

# E-Discovery with the Discovery Commissioner



3 GENERAL CLE CREDITS

**DATE:**

Thursday, August 7, 2008  
1:00 pm - 4:15 pm

**WHERE:**

Lloyd D. George U.S. District Courthouse  
Jury Assembly Room  
333 Las Vegas Blvd. S., Las Vegas

**COST:**

\$75/CCBA Member  
\$135/Non-member  
\$50 Legal Asst/NV Paralegal Assoc./  
UNLV Law Student Member  
\$60 Legal Asst/UNLV Law Student Non-member

CO-SPONSORED BY:



**SPEAKER:**

**Discovery Commissioner Bonnie Bulla**  
*8th Judicial District Court*  
**Ira Victor**  
*Data Clone Labs, Inc.*

**PRODUCED BY:**

CCBA's CLE Committee

**TOPICS:**

- Technical considerations in preserving and disseminating electronic data.  
Can you put your hands on a specific document within an hour?
- Maintaining the attorney-client and work product privileges for electronic data.  
Is your malpractice risk as low as it can be?
- The future of electronic discovery: technical advances and trends in recent case law.  
Coaching your clients to keep litigation ready records!

Have you heard?  
**12 CLE Credits**  
for only \$200!  
When you use your CLE Passport  
register for CCBA CLEs. For details  
visit [www.clarkcountybar.org](http://www.clarkcountybar.org)

CCBA CLE seminars are proudly sponsored by: Bank of Nevada, Cox Communications, Depo International, Thomson West and TREW



## E-Discovery in the Information Age

### Introduction

The purpose of this seminar is to examine certain technical and legal issues associated with the discovery of electronically stored data or e-discovery. In this information age where significant amounts of information are compiled and disseminated in seconds, managing such information in a litigation setting is a daunting task. This is particularly true because the advances in technology fast outpace appropriate changes in the law to address these advances. Thus there are many issues of first impression in the context of e-discovery. However, the Nevada Rules of Civil Procedure that apply to traditional discovery disputes also apply to e-discovery disputes. On December 1, 2006, the Federal Rules of Civil Procedure were amended to include the language of “electronically stored information” into certain rules.<sup>1</sup> The Nevada Rules of Civil Procedure do *not* include such language; however, the discovery of electronically stored information is unequivocally permissible in Nevada. After all, e-discovery is still discovery.

Three phases of the e-discovery process will be addressed:

1. The Preservation of Electronic Discovery;
2. The Retrieval of Electronic Discovery; and,
3. The Disseminate or Production of Electronic Discovery.

Each phase presents technical and legal challenges. Set forth below is a discussion of selected challenges.

#### **I. The Preservation of Electronic Information.**

In general, litigants have the duty to preserve evidence. The Nevada Supreme Court in *GNLV Corp. v. Service Control Corp.*, 111 Nev. 866, 900 P.2d 323 (1995), found that a litigant has a duty to preserve evidence which the litigant knows, or reasonably should know, is relevant to the action, even when the action has not yet commenced. Such evidence reasonably includes electronically stored data.

The District Court of Connecticut recently addressed the duty to preserve electronically stored data in *Doe v. Norwalk Community College*, 248 F.R.D. 372 (D. Conn. 2007). In this case, the Plaintiff, a student, sued the college and a professor alleging violations of Title IX (sexual harassment) and other state law claims. During discovery the Plaintiff and her team of experts, inspected the hard drives of key witnesses and the professor, who had previously resigned. The experts discovered the hard drives had been scrubbed and certain data had been

---

<sup>1</sup> The Federal Rules of Civil Procedure include the specific reference to “electronically stored information” in the following rules: See FRCP 16, FRCP 26 (a)(1)(A)(ii); FRCP 26 (b)(2)(B); FRCP 26(6)(5); FRCP26(f); FRCP 33(d); FRCP 34(a); FRCP 34(b); FRCP 37(e); and FRCP 45.

