

We got sued! SOS Save the Scripts, and Body Cam, Too!



Clarissa M. Rodriguez, Partner
Kelly R. Albin, Partner
Denton Navarro Rodriguez Bernal Santee &
Zech, P.C.

What is E-Discovery and ESI?

E-Discovery is the process of identifying, locating, preserving, collecting, preparing, reviewing, and producing information requested in requests for production in the discovery process that is stored electronically as opposed to paper (or other tangible) form.

ESI is different than conventional paper production as it results in a significantly greater amount of production, it may be in multiple places, it may be in multiple formats, deletion of information may not really eliminate the ESI, and it may not have an equivalent for documents or tangible items.

What is E-Discovery and ESI?

Types of Data

- Active Data- data on hard drives
- Archival Data- long term storage; record keeping
- Backup Data- recovery source for data
- Backup tape recycling- overwritten with new data (ie: security video)
- Deleted data- deleted by system or user
- Legacy data- obsolete data on hardware or software
- Near line data- available in a system that retrieves removable storage media or tapes

Metadata- how, when, why, whom- data was created, modified, etc

Forensics/Forensic Copy- examination/copy of examination of ESI

Mirror Imaging- forensic imaging/duplication of stored ESI

Form of Production

- Native format- original format of ESI (Word, Excel, etc)
- Static format- ESI that can be viewed as an image on a computer (pdf, tiff, jpg, etc)

Hard drive- storage device that has components that can be written over or erased magnetically

Systems data- computer records about its use

Sued or Not Sued...Don't Sink!

Immediate Anticipated Claim or Litigation

- A citizen or Attorney sends a demand letter
- A citizen or attorney sends e-data preservation letter
 - Notice Letter Under Texas Tort Claims Act
- A serious accident occurs involving city property or personnel
- An employee files an EEOC or TWC complaint
- A police use-of-force incident
- A contract dispute is escalating
- Controversial ordinance passed



We got this letter...what do we do with it???

| | |
|------------------|-------------------------------|
| SAVE | SAVE THE E-DATA |
| Safeguard | Safeguard the Data |
| Alert | Alert Custodians |
| Verify | Verify Locations/Sources |
| Ensure | Ensure Retention & Compliance |

Why Do We Care as a City Attorney- there is no lawsuit?

- **Anticipation of Litigation- Claim or Investigation**
 - PRESERVATION as **SOON** as you KNOW!
- **TPIA** Considerations
- **Modern Evidence Is Often Transient**
 - Evidence is routinely overwritten or deleted:
 - Surveillance video may auto-delete after 30–90 days.
 - **INVENTORY** Digital Storage Devices
 - Text messages may disappear when phones are replaced.
 - **DO NOT LET ANYONE WIPE A PHONE!**
 - Cloud platforms may have short retention settings.
 - Social media content can be removed.
 - Without early intervention, critical evidence may vanish before anyone thinks about a lawsuit.
- Legal **Compliance** Later
- Protects City **Defenses**



Save the S____ (Stuff!)

- E-Data Preservation Letter Pre Litigation
 - Specific or Otherwise
- E-Data Preservation Direction/Letter as a City Attorney after Litigation Filed
- That is a LOT- Why???
- Spoliation...Later...
 - Sanctions –
 - \$\$ and risk of losing use of key evidence
- Value to Plaintiffs
- Adverse Jury Instruction
- Duty to Protect & Effective Representation of the City as Client
 - Rule 1.01- Competent and Diligent Representation
 - Rule 1.13- Organization as Client

| | | | |
|--|---|---|--|
| <p>Rule 1.01 – Competence</p> | <p>Provide competent representation, including required legal knowledge, skill, and preparation.</p> | <p>Lawyers must understand enough about technology to identify, preserve, and produce ESI defensibly; may require consulting technical experts.</p> | <p>A city attorney ensures they understand email archiving systems and retention schedules to respond to both litigation discovery and TPIA requests.</p> |
| <p>Rule 1.13 – Organization as Client</p> | <p>The client is the entity, not the individual officials or employees. Escalate issues internally if an officer's conduct threatens the client's legal compliance.</p> | <p>Counsel must act in the entity's best interests when officials or employees fail to preserve ESI or refuse production.</p> | <p>A county commissioner refuses to produce texts from a personal phone about county business; counsel informs the county judge and IT to preserve the data and comply with both discovery and TPIA.</p> |

Pre-Litigation Letter from Us



Daniel Navarro Bernal Santer & Zech
Attorneys & Consultants at Law • dnp.dnrbs.com
San Antonio | Rio Grande Valley | Austin | El Paso | Dallas
2517 N. Main Avenue | San Antonio, Texas 78212-4685
© 2010-2023-2024 | P 210-225-4488

**PRIVILEGED & CONFIDENTIAL
ATTORNEY CLIENT WORK PRODUCT
NOT A PUBLIC RECORD**

June 4, 2025

PRESERVATION OF EVIDENCE, DOCUMENTS, RECORDS AND ELECTRONIC DATA

Dear

We have been notified of a potential litigation claim involving an arrest, detention, investigation, charging, and/or prosecution of which involved the from his attorney. This letter is to advise you and the City staff that it is incumbent on the City to identify and preserve electronic and paper data that may be relevant to potential future claims and the City's defenses.

