McGraw Morris P.C.

Don't Let This Happen to You – How to Prepare Your Municipality to Avoid Litigation Horror Stories

Presented By:
Stacy J. Belisle

Michigan Court Rule Regarding Discovery of Electronically Stored Information ("ESI") - MCR 2.302(B)(5) and (6)

- Electronically Stored Information. A party has the same obligation to preserve electronically stored information as it does for all other types of information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

- Limitation of Discovery of Electronic Materials. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of MCR 2.302(C). The court may specify conditions for the discovery.

How to Proactively Manage Data

- When a lawsuit is filed, stay in front of discovery requests and consider the following:
  - How will ESI come into play?
  - How will ESI will be preserved?
  - How will ESI be searched and what limitations will apply?
  - How will ESI be produced?

PRESERVATION OBLIGATIONS

Under Michigan common law, the duty to preserve arises when a party has notice of the information's relevance to litigation or impending litigation. Unfortunately, notice is often examined in hindsight, and Michigan law provides little, if any, bright-line guidance on when a preservation obligation arises.

How to Comply

- **Take Precautions to Prevent Discovery and Spoliation Sanctions**
- **Issue a Litigation Hold Memorandum/Letter**
- **Identify Individuals and Systems with Responsive Information**
- **Take Action to Retain Backups**
- **Suspend Automatic Email Deletion**

Efforts to Search for Relevant Data

Nissan N. Am., Inc. v. Johnson Elec. N. Am., Inc., 2010 U.S. Dist. LEXIS 43753, 13-14 (E.D. Mich. May 5, 2010)

- The plaintiff was ordered to supplement its discovery responses to specifically identify sources of ESI which were not reasonably accessible, the reasons for its contention that the ESI is not reasonably accessible without undue cost and effort, and the anticipated costs and efforts involved in retrieving that ESI.

SPOLIATION/SANCTIONS

- Spoliation is 'the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.'" *Orbit One Communications, Inc. v. Numerex Corp*., 271 F.R.D. 429 (S.D.N.Y. 2010).
- "The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation," including instances where suit has not been filed but the party "should have known that the evidence may be relevant to future litigation." *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998).
- The determination ot been filed but the party "should have of whether sanctions should be imposed for the destruction of evidence ultimately turns on whether relevant information has been lost. *Mastr Adjustable Rate Mortgages Trust 2006-OA2 v. UBS Real Estate Securities Inc*., No. 12 Civ. 7322 (S.D.N.Y. Oct. 23, 2013).

E-Discovery Costs

Fair Housing Center of Southwest Michigan v. Hunt, No. 09-cv-593 (W.D. Mich. Oct. 21, 2013).

- After concluding that the plaintiffs were "prevailing parties" in a civil rights action alleging housing discrimination in violation of the Fair Housing Act, the court held that the attorney fee request was unreasonable largely because too much time was spent on e-discovery.

PROPORTIONALITY

- The federal court rules require that "proportionality" of efforts be balanced when ESI, or any discovery, is at issue. The rule states:
  - On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:
    - the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;
    - the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
    - the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

POSSESSION, CUSTODY OR CONTROL

Puerto Rico Tel. Co. v. San Juan Cable LLC, No. 11-2135 (D.P.R. Oct. 7, 2013).

- The court held that the defendant had a duty to preserve relevant emails that came from the personal email accounts of its former officers because it "presumably knew" that the officers used their personal email accounts to engage in company business. Because some of these emails were "lost" and could not be obtained through other sources, the plaintiff requested sanctions for spoliation.
- The court denied the plaintiff's request without prejudice because there was no evidence of bad faith or that the lost emails would help prove the plaintiff's claims. The court stated, however, that "[f]orensic analysis of these three former employees' personal email accounts and computers may be appropriate to determine whether critical emails have been deleted."

Discovery of Text Messages Ordered

Flagg v. City of Detroit, 252 F.R.D. 346 (E.D. Mich. 2008)

- Defendants, the City of Detroit and Christine Beatty, among others, filed motions to preclude discovery of communications exchanged among certain officials and employees of the city via city-issued text messaging devices, arguing that the Stored Communications Act ("SCA") wholly precluded the production in civil litigation of electronic communications stored by a non-party service provider.
- The court rejected the defendants' reading of the SCA as establishing a sweeping prohibition against civil discovery of electronic communications. The defendants' position, if accepted, would have dramatically altered discovery practice, in a manner clearly not contemplated by the existing rules or law, by permitting a party to defeat the production of electronically stored information created by that party and still within its control through the simple expedient of storing it with a third party. Because nothing in the plain language of the SCA required that result, and because the defendants did not identify any other support for this proposition, the court held that the discovery effort contemplated in its opinion and related order could go forward, albeit through a means somewhat different from that employed by plaintiff to date.