“altered, destroyed and filtered.” The Court found that the defendants had a duty to preserve certain electronically stored data and sanctioned the defendants for failing to do so, including the imposition of an adverse inference based on spoliation of evidence. An adverse inference is an inference that the lost or destroyed evidence would have benefited the party requesting production of the evidence. In Nevada, a party may be entitled to an adverse-inference jury instruction where evidence has been negligently lost or destroyed. An adverse presumption, however, applies only in cases involving willful suppression of evidence. See *McCarthy v. Underhill*, 2006 U.S. Dist. LEXIS 25555 (D. Nev. Feb. 16, 2006). The problem, of course, is that where electronically stored data is at issue, the line between what may have been “lost” versus “willfully suppressed” is not always easily discernable.

It is imperative that once counsel is retained by a client, a letter is sent to the client advising the client to preserve relevant evidence. This letter should be sufficiently specific to include preservation of e-discovery including metadata, back-up discs, hard drives, etc. Failure to do so may have significant consequences for both client and counsel.

## **II. The Retrieval of Electronic Discovery.**

The issues involving the retrieval of electronically stored data are preliminary technical in nature. The initial question may be what information should be retrieved? Obviously, information that falls within the parameters of NRCP 16.1 must be retrieved and produced.

If electronically stored data requires a protective order to be in place before it is produced, at a minimum, the information should be identified in the 16.1 disclosure with a statement that it will be produced once a protective order is in place.

A party serving a request to produce electronically stored data must be specific as to the information being sought in its request. For example, metadata must be specifically requested. Otherwise, courts will not compel its production. See, *Autotech Technologies v. Automationdirect.com*, 248 F.R.D. 556 (N.D. 111. 2008).<sup>2</sup> However, even if the request for production of documents is incomplete, the party who is in possession of potentially relevant electronically stored information must preserve it, even if it has *not* been requested. Further, if the party who possesses the information intends to use it at trial, that party is required to produce it pursuant to NRCP 16.1.

## **III. The Dissemination or Production of Electronic Discovery.**

Although the Nevada Rules of Civil Procedure do not incorporate the federal rules changes regarding electronically stored data, the federal rules provide reasonable guidelines to address certain production issues. These guidelines include the following:

1. The party who is producing electronically shared data may select the means by which the information is produced; the party need only produce the information by one means.

---

<sup>2</sup> Metadata refers to certain markers that are affixed to a document at its creation and every time it is modified. Metadata may be relevant in cases where authenticity of documents is at issue.

2. The means by which electronically stored data is produced must be reasonable. Production of thousands of documents on a CD without the documents being beta stamped and without an index is NOT reasonable.
3. Reasonable costs may be charged for the production of electronically stored data, which may also include the reasonable costs of retrieving the information (this will be determined on a case by case basis). See NRCP 34(d).

Unfortunately, another issue which may arise in the production of electronically stored data is in the inadvertent disclosure of privileged information. Efforts to avoid such disclosure should be addressed at the time of the NRCP 16.1 Conference. Specifically, if a protective order is contemplated by the parties this order should be in place prior to exchanging documents, legitimately protected by such an order. Non-protected documents should be exchanged as contemplated by NRCP 16.1.

Under the Federal Rules of Civil Procedure, information inadvertently produced by one party to another must be promptly returned upon. See, NRCP 26(b)(5). This is known as a “claw back” provision. There is not a similar provision in the Nevada Rules of Civil Procedure. Further, Rule 4.4(b) of the Nevada Rules of Professional Conduct, specifically provides as follows: “A lawyer who receives a document relating to the representation of the lawyer’s client and knows or reasonably should know that the document was inadvertently sent shall promptly notify sender.”

The Nevada Rules of Professional Conduct do not specifically address whether the information inadvertently sent has to be returned. Obviously, the resolution of an inadvertent disclosure will be addressed on a case by case basis. To avoid the potentially devastating consequences of an inadvertent production, a protective order should be in place early on in the litigation and the parties should address in the protective order how a possible inadvertent disclosure will be addressed. The parties’ discussion of these issues can be documented in the Joint Case Conference Report.

