McGRAW MORRIS P.C.
ATTORNEYS

DON'T LET THIS HAPPEN TO YOU – HOW TO PREPARE YOUR MUNICIPALITY TO AVOID LITIGATION HORROR STORIES

PRESENTED BY:

STACY J. BELISLE

McGRAW MORRIS P.C.

2075 WEST BIG BEAVER ROAD

SUITE 750

TROY, MICHIGAN 48084

248.502.4000

WWW.MCGRAWMORRIS.COM

SBELISLE@MCGRAWMORRIS.COM

I. DISCOVERY OF ELECTRONICALLY STORED INFORMATION

A. Michigan Court Rule Regarding Discovery of Electronically Stored Information ("ESI")

1. 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.

a. Federal court rules are consistent with this requirement. However, production of electronically stored information is limited in the following manner:

> Absent an order of the court upon a showing of good cause or stipulation of the parties, a party from whom ESI has been requested shall not be required to search for responsive ESI:

i. from more than 10 key custodians;

ii. that was created more than five years before the filing of the lawsuit;

iii. from sources that are not reasonably accessible without undue burden or cost; or

iv. for more than 160 hours, exclusive of time spent reviewing the ESI determined to be responsive for privilege or work product protection, provided that the producing party can demonstrate that the search was effectively designed and

efficiently conducted. A party from whom ESI has been requested must maintain detailed time records to demonstrate what was done and the time spent doing it, for review by an adversary and the court, if requested.

2. **How to Proactively Manage Data**.

a. When a lawsuit is filed, stay in front of discovery requests and consider the following:

i. How will ESI come into play?

ii. How will ESI will be preserved?

iii. How will ESI be searched and what limitations will apply?

iv. How will ESI be produced?

3. **Preservation Obligations.**

a. 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.

b. Federal courts analyzing the issue examine the following:

i. Knowledge that a suit will be filed;

ii. Investigation of a possible claim by a plaintiff's attorney;

iii. Pre-litigation correspondence or pre-litigation discussions between counsel; and

iv. Filing of an administrative claim.

B. **How to Comply**.

1. Take Precautions to Prevent Discovery and Spoliation Sanctions

a. Make a good faith effort to take reasonable steps to prevent loss of data during litigation.

b. Document efforts to retain information.

2. **Issue a Litigation Hold Memorandum/Letter**

a. A prompt litigation hold is the most valuable tool for preventing user-initiated or automatic loss of data. Litigation holds can contain simple or detailed descriptions of the subject matter of the data to be preserved, and their distribution can be focused or municipality-wide. The recipients should include any known custodians, supervisors (who can inform subordinates), and information technology staff, who may even have prearranged procedures in place for holds.

3. **Identify Individuals and Systems with Responsive Information**

a. Identify record custodians early in litigation and assign responsibility for locating data.

4. **Take Action to Retain Backups**

a. Parties may be obligated to retain backups if:

i. They can identify where in the back-ups particular employees' data would be stored;

ii. The backups contain key employees' data; and

iii. The relevant information is not otherwise available from readily accessible sources.

5. **Suspend Automatic Email Deletion**

a. Systems that automatically delete e-mail after a certain time might circumvent litigation holds. Federal decisions suggest that if such deletion continues after the duty to preserve arises, data loss is outside any protection in the discovery rules. Auto-delete rules, if they pose a threat, should be deactivated for employees who are potentially in possession of relevant data until that data is captured or evaluated.

C. **Case Law**

1. **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).

a. In connection with discovery requests, the Defendant asserted that the Plaintiff did not identify which readily accessible data systems

it searched, how it searched them, or what non-readily accessible systems were not searched. In contrast, the Plaintiff asserted that it diligently searched for and produced relevant, non-privileged ESI from its readily accessible data systems, including email, group directories, user shares, personal computers and other systems, but did not search non-readily accessible sources such as disaster recovery sources which were not restorable without excessive cost and effort.

b. Federal Rule of Civil Procedure 26 provides that 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." Fed.R.Civ.P. 26(b)(2)(B). On a motion to compel, "the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost."

c. 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.