TEXT MESSAGES NOT DISCOVERABLE

Elcometer, Inc. v. TQC-USA, Inc., 2013 U.S. Dist. LEXIS 135437, 10-11 (E.D. Mich. Sept. 23, 2013).

- In contrast to *Flagg*, the dispute in this case was over a third party subpoena, as opposed to a discovery request directed to a municipal party. Unlike the present case, the defendant in Flagg was available and responsive, but refused to consent to the production of electronic messages that were stored by a third-party service provider. While the Court found that the information in question was discoverable, it did not permit access to the material by enforcing a third-party subpoena, but directed the plaintiff to serve document requests to the defendant, who was then directed to instruct the third-party service provider to produce the responsive material to the plaintiff.

Discovery of Personal Facebook Content

Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012).

- The issue before the court was raised in a motion to compel the plaintiff to execute authorizations allowing Facebook to divulge the plaintiff's own personal Facebook content. The lawsuit was over a slip-and-fall injury in which the plaintiff claimed back and other injuries related to an accident at Detroit Metropolitan Airport. The plaintiff alleged that as a result of her injuries, she was impaired in her ability to work and to enjoy life. The defendant requested that the plaintiff sign authorizations for records from her Facebook account.

Improper Access to Facebook

The Stored Communications Act (SCA) regulates when an electronic communication service provider may disclose the contents of, or other information, about a customer's emails and other electronic communications to private parties. Congress passed the SCA to prohibit a provider of an electronic communication service "from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient."

Improper Access to Facebook

- *Ehling v. Monmouth-Ocean Hospital Service Corp*, unpublished opinion per curiam of the United States District Court for the District of New Jersey, Docket No. 2:11-cv-03305 (decided August 20, 2013).
  - The judge in this case determined, for the first time, that private Facebook postings an employee posted about her employer are subject to the SCA. This decision could be problematic for employers who take action against employees for private information posted by employees on social media sites.

Privacy Rights in the Workplace

- *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300; 990 A.2d 650 (2010).
  - The New Jersey Supreme Court issued a decision concerning the extent to which employers can monitor and restrict their employees' personal use of company computers.
  - In contrast, in *Holmes v. Petrovich Development Co.*, 191 Cal. App. 4th 1047 (2011), the court reached a different conclusion. In this case, the plaintiff sent emails to her attorney using her work provided computer and using her work email. In contrast to the *Stengart* case, the employer in *Holmes* had a much more restrictive policy.

Michigan's Internet Privacy Protection Act

In 2012, the Michigan legislature enacted the Internet Privacy Protection Act to address employers' attempts to force employees and prospective employees to provide access to social media or passwords to social media.

Michigan's Internet Privacy Protection Act

An employer shall not do any of the following:

- Request an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.
- Discharge, discipline, fail to hire, or otherwise penalize an employee or applicant for employment for failure to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal internet account.

"Public Record" – The Basics …

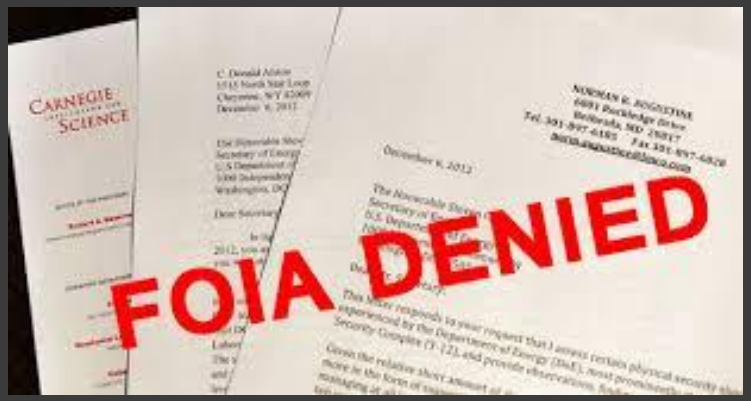
1. The record must be "a writing."
2. The record must be involved in the performance of an official function of the public body.

EXEMPTIONS

FOIA EXEMPTIONS ARE CONSTRUED NARROWLY

FOIA requires the full disclosure of public records, unless those records are exempted under MCL 15.243. The exemptions in MCL 15.243 are narrowly construed, and the burden of proof rests on the party asserting the exemption. If a request for information held by a public body falls within an exemption, the decision becomes discretionary. *Kent County Deputy Sheriffs' Ass'n v. Kent County Sheriff*, 463 Mich. 353, 360-361; 616 N.W.2d 677 (2000).

DENIALS



- The request was improperly made.
- The requested document never existed.
- The requested document was properly destroyed.
- The requested document or information is exempt from disclosure.