### **Conclusion**

In general, discovery of electronically stored data is governed by the same rules of civil procedure that apply to traditional discovery. The three phases of discovery of electronically stored data, preservation, retrieval and production, may be complicated by technical considerations. Advanced planning for the production of electronically stored information, including the execution of a protective order, may avoid pitfalls including, for example, inadvertent disclosures and costly document productions. Finally, the Federal Rules of Civil Procedure and corresponding case law, offer guidance when engaging in electronic discovery and should be utilized as a resource when appropriate.

## E-Discovery in the Information Age

Bonnie Bulla  
Discovery Commissioner



Ira Victor, Esq. QTTTA QCPA DPCI QREC  
Director, Compliance Practice



---

---

---

---

---

---

---

---

### Agenda

1. Brief overview of the new federal rules governing e-discovery
2. Planning for electronic discovery
3. Establishing document retention and purging policies
4. Preservation of data in anticipation of claims
5. Anticipated issues in electronic discovery
6. Maximizing outcome and minimizing risk through IT personnel
7. Appendix: email data flow

---

---

---

---

---

---

---

---

### About Bonnie Bulla

- > Discovery Commissioner for the Eighth Judicial District Court
- > Licensed in Nevada since 1987; prior practice areas included professional negligence and personal injury defense
- > Frequent speaker at CLE programs on discovery and the rules of civil procedure

---

---

---

---

---

---

---

---

<b>About Ira Victor</b>	
<p>-&gt; Information security consultant and auditor to corporations, law firms and government entities. Director of Compliance Practice, Data Clone Labs</p> <p>-&gt; Security certifications from the SANS Institute</p> <p>-&gt; Co-Host, Data Security Podcast: 30 min every week on Data Security, Privacy and the Law. <a href="http://datasecuritypodcast.com">http://datasecuritypodcast.com</a></p> <p>-&gt; President, Sierra Nevada InfraGard, a public private partnership between law enforcement and the private sector to protect critical infrastructure and stop cyber criminals. Represented InfraGard on SB410, NV Computer Forensics Bill</p>	

---

---

---

---

---

---

---

---

<b>Overview of the new federal rules governing eDiscovery</b>	
<p><b>Fed. R. Civ. P. 16</b> -&gt; Pretrial scheduling orders may address discovery of ESI</p> <p><b>Fed. R. Civ. P. 26(a)(1)(A)(ii)</b> -&gt; Initial disclosure obligation encompasses ESI</p> <p><b>Fed. R. Civ. P. 26(b)(2)(B)</b> -&gt; Party may identify ESI source as "not reasonably accessible" -&gt; Assertion may be challenged</p> <p><b>Fed. R. Civ. P. 26(b)(5)</b> -&gt; Procedure regarding inadvertent production ("clawback")</p>	

---

---

---

---

---

---

---

---

<b>Overview of the New Federal Rules Governing eDiscovery</b>	
<p><b>Fed. R. Civ. P. 26(f)</b> -&gt; Must discuss preservation of discoverable information -&gt; Must develop plan for production of ESI -&gt; Must develop plan to address privileges issues</p> <p><b>Fed. R. Civ. P. 33(d)</b> -&gt; Disclosure of business records may include ESI</p> <p><b>Fed. R. Civ. P. 34(a)</b> -&gt; Scope includes ESI</p> <p><b>Fed. R. Civ. P. 34(b)</b> -&gt; Form of production</p>	

---

---

---

---

---

---

---

---

**Overview of the New Federal Rules Governing eDiscovery**

**Fed. R. Civ. P. 37(e)**  
-> Restricts sanctions for loss of ESI

**Fed. R. Civ. P. 45**  
-> ESI can be sought through subpoena duces tecum  
-> Form of production  
-> Only if "reasonably accessible"  
-> Privilege claims