We seek your assistance to advise the City and its employees of the legal duties which the City's employees and officials have to PRESERVE DOCUMENTS AND EVIDENCE IN ALL FORMS, INCLUDING ELECTRONIC AND OTHER TYPES OF RECORDED INFORMATION. This duty requires all persons in possession of information potentially relevant to anticipated litigation or discovery conducted in the litigation to REVIEW, SAFEGUARD, AND PRESERVE this information.

We hereby request that you forward a copy of this letter to those staff members necessary to preserve relevant information and obtain their acknowledgment and agreement to perform their duties as the law requires. Some are listed below. We ask that you remind personnel of the necessity of maintaining records by and between individuals from the date of the incident (or about July 8, 2025) and moving forward.

June 4, 2025
Page 2

The law requires us to preserve and maintain evidence, as well as preventing anyone with access to data from modifying, destroying, or hiding electronic evidence or recordings. Potentially, relevant information may include, but is not limited to:

- Digital communications (e-mail, voice mail, instant messaging, which would include e-mail activity in inboxes, sent boxes and deleted histories);
- Word processed documents (Word or WordPerfect documents and drafts);
- Spreadsheets and tables (Excel or Lotus 123 worksheets);
- Image and facsimile files (pdf, ppt, jif, gif, images);
- Sound recordings (WAV and MP3 files);
- Video and animation (AVI and MOV files);
- Databases (Access, Oracle, SQL, Serve data, SAP);
- Contact and Relationship Management Data (Outlook, ACT);
- Calendar and Diary Application Data (Outlook PST, Yahoo, blog tools);
- Online Access Data (Temporary Internet Files, History, Cookies, cache files);
- Presentations (PowerPoint, Corel Presentations);
- Third party information;
- Telephone/Voicemail systems (stationary and mobile);
- City-issued cellular phones and personal cell phones with City information related to this incident before, during and after the occurrence;
- Text Messages;
- Metadata; and
- Open Record Requests.

Electronic information can be obtained in several forms: active data (currently accessible data from a computer), replicant data (data derived from electronic archives and automatic backups), residual data (deleted or unallocated data on a computer), and metadata (data about electronic data that includes dates of creation, alteration, deletion, and who accessed the data, and from where, amongst others). The City will need to identify if there are any access codes that are necessary to access this information. The City will also need to **cease routine document destruction**, keep backup tapes, and instruct employees to refrain from deleting documents until forensic copies of hard drives can be obtained, if necessary. Although the letter

We have identified the following persons whose electronic and other information should be preserved during the relevant time period related to the subject incident:

and yourself, all records noted in the preservation letter from the Police Department for the necessity of maintaining records by and between them regarding the potential claimant(s) and/or their agents and representatives and other information related to the incident involving claimant(s) prior to and post incident noted in the preservation letter. To the extent any of the information from and/or to the above-referenced individuals are within the City's control and can be saved or retrieved, please do so.

We are available to consult with you on the scope of these responsibilities and how they should be implemented in the context of specific software, programs, or systems, and will assist

June 4, 2025
Page 3

you in dealing with any IT consultants or service providers involved in the design, maintenance, and use of your systems.

It is also very important that any and all recordings (video or audio) of conversations, hearings, meetings or other relevant information regarding this incident, including those with possible claimant(s) be retrieved, reviewed, and preserved. We ask that you instruct personnel (including former personnel to the extent possible) to cooperate with the City's efforts to obtain any necessary information. Once you retrieve the information, please forward to my attention. Please keep in mind that it is critical for all other pertinent City Departments and personnel to preserve electronic data and recordings.

Thank you for working with us to ensure the City's potential legal defenses are enhanced in this legal matter. I sincerely appreciate your efforts to oversee preservation of e-data that may be used as evidence in this case. Please, do not know if you or City staff members have any questions.

