefully log any and all activities undertaken to locate, acquire, and secure any relevant electronic evidence. Using



Figure 7.4 Clear and concise reports will make all the difference.

the samples we give you in Appendix II, or something similar that is appropriate for your organization, you should carefully document all of the following:

- The owner(s) and custodian(s) of the data in question
- The physical and logical locations of the data
- The tools and methods used to acquire the data, including names and versions of acquisition applications and types of hashes or other integrity assurance tools used
- The time and date of acquisition
- The movement of data to or from any type of storage (chain of custody), including who moved it and why
- The security procedures, both physical and logical, used to ensure the data could not have been compromised or accessed by anyone without the correct authority
- The physical and logical medium on which the data is stored or transferred to or from, including the name or type of media and a unique identifier such as a serial number, model number, or label

If you are investigating or analyzing electronic devices or systems to find relevant evidence, you should also log every step of your investigative process. You should include the time and date of each part of the investigation as well as the tools you used and the results of your analysis.

There is an easy way to do this if you are using the Windows operating system. Every Windows OS includes a simple text application called “Notepad.” Start up Notepad and create a new file with the first line: ‘LOG’ (without the quotes) and then close the application. Then when you open it up again it will “automagically” insert a date and time stamp.

I have all of my investigators use this simple tool to log every step of their analyses of devices for forensics investigations or acquisition of data for e-discovery. As they are working they simply open the file, note everything they did, the tools they used, and the results and then close the file again. By doing this we get a nice time-stamped record that is extremely useful in depositions or court appearances by assisting in our recollection of what we did in an investigation.

Depending on the physical and logical location of the evidence in question, you may also need to gather up system or database event logs, ingress and egress records, application logs and metadata, or other detailed information related to the data in question.

Once you begin your reporting process by gathering or creating all of the documentation above, your next step is to winnow it down to the important information for your intended audience.

Take the time to understand who that audience will be and their level of expertise. For instance, perhaps you are creating a report to present to your manager who has a very good understanding of the technical details and language related to the electronic data. In that case, you can use known acronyms and more technical language to describe the work you did, what you found, how and where it was acquired and preserved, and so forth.

However, if you are creating a report to be used in court or for an auditing authority, you should avoid the use of technical terms or acronyms. Instead, create a document that you could easily explain to your grandmother. In Chapter 2 we discussed in detail the idea of translating geek. This is where this skill is most important.

If you need to explain a technical process, try to come up with simple and easy-to-understand metaphors or examples. In Appendix I, we offer some great resources that explain how technical things work in easy-to-understand language.

Should you need to create a report explaining something technical such as how Internet information is stored on a computer, or how data can be fingerprinted using hash algorithms, I recommend reviewing sections in this book that address those ideas or taking the time to research some of the resources offered in Appendix I. These can give you great ideas of ways to make these technical details understandable to people without a technical background.

When creating a report, always begin by having all of the information you need, then consider your audience and tailor your presentation to their level of understanding. In every case, you want to be sure all of the important points are covered while not digressing into information that is not important, not required, or simply too esoteric or technical for the audience.

Very few jurists, judges, or lawyers have studied computer science, so they will neither appreciate nor understand your in-depth

explanation of the advantages of the latest version of Linux over the Windows operating system, for example (unless that is germane to your analysis of the evidence).

With written reports, be sure to do a good spell check and reread the report to ensure it is clear and covers all of the important information. There are sample reports in Appendix II.

If you are presenting an oral report, it is important to be comfortable with public speaking. We discuss that in the following section.

7.5 Tips for Depositions and Expert Witness

One of the most challenging and also most rewarding activities that might come from your having used this book and other resources to become an expert in electronic evidence will be the opportunity to share your knowledge as part of a legal matter (Figure 7.5).

This might take the form of simply assisting your legal counsel or your management in understanding the relevant electronic evidence and all of the details and issues that we discussed in this book. In that case, you will probably be dealing with one or only a few people at a time, and it should not be too daunting. Having done a great job in creating the written report as we discussed above, you will simply need to help them understand all of the pertinent details.

However, should you be called upon for a deposition or as an expert witness in a court case, or asked to present your findings to a larger audience, that can be a frightening proposition for some people. The first recommendation I would make is to spruce up your public



Figure 7.5 Delivering your information in court or a deposition can take some special skills.

speaking skills. There are classes and organizations available, some of which are referenced in Appendix I, which can help you with speaking and presentation skills and practice sessions. There are also some online resources with good ideas for creating presentations.