2. **Spoliation/Sanctions**.

a. "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).

i. Where a party seeks sanctions based on the spoliation of evidence, it must establish:

(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed;

(2) that the records were destroyed with a culpable state of mind; and

(3) that the destroyed evidence was relevant to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

b. "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).

i. This is an objective standard, asking not whether the party in fact reasonably foresaw litigation, but whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation. *Apple Inc. v. Samsung Electronics Co.*, 888 F. Supp. 2d 976 (N.D. Cal. 2012).

ii. The determination 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).

- In the *UBS Real Estate Securities* case, although the court found that the defendant failed to implement a timely litigation hold, it denied the request to impose sanctions for spoliation because it found that the defendant did not act in bad faith and no relevant documents were destroyed.

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

a. 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.

i. In the court's opinion, the "single-minded focus on discovery of ESI" "transformed what should have been a simple case into a discovery nightmare." "It appeared to this court on more than one occasion that plaintiffs were treating the case as a litigation workshop on discovery of ESI rather than a lawsuit."

ii. As a result, the US District Court for the Eastern District of Michigan recently approved, on a pilot period basis, the use of a model e-discovery order and checklist in appropriate cases. The model order is designed to help lower e-

discovery costs, and it imposes default limitations on the scope of preservation and review.

4. **Proportionality**.

a. 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:
>
> (i) 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;
>
> (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or
>
> (iii) 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.

b. *FDIC v. Giannoulias*, No. 12 C 1665 (N.D. Ill. Oct. 23, 2013). The court addressed three e-discovery issues:

i. Whether the producing party had to include additional search terms proposed by the requesting party;

ii. Whether the producing party had to review the documents that resulted from using search terms before producing the documents; and

iii. Whether the producing party had to organize its production to correspond to the requesting party's document requests.

- First, the court applied principles of proportionality to determine whether six additional terms should be added to the parties' agreed-upon list of 250 search

terms. The court ordered that the producing party must use four of the terms because they likely would capture relevant documents and would result in a relatively small number of additional "hits." The court did not order the use of the other two terms even though the producing party had initially proposed those terms because the likelihood of entirely irrelevant hits appeared high and the number of additional hits was substantial.

- Second, the court held that the producing party did not have to review the documents that resulted from the use of the search terms to determine if they were in fact responsive. Although the court acknowledged the general duty to produce only those documents that are responsive, the court found that it seemed likely that the vast majority of the documents generated by the parties' search terms would be relevant and that the burden to review all of those documents would outweigh any benefit to the requesting party. "False hits are probably inevitable, but we will not require the [producing party] to review thousands of documents to weed out a presumably small subset of irrelevant materials."

- Third, the court held that the producing party did not have to organize its production according to the discovery requests because it would impose a substantial burden on the party and the metadata associated with the documents could be used to sort the documents.

c. *Swanson v. ALZA Corporation*, No. 12-4579 (N.D. Cal. Oct. 7, 2013). In another case in which the requesting party sought to compel the producing party to use additional search terms, the requesting party argued that the other side had not complied with its requests for production because the search terms used to identify potentially relevant ESI were inadequate. To support its argument, the requesting party identified specific categories of documents that it believed were missing from the production. After a hearing, the court held that it would not be unduly burdensome for the producing party to perform certain of the eleven proposed Boolean searches. The court held, however, that any benefit of the remaining searches was outweighed by the burden of production.

c. *Ewald v. Royal Norwegian Embassy*, No. 11-cv-2116 (D. Minn. Oct. 8, 2013). The court in this case commented on the amount of discovery, including ESI, taken in a single plaintiff employment dispute, stating that: "The scale of discovery and diligence of the parties in pursuing information in this case, when viewed in the light of the nature of the dispute, is breathtaking." "If ever a case implicated the proportionality principles and provisions of the Federal Rules governing discovery, this case does."

i. The issue before the court was the plaintiff's motion to compel discovery. Among other things, the plaintiff requested the court to order forensic images of laptops, phones, memory cards, and tablets. The court rejected these requests largely because the plaintiff failed to raise these issues at the beginning of the case. The court explained that at the Rule 16 Conference, it directed the parties to identify sources and custodians of ESI, and that the parties subsequently negotiated an agreement regarding the discovery of ESI. Neither the agreement nor the plaintiff's initial discovery requests raised such things as text messages or voicemails as an issue.

ii. According to the court, "requesting this information so long after the production of tens of thousands of documents and the depositions of nine witnesses is an attempt to amend the [agreement] and revisit all of the ESI issues the Court urged the parties to negotiate and address in the [agreement] under their obligations in drafting and formulating a Rule 26(f) report." "To go back and engage in discovery with respect to those devices at this stage in the litigation and in light of the expenses and costs the parties have already incurred is simply not feasible. Allowing additional discovery would eviscerate Rule 26's concept of proportionality."