**Fed. R. Civ. P. Form 35**  
-> Discovery plan guidelines

---

---

---

---

---

---

---

---

**Data Planning for ESI**

The eDiscovery Baker's Dozen

1. Plan WITH a team that includes lawyers senior management, IT, InfoSec, Human Resources
2. Use C.I.A.
3. Document every step you take with exacting detail
4. Identify relevant regulations and other mandates
5. Prepare encryption plan and other tactics to handle select data
6. Diagram data flow, identify where information assets are located
7. Identify the information asset hardware
8. Pay special attention to: eMail and Operating Systems
9. Gather Data
10. Watch Lists
11. Keep data loss to an absolute minimum
12. Evaluate all the data you find
13. Summarize findings in plain English

---

---

---

---


---

---

---

---

**C.I.A. Central Intelligence Agency**



---

---

---

---

---

---

---

---

**C. I. A. - The Standard for InfoSecurity**

1. **Confidentiality**; Assurance that information is shared only with those authorized to have access to it.
2. **Integrity**; Assurance that the information is authentic and complete.
3. **Availability**; Assurance that the delivery, processing and storage of information is accessible when needed, by those who need them.

---

---

---

---

---

---

---

---

**Identify and Document Security Policies and Practices**

- The lack of a CIA-based security policy may result in:
- > The unauthorized disclosure of privileged information
  - > The unauthorized deletion of information
  - > Difficulty accessing information critical to proving a case

---

---

---

---

---

---

---

---

**CIA Example: Removable media**

- The lack of proper software and controls on removable media can also result in:
- > The unauthorized disclosure of privileged information
  - > The unauthorized deletion of information
  - > Difficulty accessing information critical to proving your case

---

---

---

---

---

---

---

---



<b>eDiscovery Planning Team</b>	
<ol style="list-style-type: none"> <li>1. The lawyers senior management, IT, InfoSec, Human Resources</li> <li>2. Review of Government Regulations</li> <li>3. Review of Contractual Mandates</li> <li>4. Review of Criminal Laws</li> <li>5. Your planning needs to "bake in" C. I. A. from the beginning</li> <li>6. Scope of Search – including nature of information search</li> </ol>	

---

---

---

---

---

---

---

---

<b>Establishing Document Retention and Purging Policies</b>	
<p>"Preservation" v. "Retention"</p> <p>Three requirements in creating a records management plan</p> <ul style="list-style-type: none"> <li>-&gt; Involve key players</li> <li>-&gt; Establish standards</li> <li>-&gt; Effective implementation</li> </ul> <p>Need for records management evidence</p> <p>Sources of standards</p>	

---

---

---

---

---

---

---

---

<b>Preservation of data in anticipation of claims</b>	
<p><b>ABA Civil Discovery Standard 10:</b></p> <p>"When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences of failing to do so. The duty to produce may be, but is not necessarily, coextensive with the duty to preserve . . ."</p>	

---

---

---

---

---

---

---

---

**Preservation of Data in Anticipation of Claims**

**Litigation hold and preservation plan**  
-> Need to have a plan ready

**Plan components**  
-> Communicate with client  
-> Identify relevant information  
-> Preserve information  
-> Follow up

**Consequences of failure**

---

---

---

---

---

---

---

---

**Preservation of Data**

**A. Most Important:**  
Minimize Data Loss when you gather evidence  
Steer clear of adding data when gathering evidence

**B. How does one steer clear of adding data?**  
Acquire forensically sound images; use a software or hardware write blocker  
What is a software write blocker? What is a hardware write blocker?

---

---

---

---

---


---

---


---

**Gathering of Data (con't)**

**Write Blockers:**  
Hardware Example



Software Example:



---

---

---

---

---

---

---

---

**What Information is Discoverable?**

**Forms of electronic data**

1. Data files	2. Background Information	3. Email
<ul style="list-style-type: none"> <li>• Active</li> <li>• Nearline</li> <li>• Archival</li> <li>• Backup</li> <li>• Residual</li> <li>• Legacy</li> <li>• Internet</li> </ul>	<ul style="list-style-type: none"> <li>• Audit trails</li> <li>• Access control lists</li> <li>• Metadata</li> </ul>	