The same ideas apply here as with a written report. Make sure you understand your audience and have all of your information at hand. The actual information you present will depend on the specific requirements and level of expertise of your audience. However, I recommend bringing along any logs or other documentation that you might be questioned about as reference for yourself.

Be concise and ensure you are able to answer any question that might be asked of you. It can be very valuable to sit down with your legal counsel and rehearse possible questions and answers that might be brought forward during the case or deposition.

An important caveat, especially in a court setting, is to only answer the question you are asked. It is not your job to try to figure out what else the questioner might want to know, or to give details that were not specifically requested. It is a common mistake for someone in the witness stand or during a deposition to try to be helpful and to expound on their deep knowledge of a subject without having been asked. This might confuse the actual issue or give opposing counsel information that is not relevant or might even be used against your side. It can lead to your counsel's inability to control the case to their advantage.

Another important tip for appearing in court: Do not allow your questioners to paint you into a corner by insisting on an answer. It is perfectly legitimate for you to reply that you do not know an answer, or that you have provided them with all the information you have. It is a relatively common tactic to try to get the answer they want by insisting that you tell them, "Yes" or "No," or give some other response that leads to the conclusion they want. You can usually avoid this trap by being very careful to answer only with what you know for sure and being ready to say, "I don't know."

Take the time to review all of your data and to go over the possible issues with your own legal counsel beforehand. A mock deposition or trial rehearsal is a great idea if you have the time. It can help to bring up any areas where you might need more information or research. It can also be a way for you and your legal counsel to decide

what information is truly relevant and what might be privileged or unnecessary.

Finally, remember that there are specific rules and protocols for expert witnesses and evidence. We discussed those in more detail in Chapter 1, and your legal support will understand and apply those rules as appropriate.

Your responsibility is to be honest, prepared, and respectful. That will mean dressing appropriately, speaking clearly, and being polite and respectful to everyone present. The more prepared you are ahead of time, the less nervous you will be in your presentation.

Presenting to any audience, whether a group of managers, attorneys, a judge and jury, or any other group can be intimidating. However, if you are prepared, have practiced, and have taken the time to hone your presentation skills, you will come off as knowledgeable and reliable.

If it is your job to assist your side of a case, everything might depend on the impression you make. A confident, well-spoken, and clear speaker will be much more believable than someone who is reserved, nervous, and difficult to understand. Even if that nervous person is telling “the whole truth and nothing but the truth,” he or she is much less likely to be trusted by a jury or any other audience.

7.6 Conclusion

Well, you made it through to the end. I hope that whether you used this as a reference and skipped around, or worked your way through all seven chapters, you have found this useful in helping to better understand and manage electronically stored information.

The appendices that follow offer many resources for learning more or for further enhancing your understanding of this important subject.

By taking the time to read this book and to better understand these ideas, you have become a more unique and valuable person than you already were, whether just for your own knowledge or for the betterment of your organization. I encourage you to keep learning and to pass on this knowledge to ensure that more people are aware of the data fog we all live in today and all of the important means we have to manage and control that electronically stored information.

CHAPTER ELEVEN

A Simple Solution for Producing ESI

A GREAT DEAL OF attention is paid to the collecting, processing, and reviewing of ESI. Much less attention is given to the production of the results of such efforts, particularly when you are looking for an easy-to-use tool that can create a set of documents that can be viewed and searched by anyone. If the intended recipient of these electronic files has no litigation support program available, what can you do to provide deliverables that are immediately usable? dtSearch Publish is a tool that lets you quickly publish a document collection to a CD, DVD, or portable hard drive that is instantly searchable by the recipient using dtSearch Publish's powerful search engine technology. What is more is that the recipient does not even need to have dtSearch Publish installed on his or her computer to be able to use it to search the documents on the CD, DVD, or external memory device you provide. The search capabilities are automatically built into the CD, DVD, or hard drive, requiring no software installation on the recipient's hard drive.

dtSearch Publish

To create your dtSearch Publish collection on a CD, DVD, or external hard drive, a simple wizard is used. See Figure 11.1. All you need to do is follow the steps and you will easily create a usable end product. Click on the "New CD" button on the wizard to designate a master folder on your hard drive to hold the files until they are burned to CD, DVD, or external drive. Once you have created the target, add the documents you want to produce. You have the option of adding individual files using Explorer to copy the files into the documents folder or to copy items in bulk using the "Add Folder" command. See Figure 11.2.