5. **Possession, Custody or Control.** *Puerto Rico Tel. Co. v. San Juan Cable LLC*, No. 11-2135 (D.P.R. Oct. 7, 2013).

a. 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.

i. 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."

6. **Discovery of Text Messages Ordered.** *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008)

a. 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.

b. The court determined that the text messages exchanged among city officials and employees were potentially discoverable under the Federal Court Rules and established a protocol under which two designated Magistrate Judges reviewed the messages to make an initial determination as to which of them were discoverable.

c. Because the text messages were still within the control of the individuals, as opposed to being solely within the control of the service provider and because the discovery requests were directed to the individual defendants and not the service provider, the court determined that the SCA did not prohibit production of the text messages.

d. The City's control over the SkyTel text messages was confirmed by FOIA. In particular, Michigan's FOIA, which mandates that, subject to various exceptions, a "public body shall furnish a requesting person a reasonable opportunity for inspection and examination of its public records."

i. There was no question that the City is a "public body" under FOIA and that at least some of the SkyTel text messages satisfied the statutory definition of "public records," insofar as they captured communications among City officials or employees "in the performance of an official function." Indeed, the City acknowledged that at least some of these communications were "public records," both through a policy directive promulgated to its employees -- a directive which, among other things, cautions "users of the City's electronic communications system" to "bear in mind that, whenever creating and sending an electronic communication, they are almost always creating a public record which is subject to disclosure." The City also asserted that the text

messages were privileged based on the deliberative process privilege -- a privilege which, as the City recognized, encompassed only communications among City officials and employees pursuant to "their official positions within the City of Detroit government."

e. 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.

7. **Text Messages Not Discoverable.** *Elcometer, Inc. v. TQC-USA, Inc*., 2013 U.S. Dist. LEXIS 135437, 10-11 (E.D. Mich. Sept. 23, 2013).

a. 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.

b. With respect to a third party subpoena, the court determined that it did not appear that the court had the right to enforce a civil subpoena to non-party internet service providers.

i. Citing to *Flagg*, the court determined that unless the matter falls within a specific exception, the SCA "lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a subpoena or court order."

ii. While Elcometer argued that the SCA does not trump its right to access discoverable material, it presented no authority for this proposition. In fact, the court noted that "[T]he exceptions enumerated in the SCA do not include civil discovery subpoenas.

Furthermore, the SCA does not make any references to civil litigation or the civil discovery process."

8. **Discovery of Personal Facebook Content**. *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387 (E.D. Mich. 2012).

   a. 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.

   b. The plaintiff objected to the production of her entire Facebook account, including those sections she has designated as private and were therefore not available for viewing by the general public.

   c. The court noted that there was no guiding precedent from the Sixth Circuit and that other courts reached varying conclusions as to the discovery of information posted on social networking sites such as Facebook. In two cases, the courts rejected claims that Facebook postings are privileged or that their disclosure would infringe upon a right of privacy. Instead, the cases ordered disclosure under the traditional discovery principles of Fed.R.Civ.P. 26(b), that "[p]arties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense," and that for purposes of discovery, "relevant" evidence "need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence."

      i. In both cases, the public profile Facebook pages contained information that was clearly inconsistent with the plaintiffs' claims of disabling injuries. In one case, the plaintiff alleged substantial injuries, including possible permanent impairment, loss and impairment of general health, strength, and vitality, and inability to enjoy certain pleasures of life. However, the public portion of his Facebook account contained comments about his fishing trip and his attendance at the Daytona 500 race in Florida. In the other case, the plaintiff claimed that she had sustained permanent, serious injuries that caused her to be largely confined to her house and bed. The public portions of her Facebook and MySpace accounts showed that to the contrary, "she [had] an active lifestyle and [had] traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity."

ii. But in another case, the court upheld the denial of a motion to compel Facebook information not on grounds of privacy or privilege, but because the defendant "failed to establish a factual predicate with respect to the relevancy of the evidence," finding that the "defendant essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence."

d. In the *Tompkins* case, the court agreed that material posted on a private Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy. Nevertheless, the defendant did not have a generalized right to rummage at will through information that the plaintiff limited from public view. Rather, consistent with Rule 26(b) and with case law, there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence.