---

---

---

---

---

---

---

---

**What Information is Discoverable?**

**Sources containing electronic data**

<ul style="list-style-type: none"> <li>-&gt; Servers</li> <li>-&gt; PCs</li> <li>-&gt; Laptops</li> <li>-&gt; PDAs</li> <li>-&gt; Mobile Phones</li> <li>-&gt; Thumb Drives</li> <li>-&gt; Network Equipment</li> <li>-&gt; Log Systems</li> <li>-&gt; CRM Systems</li> <li>-&gt; CAD-CAM Systems</li> </ul>	<ul style="list-style-type: none"> <li>-&gt; Web page code</li> <li>-&gt; Financial Accounting Systems</li> <li>-&gt; Software development code</li> <li>-&gt; Voicemail systems</li> <li>-&gt; Video teleconferencing systems</li> <li>-&gt; Anti-spam and anti-virus systems</li> <li>-&gt; Instant Messages</li> <li>-&gt; Calendaring systems</li> <li>-&gt; Time clock systems</li> <li>-&gt; Email systems</li> </ul>
--	---

-> Any and all other systems that might retain data

---

---

---

---

---

---

---

---

**What Information is Discoverable?**

**Individuals**

- > Work stations and laptops
- > Home computers and laptops
- > Removable storage or "loose" media
- > Myriad of electronic devices

---

---

---

---

---

---

---

---

<b>What Information is Discoverable?</b>	
<b>More sources</b>	
-> Third-Party systems (e.g., ISPs, other service providers)	
-> Telephone, security, or network activity systems	
-> Nearline and offline storage	

---

---

---

---

---

---

---

---

<b>Anticipated issues in electronic discovery</b>	

---

---

---

---

---

---

---

---

<b>Government Regulations: HIPAA</b>	
1. Health Information Portability and Accountability Act of 1996	
2. Our Focus: Individually Identifiable Health Information that might be discovered	
3. Enforcement Body: Department of Health and Human Services, Office of Civil Rights	
4. Penalties Include: Fines up to \$250,000 and up to 10 yrs in Federal Prison	

---

---

---

---

---

---

---

---

Government Regulations: Security Breach Disclosure Laws	
<ol style="list-style-type: none"> <li>1. Security Breach Information Act of 2003 (California, almost 40 states have similar laws in place)</li> <li>2. Nevada: NRS 603A.010 et seq.</li> <li>3. Safe Harbor for Encrypted Data, Important for eDiscovery!</li> <li>4. Common Focus: Credit Card, SSN, Driver's License, ATM, and Bank Account numbers</li> </ol>	

---

---

---

---

---

---

---

---

---

---

Government Regulations: FERPA	
<ol style="list-style-type: none"> <li>1. Family Educational Rights and Privacy Act of 1974</li> <li>2. Our Focus: Student education records. Applies to all schools that receive Federal Funding. Includes all records directly related to a student and maintained by an educational institution or someone acting on its behalf (like a contractor).</li> <li>3. Enforcement Body: United States Department of Education, Family Policy Compliance Office</li> <li>4. Penalties Include: Cut off of Federal Educational Funding</li> <li>5. Exception: Obtain a judicial order or subpoena directing release of the information. Student must be given notice of the subpoena prior to releasing information unless the subpoena directs otherwise.</li> </ol>	

---

---

---

---

---

---

---

---

---

---

Government Regulations: SOX	
<ol style="list-style-type: none"> <li>1. Sarbanes-Oxley Act of 2002</li> <li>2. Our Focus: SOX Section 404: Internal controls and Information Security. eDiscovery work may need extra documentation in certain circumstances.</li> <li>3. Enforcement Body: Securities and Exchange Commission, Public Company Accounting Oversight Board</li> <li>4. Penalties Include: Up to \$25 million in fines and up to 20 years in Federal Prison</li> </ol>	

---

---

---

---

---

---

---

---

---

---

<b>Government Regulations: GLBA</b>
<ol style="list-style-type: none"> <li>1. Gramm-Leach-Bliley Act of 1999</li> <li>2. Focus: Consumer Financial Data</li> <li>3. What the organization does determines compliance</li> <li>4. Enforcement Body: Federal Trade Commission</li> <li>5. Penalties Include: Fines up to \$1,000,000 per incident</li> </ol>