Figure 11.1

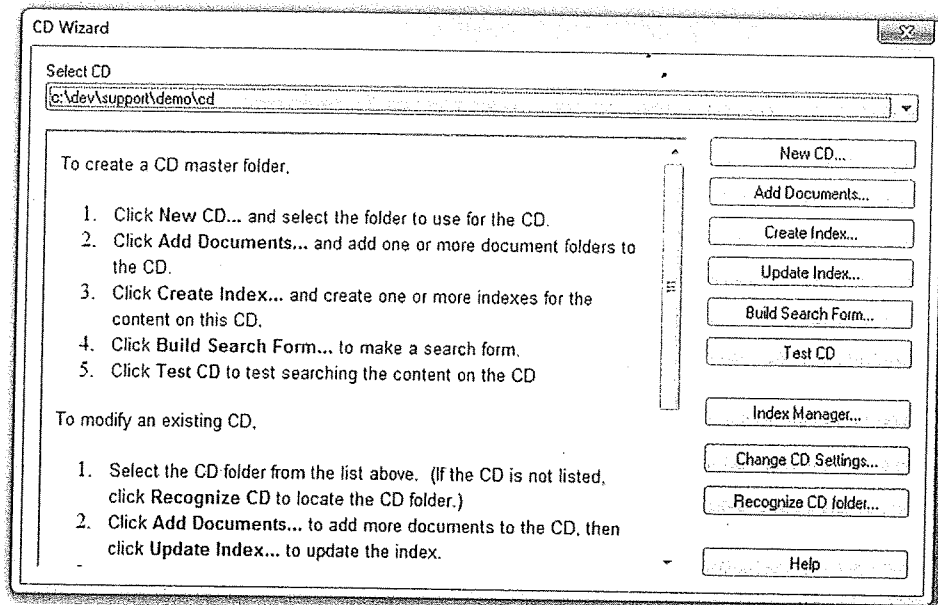
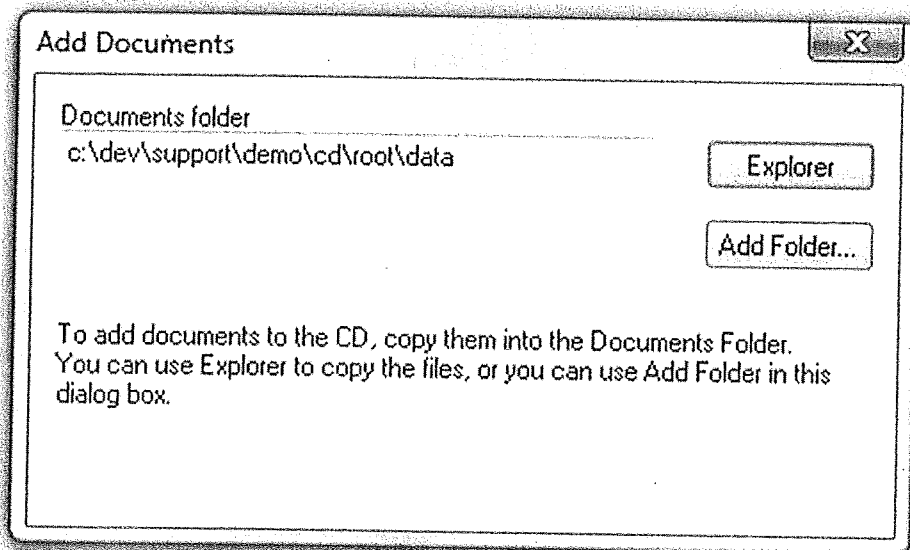


Figure 11.2



Once you have added the documents you want to produce, it is necessary to create an index. When you click on the "Create Index" button, you must name the index file, specify a location for it to be created, and then decide whether a summary or a detailed report is in order. A detailed report will list all files indexed. Advanced features give you the option to

cache document text or documents in the index and specify the fields to display in the search results. Sticking with the default settings, however, makes this a simple two-click process.

After creating the index, add the documents to the index. More advanced features are once again available, and you can choose to index only a particular file or folder, add items from an Outlook folder or the Web, or apply file filters to exclude certain types of files by extension. Once you have set the indexing parameters, the indexing process is started. When complete, the results screen allows you to view the log if desired.

The next step in the wizard is to create a search form. Again, the default can be used or you can customize the form in a variety of more advanced ways. See Figures 11.3 through 11.6.