9. **Improper Access to Facebook.**

a. **Statutory Protections**.

i. Some states have enacted statutes that specifically protect employees from their employers taking adverse employment action against them for legal off duty conduct. This conduct includes drinking alcohol, using tobacco products and participating in political activities. Michigan has not enacted a statute.

b. **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."

i. Under 18 U.S.C. § 2701, an offense is committed by anyone who: "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided;" or "(2) intentionally exceeds an authorization to access that facility; and thereby obtains...[an] electronic communication while it is in electronic storage in such system." However, it does not apply to an "electronic communication [that] is readily accessible to the general public." 18 U.S.C. § 2511.

ii. An employer would not violate the SCA when a search is authorized.

iii. *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.

- Ehling was a registered nurse and paramedic and also served as the president of the labor union that represented employees at the New Jersey hospital where she worked.

- On June 8, 2009, a white supremacist opened fire at the Holocaust Memorial Museum in Washington, D.C., and killed a security guard. The paramedics who responded to the scene performed emergency medical procedures on the shooter and saved his life. When Ehling heard the story, she posted a message on Facebook suggesting that the paramedics should have let the shooter die. When the hospital learned of the post, Ehling was immediately suspended.

- The post:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? And 2. This was your opportunity to really make a difference. WTF!!!! And to the other guards … go to target practice.

- The hospital learned of the post from another employee who was an online Facebook friend with Ehling. Ehling's Facebook security setting for her news feed was private so only friends could see those feeds. The co-worker accessed her posts and voluntarily provided them to the hospital.

There was no evidence that the hospital pressured the co-worker to do this.

- Ehling ultimately lost her lawsuit and the court dismissed all of her claims, including the SCA claim. However, the court made an unprecedented ruling that private Facebook postings are electronic communications that are subject to the SCA. Ehling only lost her SCA claim because the co-worker who accessed her private Facebook post and provided it to the employer voluntarily. The co-worker was, thus, an "authorized user" under the SCA.

iv. This ruling is important for a number of reasons.

- All Twitter and some Facebook posts are public. Therefore, in the case of publicly available posts, the SCA will almost never apply and employers are free to use information obtained from those posts.

- Where Facebook and LinkedIn users regulate the privacy of their posts and a post is private and not publicly available, employers who access posts without authorization or by pressuring "friends" of an employee to disclose the contents of private posts may be liable for damages under the SCA.

- In this case, the judge suggested that if the hospital pressured the co-worker to into providing it with the contents of Ehling's private Facebook posts, his decision would have been different.

- The takeaway from this case is to avoid pressuring or coercing "friends" of employees into providing private posts to the employer.

10. **Privacy Rights in the Workplace**. *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300; 990 A.2d 650 (2010).

a. 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.

b. In this case, the court addressed a narrow set of facts – emails sent by an employee from a company laptop via a web-based email account (Yahoo) to her attorney – and determined that they were protected from disclosure by the attorney-client privilege. In reaching this conclusion, the court also ruled and provided insight on a far broader and more practical issue for

employers – how to draft enforceable computer usage policies and/or make existing policies more effective. In this case, the employer had a very loose and vague email usage policy, stating only that the employer's system and electronic communication devices should only be used for work purposes, but that occasional personal use was permitted.

c. 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.

   i. The employer informed its employees that its computers were to be used for company business only and that employees were prohibited from using them to send or receive personal email. The plaintiff was warned that the company would monitor its computers for compliance with this policy and might inspect all files and messages of employees at any time. Employees were specifically warned that employees using the employer's computers for personal purposes, including email, had no right to privacy with respect to personal information or messages.

   ii. Based on this very restrictive policy, the court found that it was unreasonable for the plaintiff to believe that her personal emails, even with her own attorney, were private. The court noted that by ignoring the employer's policy and sending a message to her attorney using a work-provided email account, the plaintiff's actions were "akin to consulting her attorney in one of defendant's conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [the employer] would be privileged."