---

---

---

---

---

---

---

---

<b>Contractual Mandates: PCI</b>
<ol style="list-style-type: none"> <li>1. Payment Card Industry Digital Security Standard: PCI-DSS</li> <li>2. Our Focus: Confidentiality of Credit Card Data</li> <li>3. Accepting Credit Cards determines applicability</li> <li>4. Enforcement Body: PCI Council and Banks</li> <li>5. Penalties Include: Fines up to \$25,000 per day, \$500,000 per disclosure incident</li> </ol>

---

---

---

---

---

---

---

---

<b>Criminal Law: CP</b>
<ol style="list-style-type: none"> <li>1. Possession and Distribution of Child Pornography</li> <li>2. Our Focus: What to do in the first "Oh My God" moment</li> <li>3. Possessing CP determines applicability</li> <li>4. Enforcement Body: Local law enforcement, State Police, The Feds</li> <li>5. Penalties Include: (Varies) Could bring havoc to a case</li> </ol>

---

---

---

---

---

---

---

---

Special Handling of Select Data	
<p>A. Prepare encryption plan and/or other means to protect select data</p> <ol style="list-style-type: none"> <li>1. Third party involvement</li> <li>2. Storage and escrow of encryption keys</li> <li>3. Thoroughly document all actions</li> <li>4. Care attention to logging and audit trails</li> </ol> <p>B. Prepare plan if CP for other criminal content. Plan should include special handling instructions for CP or other criminal content</p> <p>C. Good C. I. A.</p>	

---

---

---

---

---

---

---

---

Maximizing outcome	
<ol style="list-style-type: none"> <li>1. Senior management</li> <li>2. Legal – including paralegals</li> <li>3. Human Resources <ul style="list-style-type: none"> <li>• May need to include consultants and past employees</li> <li>• They have the authority to hire/fire</li> </ul> </li> <li>4. Information Technology Staff</li> <li>5. Information Security Staff</li> </ol>	

---

---

---

---

---

---

---

---

Managing The Process... (con't)	
<p>-&gt; IMPORTANT: Encourage Senior Management to select a team member with good diplomatic skills to work with the legal people</p> <p>-&gt; If you have good diplomatic skills, your value to the organization will be very high</p> <p>-&gt; Identify paralegals with good diplomatic skills</p>	

---

---

---

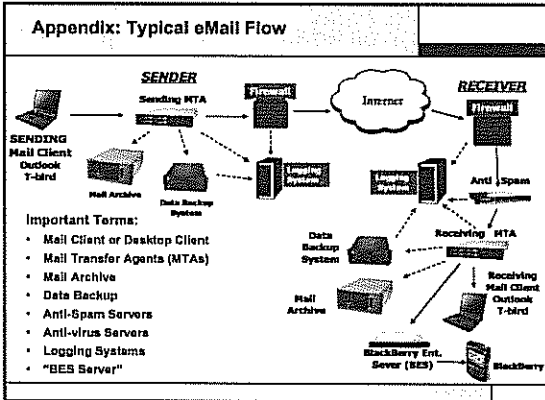
---

---

---

---

---




---

---

---

---

---

---

---

---

---

---

---

---

- ### Relevant Links
- [www.ediscoverylaw.com](http://www.ediscoverylaw.com)
  - [www.thesedonaconference.org](http://www.thesedonaconference.org)
  - [www.craigball.com/cf.pdf](http://www.craigball.com/cf.pdf)
  - [www.discoveryresources.com](http://www.discoveryresources.com)
- Page 21

---

---

---

---

---

---

---

---

---

---

---

---

### E-Discovery in the Information Age

Bonnie Bulla  
Discovery Commissioner

Ira Victor, SHAC, SHITW, OCPA, OPCI, OSEC  
Director, Compliance Practice

---

---

---

---

---

---

---

---

---

---

---

---