Figure 11.3

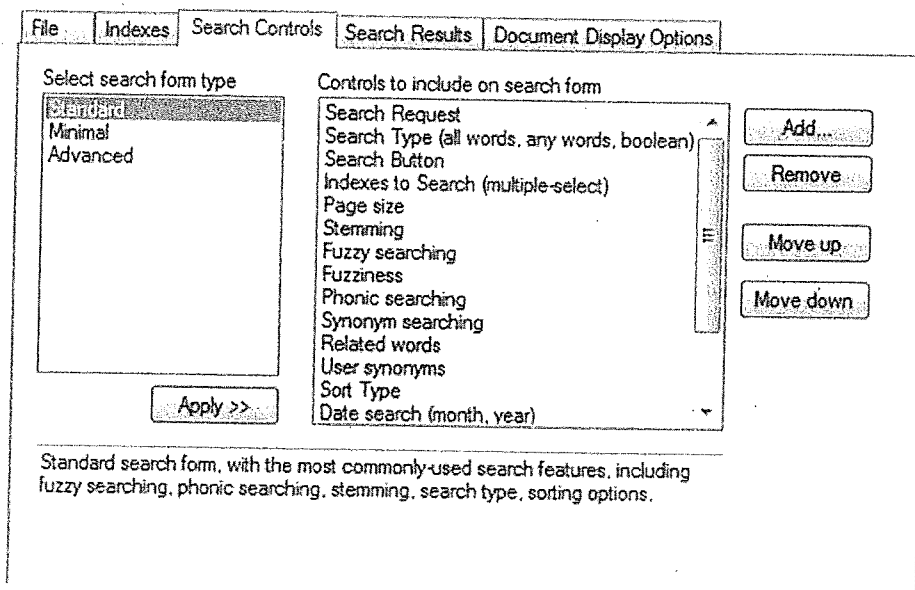


Figure 11.4

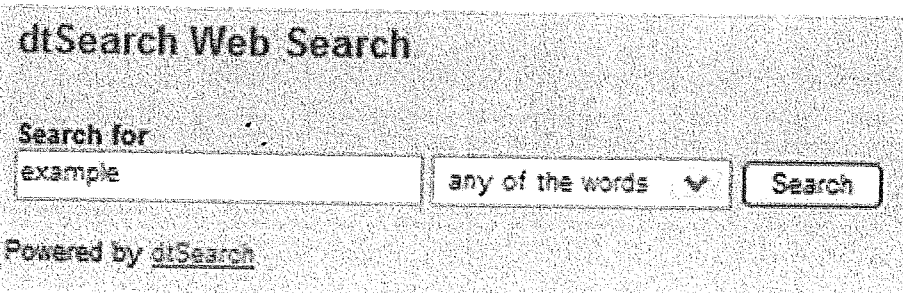


Figure 11.5

dtSearch Web Search

Search for
example any of the words

☐ Stemming
☐ Fuzzy searching
☐ Phonic searching

Sort type hits

Powered by [dtSearch](#)

Figure 11.6

dtSearch Web Search

Search for
example any of the words

Items per page 10

☐ Stemming
☐ Fuzzy searching -- Fuzziness 0
☐ Phonic searching
☐ WordNet synonyms
☐ WordNet related words
☐ User-defined synonyms

Sort type hits

File date
Jan 1999 to Aug 2005 all

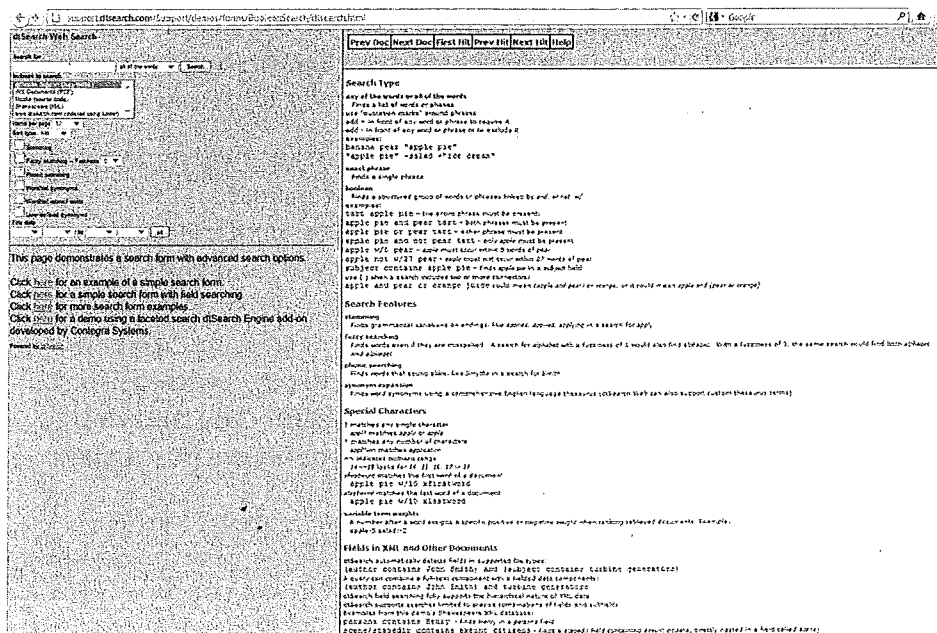
Powered by [dtSearch](#)