   iii. The court also noted that it was unreasonable for the plaintiff to believe that her communications were privileged simply because, to her knowledge, the employer never enforced its computer monitoring policy before.

   iv. Holmes emphasized that she believed her personal e-mail would be private because she utilized a private password to use the company computer and she deleted the e-mails after they were sent. However, her belief was unreasonable because she was warned that the company would monitor e-mail to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer. Likewise, simply because she "held onto a copy of the fax," she had no expectation of privacy in documents she sent to her

attorney using the company's facsimile machine, a technology resource that, she was told, would be monitored for compliance with company policy not to use it for personal matters.

II. **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.

A. "Access information" means user name, password, login information, or other security information that protects access to a personal internet account.

B. "Employer" means a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer.

C. "Personal internet account" means an account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data.

1. 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.

2. The act does not prohibit an employer from doing any of the following:

Requesting or requiring an employee to disclose access information to the employer to gain access to or operate any of the following:

- An electronic communications device paid for in whole or in part by the employer.
- An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes.

Disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal internet account without the employer's authorization.

Conducting an investigation or requiring an employee to cooperate in an investigation in any of the following circumstances:

- If there is specific information about activity on the employee's personal internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct.

- If the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal internet account.

Restricting or prohibiting an employee's access to certain websites while using an electronic communications device paid for in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law.

Monitoring, reviewing, or accessing electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal law.

1. The act does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

2. The act does not create a duty for an employer or educational institution to search or monitor the activity of a personal internet account.

3. An employer or educational institution is not liable under this act for failure to request or require that an employee, a student, an applicant for employment, or a prospective student grant access to, allow observation of, or disclose information that allows access to or observation of the employee's, student's, applicant for employment's, or prospective student's personal internet account.

4. Sanctions and Remedies.

   a. A person who violates the act is guilty of a misdemeanor punishable by a fine of not more than $1,000.00.

   b. An individual who is the subject of a violation of this act may bring a civil action to enjoin a violation of the act and may recover not more than $1,000.00 in damages plus reasonable attorney fees and court costs. Not later than 60 days before filing a civil action

for damages or 60 days before adding a claim for damages to an action seeking injunctive relief, the individual shall make a written demand of the alleged violator for not more than $1,000.00. The written demand shall include reasonable documentation of the violation. The written demand and documentation shall either be served in the manner provided by law for service of process in civil actions or mailed by certified mail with sufficient postage affixed and addressed to the alleged violator at his or her residence, principal office, or place of business.

c. It is an affirmative defense to an action under this act that the employer or educational institution acted to comply with requirements of a federal law or a law of this state.

III. MICHIGAN'S FREEDOM OF INFORMATION ACT: "PUBLIC RECORD"—THE BASICS:

A. There are several factors that determine whether something is a "public record" for FOIA purposes.

1. The record must be "a writing." FOIA defines a "public record" as a "writing prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, from the time it is created." MCL 15.232.

a. FOIA defines a "writing" very broadly as "handwriting, typewriting, printing, photography, photocopying, and every other means of recording, and includes letters, words, pictures, sounds, or symbols, or combinations thereof, and papers, maps, magnetic or paper tapes, photographic films or prints, microfilm, microfiche, magnetic or punched cards, discs, drums, or other means of recording or retaining meaningful content." MCL 15.232.

2. The record must be involved in the performance of an official function of the public body. Under FOIA, a record is a "public record" based on its content, depending primarily on its involvement in the performance of an official function by a public body.

IV. ELECTRONIC RECORDS:

A. An electronic record is information recorded by a computer that is produced or received in the initiation, conduct or completion of an agency or individual activity. Electronic records are public records if they are created or received as part of performing official duties.

1. Some examples of electronic records include email messages, Word documents, electronic spreadsheets, digital images and databases.

Electronic records are contained in computer networks, digital image storage systems and social media.

B. **Preliminary Issues.**

1. **All electronic records that are created, received or stored by a government agency are the property of the government agency**. They are not the property of its employees, vendors or customers. Employees should have no expectation of privacy when using a municipality's computer resources.

2. Electronic records created in the **performance of an official function** must be managed the same way as those created and received using municipal computer resources.