Very truly yours,

DINTEO NAVARRO RODRIGUEZ BERNAL SANTER & ZECH
A PROFESSIONAL CORPORATION

Christina M. Rodriguez
CLAIRSSA M. RODRIGUEZ
CHARLES E. ZECH

Cc:



Daniel Navarro Bernal Santer & Zech
Attorneys & Consultants at Law • dnp.dnrbs.com
San Antonio | Rio Grande Valley | Austin | El Paso | Dallas
2517 N. Main Avenue | San Antonio, Texas 78212-4685
© 2010-2023-2024

**PRIVILEGED & CONFIDENTIAL
ATTORNEY CLIENT WORK PRODUCT
NOT A PUBLIC RECORD**

July 14, 2025

PRESERVATION OF EVIDENCE, DOCUMENTS, RECORDS AND ELECTRONIC DATA

Dear

We have been retained by the Texas Municipal League Intergovernmental Risk Pool to represent the City of ("City") with respect to a lawsuit alleging discrimination based on disability in connection with employment with the City's Fire Department. It is incumbent on the City to identify and preserve electronic and paper data that may be relevant to his claim and the City's defenses.

The purpose of this letter is to seek your assistance to advise the City and its employees of legal duties which the City's employees and officials have to PRESERVE DOCUMENTS AND EVIDENCE IN ALL FORMS, INCLUDING ELECTRONIC AND OTHER TYPES OF RECORDED INFORMATION. This duty requires all persons in possession of information potentially relevant to the litigation or discovery conducted in the litigation to REVIEW, SAFEGUARD, AND PRESERVE this information.

We hereby request that you forward a copy of this letter to those staff members necessary to preserve relevant information and obtain their acknowledgment and agreement to perform their duties as the law requires. We ask that you remind personnel of the necessity of maintaining records by and between the City and/or persons communicating with on behalf of the City from the date of February 1, 2024, to present and moving forward.

The law requires us to preserve and maintain evidence, as well as prevent anyone with access to data from modifying, destroying or hiding electronic evidence or recordings. Potentially, relevant information may include, but is not limited to:

- Digital communications (e-mail, voice mail, instant messaging, which would include e-mail activity in inboxes, sent boxes and deleted histories, cell phone text messages or call logs);
- Word processed documents (Word or WordPerfect documents and drafts);
- Spreadsheets and tables (Excel or Lotus 123 worksheets);
- Image and facsimile files (pdf, ppt, jif, gif, images);
- Sound recordings (WAV and MP3 files);
- Video and animation (AVI and MOV files);
- Databases (Access, Oracle, SQL, Serve data, SAP);
- Contact and Relationship Management Data (Outlook, ACT);
- Calendar and Diary Application Data (Outlook PST, Yahoo, blog tools);
- Online Access Data (Temporary Internet Files, History, Cookies, cache files);
- Presentations (PowerPoint, Corel Presentations);
- Third party information;
- Telephone/Voicemail systems (stationary and mobile);
- City-issued cellular phones and personal cell phones with City information related to this incident before, during and after the occurrence;
- Text Messages; Metadata; and
- Open Record Requests.

Electronic information can be obtained in several forms: active data (currently accessible data from a computer), replicant data (data derived from electronic archives and automatic backups), residual data (deleted or unallocated data on a computer), and metadata (data about electronic data that includes dates of creation, alteration, deletion, and who accessed the data, and from where, amongst others). The City will need to identify if there are any access codes that are necessary to access this information. The City will also need to **cease routine document destruction**, keep backup tapes, and instruct employees to refrain from deleting documents until forensic copies of hard drives can be obtained, if necessary.

We have identified the following persons with the City whose electronic and other information should be preserved during the relevant time period related to the subject incident:

(City Secretary), (City Manager), (Fire Chief),
(Asst City Manager/Civil Service Director), (Benefits Coordinator),
(Station Chief), and yourself for the necessary of maintaining records by and between them regarding possible claimant(s) and/or their agents and representatives and other information related to the incident involving possible claimant(s) prior to and post incident. To the extent any of the information from and/or to the above-referenced individuals are within the City's control and can be saved or retrieved, please do so.

We are available to consult with you on the scope of these responsibilities and how they should be implemented in the context of specific software, programs, or systems, and will assist you in dealing with any IT consultants or service providers involved in the design, maintenance, and use of your systems.

It is also very important that any and all recordings (video or audio) of conversations, hearings, meetings or other relevant information regarding this incident, including those with possible claimant(s) be retrieved, reviewed, and preserved. We ask that you instruct personnel (including former personnel) to cooperate with the City's efforts to obtain any necessary information. Once you retrieve the information, please forward to my attention. Please keep in mind that it is critical for all other pertinent City Departments and personnel to preserve electronic data and recordings.

Thank you for working with us to ensure the City's legal defenses are enhanced in this legal matter. I sincerely appreciate your efforts to oversee preservation of e-data that may be used as evidence in this case.