Finally, you are ready to test the collection on the CD, DVD, or external drive. Assuming it tests correctly, that is all there is to it. Although you have the option of further customization, using the default settings for this simple five-step process will create everything you need to burn a CD, DVD, or create a copy on an external hard drive. The burning process is done using your default burning software.

Delivering ESI That Is Universally Viewable and Searchable

Turning now to the end result, what kind of deliverable would you receive if you were the one on the other side? The process is simple. You would place the CD or DVD you received in the appropriate drive, or you would attach the external memory device to your computer and launch the program. You are directed to the Search page in what looks like a Web browser with two panes: a search pane and a results pane, with a tool bar across the top. See Figure 11.7. This interface is very easy to use. The tool bar at the top of the page allows you to quickly access the Search page to begin a new search, to print, or to move backward and

Figure 11.7



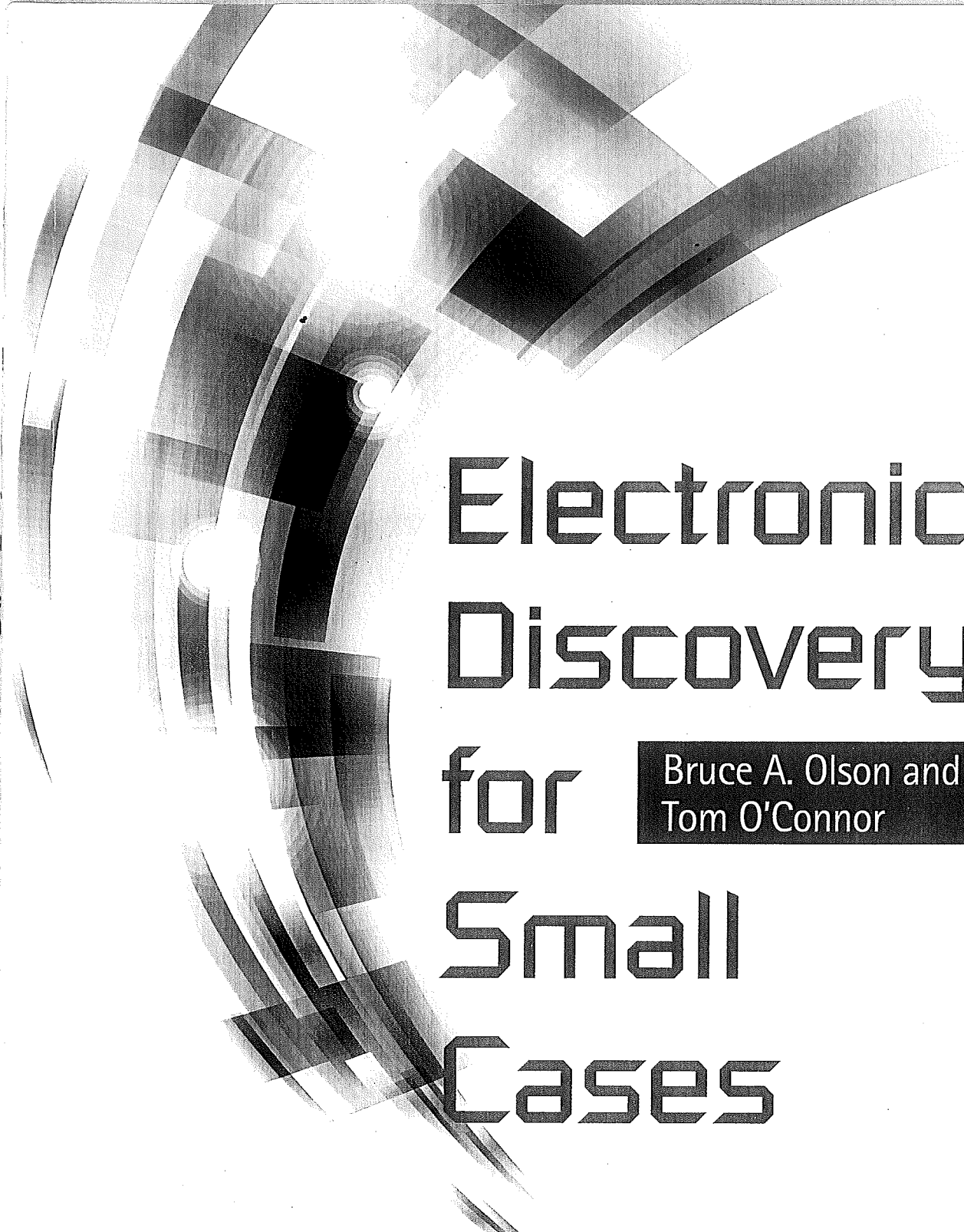
forward between the pages on which you have been working. When you first open the program, before you have begun a search, the opening page includes search instructions and hints for successful use of the program. There is also an extensive help menu that provides additional instruction where needed.