3. **Municipal employees' responsibilities for managing electronic records are the same as those for other records**. Employees are responsible for organizing their electronic records so they can be located and used. Employees are responsible for using an approved retention and disposal schedule to identify how long electronic records must be kept. Employees are responsible for keeping electronic records for their entire retention period and for deleting electronic records in accordance with an approved retention schedule.

4. **Individual employees are responsible for deleting electronic records in accordance with the appropriate retention and disposal schedule**. However, deleted electronic records may be stored on backup tapes for several days, weeks or months after they are deleted. Municipalities need written procedures for ensuring that deleted electronic records are rendered unrecoverable on a regular basis. Keep in mind that electronic records cannot be destroyed if they have been requested under FOIA or if they are part of on-going or anticipated litigation, even if their retention period has expired.

C. **Suggested FOIA Procedures**.

1. **Personnel Authorized to Process FOIA Requests:**

a. A municipality must have a FOIA compliance plan and must designate a FOIA coordinator. The FOIA coordinator should designate others to act as assistant FOIA coordinators or to serve as a FOIA contact. Establish a "chain of command" using different titles and job descriptions so the procedure is clear.

b. All FOIA requests must be directed to the FOIA coordinator if the person who received the request is not authorized to respond to the request.

2. **Retain All FOIA Requests on Paper:**

   a. Any FOIA request that is not originally submitted on paper should be printed and retained on paper. If a verbal request was made, the request should be transferred to paper, printed and retained. This allows compliance with the rule that FOIA requests must be kept on file for at least one year.

   b. A specific FOIA request form should be developed and used for all requests. The municipality should develop a worksheet that contains the following information: date request is received, date response is due, copying costs for documents, discs and tapes (whether municipal or outside resources are used), envelopes, postage and labor costs.

3. **Determine When A Request Is Received:**

   a. A non-electronic request is received <u>as soon as it is delivered</u> to the municipality's mailing address, post office box, fax machine, email address OR ANY member of the municipality's governing body, other board/commission member, official, employee, or independent contractor (assessor, building official, zoning administrator, etc.), even if in person or at their home.

   b. The month, day, and year should be stamped or written in indelible ink on every non-electronic FOIA request when it is received.

   c. 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.

4. **Separate Exempt From Non-Exempt Information:**

   a. A fee should not be charged for the cost to search, examine, review, delete, separate or redact exempt from non-exempt information unless failure to charge a fee would result in unreasonably high costs.

   b. FOIA does not require a public body to create a new record summarizing non-exempt material.

   c. Additionally, a FOIA response should reiterate the items requested and must include a statement regarding the appeal process, by restating the entire text of FOIA's appeal provision.

V. RECORDS MANAGEMENT FOR FOIA COMPLIANCE:

A. Every email message, text message, social media post or other form of electronic communication 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, texts and social media posts may be evidence of decisions and activities. All FOIA and records retention requirements must be observed for email, text and social media posts. Both senders and recipients of messages must determine if a particular message should be retained to document their role in agency activities.

B. 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.

VI. RETENTION OF ELECTRONIC COMMUNICATIONS:

A. In recent years, email and text messages have been a source of substantial liability. Public officials and government employees have been caught using electronic messaging systems inappropriately, saying things they did not want to publicly acknowledge, or destroying records unlawfully. Given the prevalence of email, texting and social media in today's workplace, it is absolutely essential that a management plan have detailed procedures with regard to electronic communications.

B. If messages are destroyed on a regular basis, in accordance with approved retention and disposal schedules, they may no longer exist when a FOIA request is received. In that case, an organization will not be penalized for not releasing the record because destruction pursuant to a records retention schedule is a legal basis for denying a FOIA request.

C. FOUR CATEGORIES OF COMMUNICATIONS:

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

a. **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..."

b. **Retention:** Retain according to agency specific and general schedules.

2. **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.

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

   b. **Retention:** Retain for up to 30 days.

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

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

   b. **Retention:** Destroy ASAP.

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

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

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

D. **When to save an electronic communication**.

1. Even where the substance of an electronic communication recommends its retention, the identity of the sender or receiver may relieve a municipality of this obligation.

2. If the same message by that sender already exists elsewhere, duplicate copies should be destroyed.

3. If the recipient was copied on the message, but was not assigned a task as a result of the message, the recipient's copy should be destroyed.