Very truly yours,

DINTEO NAVARRO RODRIGUEZ BERNAL SANTER & ZECH
A PROFESSIONAL CORPORATION

Key Points from In House Attorney Letter

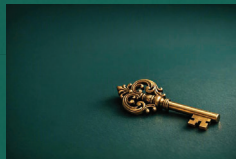
- **Triggered by a claimant's attorney** re: an arrest / detention matter (incident on or about July 8, 2025)
 - Could be pre- or post- litigation
 - TTCA Notice letter
- **Advises the City and employees** of the duty to preserve electronic and paper records for anticipated litigation.
- **Reminds personnel** to maintain records from the date of the incident forward.
- **Cease routine document destruction** keep backup tapes, and do not delete until forensic copies are made.
- **Identifies custodians** including the Police Department personnel noted in the preservation letter.



Types of E-Data to SAVE (Because paper gets destroyed in water)

General City Information

- E-Mails
- Texts
- Teams, Slack (Messaging Forms)
- What'sApp, Signal, Telegram, etc
- Body Cam
- Dash cam
- Council Chamber Camera Video
- Security/Surveillance Camera Video
- Voicemails
- AI Prompts
- Cloud Storage- SharePoint, OneDrive, Dropbox
- InCode Data
- GIS/Public Works Data



Law Enforcement & Emergency (911)

- Body-worn camera footage
- Dash camera video
- Dispatch recordings CAD (Computer-Aided Dispatch)
- Records RMS (Records Management System) data
- Digital evidence files
- 911 recordings
- Radio communications
- Dispatch logs
- Incident reporting systems
- Holding cell video

E-Discovery: Process, Lifecycle, Interplay with Ethical Obligations

Identification and Preservation of ESI - When litigation is anticipated or when there is a triggering event for a client to preserve evidence, working with the client is imperative to work with the reasonably identifiable person (e.g. IT Department) to identify and preserve all sources of ESI and persons who may have ESI as it relates to the litigation.

Collection and Production of ESI - The party does not have to produce ESI that is not reasonably accessible because of undue burden or cost.

Challenges with Collection and Production & Solutions for ESI.

Rule 26(f) Conference - Using the Rule 26(f) conference is key to producing ESI. Parties are required to confer and this includes conferring on ESI.

The Sedona Principles on E-Discovery

The Sedona Principles originated from the work of The Sedona Conference, a nonprofit think tank established in 1997 to bring together judges, lawyers, academics, and experts to address complex issues in law and policy.

There were multiple challenges to e-discovery in litigation, and the group worked on principles to provide guidance on fairness, reasonableness, and proportionality in e-discovery, emphasizing cooperation among parties and the need to balance costs with the value of information.

Sedona provides principled and best practices for courts, attorneys, and litigants in e-discovery processes and procedures under the Federal Rules of Civil Procedure.

There are 14 Sedona Principles and numerous commentaries on various topics on E-Discovery such as preservation, legal holds and so forth.

| Sedona Principle | Relevant FRCP Rule(s) | Practical Example |
|--|----------------------------------|--|
| 1. Reasonableness and Good Faith in Preservation | Rule 26(b)(1), Rule 37(e) | Implement a targeted litigation hold on relevant custodians rather than halting deletion of all ESI. |
| 2. Proportionality | Rule 26(b)(1) | Limit discovery to a 6-month window and key custodians to reduce costs while covering disputed issues. |
| 3. Cooperation | Rule 1, Rule 26(f) | Agree on search terms and custodians during the Rule 26(f) conference to prevent later disputes. |
| 4. Reasonable Accessibility | Rule 26(b)(2)(B) | Deem backup tapes "not reasonably accessible" due to extreme costs; produce only upon good cause. |
| 5. Early Judicial Management | Rule 16, Rule 26(f) | Judge orders phased discovery, beginning with emails before financial records. |
| 6. Duty to Preserve Once Litigation Is Anticipated | Rule 37(e) | Issue a litigation hold upon receipt of a demand letter—not after suit is filed. |
| 7. Production Formats and Metadata | Rule 34(b)(2)(E) | Produce emails in native format with metadata to preserve searchability. |
| 8. Protection of Privilege and Work Product | Rule 26(b)(5)(B) | Use a Rule 502(d) order to prevent privilege waiver for inadvertent productions. |
| 9. Cost Allocation | Rule 26(c), Rule 26(b)(2)(B) | Court orders requesting party to share costs of restoring inaccessible backup data. |
| 10. Sanctions for Spoliation | Rule 37(e) | Court declines sanctions where data loss occurred before duty to preserve and without bad faith. |
| 11. Cross-Border Data | Rule 26(b)(1), (b)(2) | Negotiate production parameters to comply with GDPR restrictions. |
| 12. Technology-Assisted Review (TAR) | Rule 26(b)(1), Rule 34 | Parties agree to use TAR with validation metrics instead of linear review. |
| 13. Ethics and Competence | Rule 26(g), Model Rule 1.1 | Counsel engages e-discovery experts to ensure technical competence. |
| 14. Continuous Improvement | Not codified; aligns with Rule 1 | Firm implements post-case process reviews to improve future workflows. |

The Sedona Principles & the FRCP Crosswalk