The opening view presents a "Search for" field on the left side of the page where you enter the words or phrases you want searched. A drop down menu gives you the option of searching for all the words, any of the words, the exact phrase, or you can use Boolean search terms and techniques. You can also select whether stemming, fuzzy, or phonic searching should be included. Finally, you have the option to organize the hit list by number of hits, date, name, or size of the file.

Once you have entered your search terms and run the search, you will have data appearing in the search results list below the search box. Each box displays a hot link to a document using the document's file name, along with additional information about the document based on the display fields that were specified by the person who created the CD, DVD, or external drive. The default result includes the number of hits, the date, the size of the file, and the title of the document. If you left click on the highlighted link to the document, the document will be viewable in the viewer in the right-hand pane. The viewer technology that is used gives you a rendered view that looks like the original, but you do not need the original application installed to be able to view the document. Using buttons on the viewer pane, you can navigate quickly from hit to hit within the document, or from document to document.

Assuming you have found a document that you want to copy for further analysis and use, you can right click on the viewer pane and select from several options. First, you can highlight individual text and simply copy and paste it into another document, or do a copy all and paste. You can also print the document. If you choose print preview, you will access several options for formatting the result you want to print. You can turn headers and footers on and off, print the full page with the search results and viewer both printed on the page, or print only the selected pane, which would give you just the document result or the search results.

At the time this book was written, a single location e-discovery license of dtSearch Publish cost approximately \$3,500 per year. dtSearch Publish is easy to use, both for the creator of the CD, DVD, or external hard drive and the recipient. It is a great solution to creating a production set of ESI that is immediately usable by the recipient. No specialized litigation software is needed, and no advanced IT support is required to access the contents of the CD, DVD, or external drive. dtSearch Publish is an ideal tool for lawyers who must produce ESI in discovery for other lawyers who lack other litigation support capabilities.



Electronic Discovery for Small Cases

Bruce A. Olson and
Tom O'Connor

Managing Digital Evidence and ESI

ABA **LAW PRACTICE MANAGEMENT SECTION**
MARKETING • MANAGEMENT • TECHNOLOGY • FINANCE

Discovery Project Management Template

Case Name _____

Client Matter Number: _____

Item	Task	Responsible	Date Due	Notes
1	Initial discussions with client re status to date			
2	Conduct litigation hold strategy meeting			
3	Determine scope of hold			
4	Determine recipients of hold			
5	Coordinate with HR re incoming/departing employees subject to hold			
6	Determine if third parties have relevant data			
7	Determine if computer forensics implicated			
8	Issue litigation hold communication			
9	Schedule periodic follow-up reminders re litigation hold			
10	Send opposition appropriate preservation demand			
11	Receive confirmation of hold instructions from recipients			
12	Develop outline of legal and factual issues			
13	Prepare and interview IT staff re systems, back-ups, etc.			
14	Identify sources of data and possible 30(B)(6) witness(es)			
15	Determine relative accessibility of data sources			
16	Determine if back-up tapes are implicated			
17	Determine if ongoing conduct implicated			
18	Consider taking snapshot of system			
19	Develop plan for gathering electronic data			
20	Develop plan for dealing with databases			
21	Develop plan for gathering paper documents			
22	Contact US-LitSupport for vendor recommendations/bids			
23	Select outside vendors if required			
24	Select platform for hosting data			
25	Develop initial budget for discovery			
26	Prepare custodian interview questions			
27	Prepare 30(B)(6) witness(es)			
28	Perform interviews of custodians			
29	Meet and confer with opposition			
30	Negotiate and obtain appropriate protective order re data			
31	Determine desired production format(s)			
32	Negotiate production format(s) with opposition			
33	Negotiate timetable for production(s)			
34	Negotiate timetable for receiving production(s)			
32	Create tracking log for gathering, processing, review and production			