4. Original copies of all electronic "records" generated by a sender should be retained. Additions to an email string of new substantive "record" material and/or new individuals assigned a task as a result of the message should be retained.

   i. When it comes to message strings, retain only the last message in the conversation, if it includes the content of all the previous messages.

ii. Make retention decisions right away. The longer you wait to clean out messages, the harder it will be to remember which messages are important. The email trash bin should be emptied daily.

VII. RESPONSIBILITIES:

A. EMPLOYEE RESPONSIBILITIES:

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

2. Empty email trash bins to purge deleted messages frequently;

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

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

B. MANAGEMENT RESPONSIBILITIES:

1. Ensure that retention and disposal schedules are accurate and comprehensive;

2. Adopt and distribute an email retention policy for staff;

3. Adopt and distribute an acceptable use/etiquette policy; and

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

C. ELECTRONIC COMMUNICATION RETENTION CHECKLIST:

1. Do I need to keep this message to document my work? Is it evidence of the official function of a public body?

2. Is the message string completed, or could additional messages follow that I will want to retain?

3. Are the other records about this topic/issue/case kept in a hardcopy file or an electronic file?

4. Is this a message that my co-workers are receiving too? Am I responsible for retention or is someone else responsible?

5. Should this message be stored in a shared file? Do my co-workers need to access it?

VIII. CASE LAW

A. *Howell Education Assoc. v. Howell Board of Education,* 287 Mich. App. 228; 789 N.W.2d 495 (2010).

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

a. The case stems from a series of FOIA requests to the Howell Public School System seeking all emails sent to and from three teachers between January 1, 2007 and March 2007. The teachers were also officials of the teachers' union, the Howell Education Association, and the FOIA requests arose out of contested negotiations for a new collective bargaining agreement. The union objected to having to release union communications and took the position that the emails were not public records. The union's attorney informed the union that there was no case law regarding the issue of whether personal emails or internal union communications maintained on the computer system of a public body were public records subject to disclosure under FOIA. Counsel suggested that the parties participate in a "friendly" lawsuit to determine the applicability of FOIA to the requested emails.

b. The court of appeals' decision has nothing to do with FOIA's privacy exemption. The court determined that personal emails are not necessarily public records, not that the emails were exempt for containing private or personal information. "Some documents are not public records because they are private while other documents are public records but will fall within the privacy exemption." An employee's personnel file is a public record but private information like addresses and phone numbers are exempt and may be redacted. A personal email is not considered a public record and is not subject to production under FOIA on that basis. Personal emails are messages that are created for a clearly personal purpose, such as lunch or dinner plans, childcare or carpooling.

c. The defendants asserted that the emails were rendered public records because the school district's email use policy warned that all emails were the property of the school district and use of the email system for personal use was prohibited. The court of appeals disagreed. While personal emails may be viewed by the employer or properly produced in response to a subpoena or discovery request in litigation on the basis of this policy, emails are not public records unless they relate to an official function of the municipality.

d. The defendants also tried to argue that personal emails are transformed into public records because they violate the public agency's email use policy. The court of appeals disagreed. In fact, an employee's violation of an email use policy actually supports the conclusion that such emails are not public records, because they are personal in nature and, thus, violate the email policy.

e. A document that is not initially considered a public record (for example, a letter from a resident to a Township supervisor regarding the municipality's water system) may be transformed into a public record based on how the municipality uses it (such as reading it aloud at a Township Board meeting). However, it is only the document's subsequent use or retention "in the performance of an official function" that renders such documents public records. Mere retention of emails by a public agency without more is not a use that renders a document a public record. A municipality's email backup system is not an official function sufficient to render the emails at issue public records subject to FOIA.

f. The court noted that in another case (*WDG Investment Co. v. Dep't of Mgt. & Budget*, unpublished opinion of the Michigan Court of Appeals, Docket No. 229950 (issued November 14, 2002)), it refused to exempt documents from disclosure as public records under FOIA merely because they were an individual's personal notes. However, that is different from this case because those personal notes were taken in the course of the individual's participation in awarding a bid.