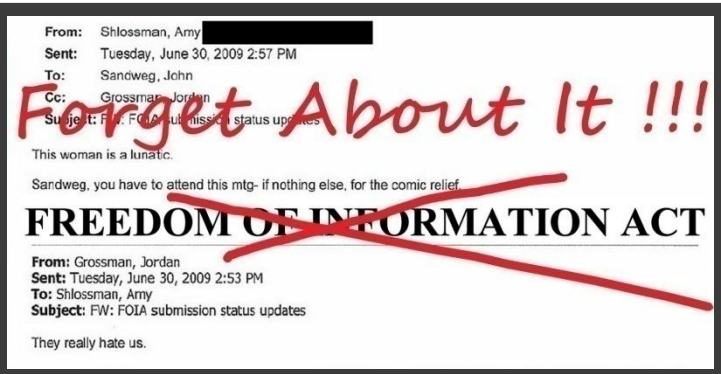
Electronic Records

- All electronic records that are created, received or stored by a government agency are the property of the government agency.
- Records created in the performance of an official function must be managed the same way as those created and received using municipal computer resources.
- Municipal employees' responsibilities for managing electronic records are the same as those for other records.
- Individual employees are responsible for deleting electronic records in accordance with the appropriate retention and disposal schedule.

Suggested FOIA Procedures

- **Personnel Authorized to Process FOIA Requests**
- **Retain All FOIA Requests on Paper**
- **Determine When A Request Is Received**
  - A non-electronic request is received as soon as it is delivered to the township mailing address, post office box, fax machine, email address OR ANY township board member, other board/commission member, official, employee, or independent contractor (assessor, building official, zoning administrator, etc.), even if in person or at their home.
  - The month, day, and year should be stamped or written in indelible ink on every non-electronic FOIA request when it is received.
  - An electronic request is received on the business day following the day the transmission is received on ANY device maintained to receive that form of transmission.
- **Separate Exempt From Non-Exempt Information**

Records Management For FOIA Compliance



- Every email message, text message and social media post must be evaluated for its content and purpose to determine the length of time it must be retained in accordance with the appropriate retention and disposal schedule. Just like paper records, email messages may be evidence of decisions and activities. All FOIA and records retention requirements must be observed for email. Both senders and recipients of messages must determine if a particular message should be retained to document their role in agency activities.

- Pursuant to state records retention schedules, **a municipality does not need to keep every document in its possession and certainly does not need to keep every duplicate copy**. The law allows municipalities to destroy documents that are not protected from destruction by statute or regulation, or needed for ongoing business purposes.

Four Categories of Electronic Communication

Records - recorded information that is prepared, owned, used, in the possession of, or retained by an agency in the performance of an official function.

Example: "After further review, it is our decision that there is not sufficient justification to approve the reallocation for Susan's position, based upon the fact that..."

Retention: Retain according to agency specific and general schedules.

Four Categories of Electronic Communications…

Transitory Records - records relating to agency activities that have temporary value and do not need to be retained once their intended purpose has been fulfilled.

Example: "The staff meetings will be held on Tuesday mornings from now on instead of Thursday afternoons.

Retention: Retain for up to 30 days.

Four Categories of Electronic Communications…

Nonrecords - recorded information in the possession of an agency that is not needed to document the performance of an official function.

Example: "The American Red Cross Blood Drive will be held in Baker-Olin West on December 20, 2009."

Retention: Destroy ASAP.

Four Categories of Electronic Communications…

Personal-records that document non-government business or activities.

Example: "Honey. My meeting is running later than expected. Please save dinner for me. Thanks."

Retention: Do not use government technology resources. Destroy ASAP.

RESPONSIBILITIES

Employee Responsibilities:

Decide which messages to keep and which to destroy as soon as possible;

Empty email trash bins to purge deleted messages frequently;

File the messages that are retained in an organized filing system; and

Identify which retention schedule mandates the message's retention or authorizes its destruction.

Management Responsibilities:

Ensure that retention and disposal schedules are accurate and comprehensive;

Adopt and distribute an email retention policy for staff;

Adopt and distribute an acceptable use/etiquette policy; and

Communicate with appropriate employees, attorneys and information technology staff when a FOIA request is received or when litigation appears imminent.

Email Retention Checklist

Case Law

Howell Education Assoc. v. Howell Board of Education

Personal emails are not public records merely because they were captured in an email system's digital memory.

Email Storage Options

Live Email System

Email System Archives

Saving Outside the Email System

Paper Printout

Microfilm

Document Management System

Record Retention Policy

Each municipality should adopt a policy that notifies employees about their responsibilities for retaining official electronic communications and identifies how they should be stored. Management, information technology staff, and attorneys should work together to finalize a policy that addresses technology resources and legal vulnerabilities.

Questions, Suggestions, Comments?