33	Gather electronic data			
34	Gather paper data			
35	Determine OCR strategy for paper			
36	Determine extent of coding required for paper			
37	Develop estimate of amount of data			
38	Determine review platform and process			
39	Determine culling strategies; keyword list; date range limitations			
40	Determine review team composition			
41	Train review team			
42	Intensive review of key custodian(s) data			
43	Develop budget estimate for discovery			
44	Load data for review			
45	Review data for relevance and privilege			
46	Create privilege log			
47	Determine disposition of data post litigation			
	Roles			
	IT = Client IT staff			
	IC = Inside Counsel			
	OC = Outside Counsel			
	LS = Outside Counsel's Litigation Support Team			
	V = Outside Vendor			

Using In-House Staff or Hiring Third-Party Vendors

When a party is producing documents pursuant to a production request, it is necessary to decide whether the party wants its own information technology department to prepare the ESI or whether a third-party vendor will be hired to coordinate the production. A number of factors must be weighed in this decision. Three key factors include the amount of data to be produced, the amount of time the party has to produce them, and the complexity of transferring the data itself. Exhibit 7-5 shows a process that a client and legal team might follow to produce documents in a case.

In a Fortune 500 business merger, the U.S. Department of Justice requested a large amount of documents in a number of categories in conjunction with the merger. The organizations and their attorneys decided that the document production was too large for the organizations' own IT departments to handle. Instead, they issued a request for proposals and hired a third-party vendor. The vendor assisted the businesses in producing more than 30 million pages of documents in less than 60 days. To make matters worse, the Department of Justice required some files to be in their native format, whereas other files were to be produced as TIFF files. The vendor had special proprietary software that allowed the attorneys to review the ESI in a single database/platform while still being able to deliver the documents to the Department of Justice in multiple formats and meet its deadlines and requirements.

EXHIBIT 7-5
Steps in e-discovery
production process

No.	E-Discovery Production Steps
1.	Legal team issues letter to client advising them to preserve data related to litigation.
2.	Legal team meets with client to discuss strategies and problems related to ESI early on in case, including cataloging the ESI and discussing any special problems (unique or uncommon file formats, location of files/access, dates of files that may be requested, and any problems such as backup issues, etc.).
3.	If litigation is imminent, client and legal team decide whether production will be handled by a third-party vendor or the client's internal information technology (IT) team.
4.	If a third party will be used, a request for proposal may be issued, bids received, and a vendor selected.
5.	Parties to the lawsuit have a meet and confer conference to disclose ESI information and try to reach an understanding/resolution on ESI issues, including format of requested ESI.
6.	Document request is received. Legal team analyzes the request and decides if a protective order should be sought.
7.	Legal team meets with client and third-party vendor/client's IT team regarding production strategy, timelines, and any problems.
8.	Third-party vendor/client's IT team harvests ESI, processes the data into a common file format, and creates a database.
9.	Legal team reviews the ESI gathered. Sufficient time is allowed so that relevance and privilege issues are considered. If a third-party vendor is used, it is usually done at their site or remotely using the Internet and proprietary custom software. Such review includes the ability to search the database.
10.	ESI is produced and delivered to the opposing party.

Preparation for Discovery

After sending the initial legal hold, it's time to focus on who the key custodians are in the case and ensure their data is defensibly preserved.

In part 2, clearly understand what key custodians have, preserve potentially relevant data from them, and start preparing for search/collection and review stages.



Step 9

Litigation Support and Custodian:



Conduct face-to-face interview to review answers provided in legal hold questionnaire

- a) Confirm data sources
- b) Collect physical files

Step 10

Litigation Support:



- a) Record face-to-face interview notes in legal hold tool
- b) Update chain of custody form

Step 11

Litigation Support:



- a) Identify additional data for collection per face-to-face interview
- b) Initiate preservation or collection process

Step 12

IT/Compliance/Security:



- a) Apply in-place preservation if possible; or
- b) Collect data and store in collection repository
- c) Update chain of custody form

Step 13

Litigation Support:



- a) Scan physical files and save in collection repository
- b) Return physical files to custodian
- c) Update chain of custody form

Step 14

Custodian:



Receive legal hold reminder first business day of each quarter

Outside Counsel:



Receive legal hold case status report first business day of each quarter

Step 15

In-House Counsel, Paralegal, Litigation Support:



Meet to discuss legal hold status and outstanding issues



Missed Part 1 in this corporate in-house e-discovery workflow?

[Download it now and see steps 1-8](#)

exterro®

Yesterday's Technology, Today's Problem

Any piece of technology that stores information could be compromised—even obsolete devices that get thrown out with the garbage **By Jason Tashea**

Technology

In 2010, Affinity Health Plan, a Bronx, New York-based managed care provider, suffered a cybersecurity breach that put hundreds of thousands of health care records at risk. But the breach didn't occur because of a socially engineered ruse or a malicious hack.

It happened because the lease was up on the copy machines.

"A lot of lawyers aren't thinking that the copier has a hard drive in it," says Joe Lazzarotti, a principal at Jackson Lewis where he co-leads the firm's privacy, e-communication and data security practice.

Affinity's photocopiers had hard drives. In the normal course of business, they were rolled out the front door along with the electronic health care information of more than 344,000 people, according to a 2013 settlement with the U.S. Department of Health and Human Services.

Affinity failed to consider copy machines as a potential security risk, costing the company over \$1.2 million in a civil penalty. The settlement also required the company to expend resources to retrieve the machines, conduct a risk assessment and implement a new security plan.

"These peripheral devices of all kinds present risks that we're not thinking about," Lazzarotti says.

With so much attention paid to phishing attacks and hacking, ubiquitous

technologies are being overlooked. Beyond photocopiers, fax machines, smartphones and USB drives create unique security vulnerabilities. For lawyers, overlooking these devices could have serious consequences for attorney-client privilege and create ethics violations.

UNDERSTANDING THE RISKS

In 2012, the ABA Model Rules of Professional Conduct increased attention on technology's role in legal ethics. For example, Model Rule 1.1 regarding competency requires that lawyers be "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."

However, this is easier said than done. "Most lawyers are not trained to deal with the issues associated with inadvertent loss of information or unauthorized loss of information," says John Barkett, a partner at Shook, Hardy & Bacon in Miami and a member of the ABA Standing Committee on Ethics and Professional Responsibility, referencing the updated Model Rule 1.6(a) on confidentiality. "They don't understand technology well enough to be able to deal with that."

He says that reasonable attempts to follow the ethics rules may include talking with IT professionals and reading privacy policies and terms of service agreements to understand a device or piece of software.

The risks created by easily accessible software are increasingly coming into focus. Recent research from Northeastern University in Boston has found that apps for Android phones were acting beyond their terms of use by recording users' screens and sending that information back to the company. Of the 17,260 apps researched, they found over half had the potential to exfiltrate data collected through the phone's camera, microphone or ability to record the device's screen.

"It's alarming, but there's nothing you can trust in regard to your mobile phones and smart devices," says Elleen Pan, previously an undergraduate researcher at Northeastern and now a

software engineer at Square, a mobile payments company in Atlanta.

"Screen recording could be more of a privacy risk than access to your camera or microphone," says Pan. This software could capture the typing of credit card numbers, passwords and other personal information. The research notes that these actions were not always clear in user agreements and can't be turned off by users.

SMALL DEVICE, BIG BREACH

Smartphones aren't the only ubiquitous threat. USB drives and the expanding world of internet-enabled products, termed the "internet of things," also create and compound security vulnerabilities.

"The idea that you would take something that you know nothing about and put it in your machine is repugnant," says Jason McNew, CEO of Stronghold Cyber Security based in Gettysburg, Pennsylvania. "You have no idea where the thing was manufactured."

Comparing the ministorage devices to a dirty needle, he says they can come preloaded with malicious software and are used by hackers and penetration testers to exploit human vulnerabilities to access a network. While there is no Consumer Reports for secure devices, he notes that the National Security Agency does evaluate and validate some products for high-security purposes, such as hard drives, encryption devices and paper shredders.

Regarding the internet of things, including web-enabled cameras and smart thermostats, reports have shown that poor security has led to people's devices taking part in denial-of-service attacks while the owners were unaware. In other instances, device manufacturers built in secret "backdoors" so devices could be accessed remotely, which left the technology vulnerable to attacks.

"It's important to consider those things when you bring them into your environment," he says. "Once you get a foothold in the network—then it's anyone's guess to what you can and can't do." ■