g. In another case (*Hess v. City of Saline*, unpublished opinion of the Michigan Court of Appeals, Docket No. 260394 (issued May 12, 2005)), the court determined that a video that recorded city officials talking after a council meeting was not a public record merely because the city retained a copy of the tape. The court compared that decision to the present case. Similarly, simply because the public agency here retained personal emails did not mean that they were public records.

h. A public agency's subsequent use of personal emails can render those emails public records. For instance, if a teacher was disciplined for violating the school district's email policy and the emails were used to support the discipline, they would then be considered public records.

i. The court also considered whether emails involving internal union communications are personal emails. The court determined that such emails were personal and not public records. Specifically, the

> court concluded that "such communications do not involve teachers acting in their official capacity as public employees, but in their personal capacity as [union] members or leadership. Thus, any emails sent in that capacity are personal. . . . The release of emails involving internal union communications would only reveal information regarding the affairs of a labor organization, which is not a public body."

B. The Arizona Supreme Court held in *Griffis v. Pinal County*, 215 Ariz. 1; 156 P.3d 418 (2007), that emails sent and received by a former county manager on a government-owned computer during a specific time period were not public records subject to disclosure under Arizona's FOIA equivalent. In holding that all information on a computer was not automatically a public record, the Arizona Supreme Court reasoned that "only those documents having a 'substantial nexus' with a government agency's activities qualify as public records" and ultimately held that "because the nature and purpose of the document determines its status, mere possession of a document by a public officer or agency does not by itself make that document a public record, nor does the expenditure of public funds in creating the document."

C. In *Denver Publishing Co. v. Board of County Commissioners of Arapahoe*, 121 P.3d 190 (2005), the Colorado Supreme Court analyzed a trial court order that required disclosure of all email communications between a county recorder and assistant chief deputy. The court explained that "[t]he simple possession, creation, or receipt of an e-mail record by a public official or employee is not dispositive as to whether the record is a 'public record.' The fact that a public employee or public official sent or received a message while compensated by public funds or using publicly-owned computer equipment is insufficient to make the message a 'public record.'" The Colorado Supreme Court held that to be public record, the requested emails had to have "a demonstrable connection to the performance of public functions."

D. In *Florida v. City of Clearwater*, 863 So.2d 149 (2003), the Florida Supreme court held that "private documents cannot be deemed public records solely by virtue of their placement on an agency-owned computer. The determining factor is the nature of the record, not its physical location." In this case, the city had a "Computer Resources Use Policy." The court held that such a policy "cannot be construed as expanding the constitutional or statutory definition of public records to include 'personal' documents."

E. In *Schill v. Wisconsin Rapids School District*, 327 Wis. 2d 572; 786 N.W. 2d. 177 (2010), the Wisconsin Supreme Court examined a request for all emails of public school teachers sent and received via school district email accounts on school district-owned computers. Ruling that such emails were not records under Wisconsin's Public Records Law, the court stated that "while government business is to be kept open, the contents of employee's personal emails are not a

part of government business" simply because they are sent and received on government email and computer systems.

F. *Hopkins v. Twp. of Duncan,* 294 Mich. App. 401; 812 N.W.2d 27 (2011).

1. A township resident filed a complaint against the township alleging a violation of FOIA after the township did not produce any records responsive to his request for copies of any notes taken by any elected official during a township board meeting. The township filed a motion to dismiss the case and submitted affidavits revealing that only one specific individual took notes at such a meeting, the notes were strictly for his personal use, they were kept in his personal journal, they were not shared with other members of the township board, and they were never placed in the township's files. The trial court granted the township's motion and the decision was upheld on appeal.

a. The appellate court found that **the handwritten notes of a township board member taken for his personal use, not circulated among other board members, not used in the creation of the minutes of any of the meetings, and retained or destroyed at his sole discretion, were not "public records" subject to disclosure under FOIA.**

G. *Adamski v. Township of Addison,* 2005 Mich. App. LEXIS 1194 (May 12, 2005).

1. The plaintiff requested a copy of an audio tape of a Township Board meeting. The township denied the plaintiff's request on the basis that the township's Board Meeting Guidelines provided that the copies of such tapes were only available until written meeting minutes were approved. However, the township also informed the plaintiff that she "may come to the township and listen to the tape." The township only provided the actual tape after the plaintiff filed her lawsuit.

2. The primary issue on appeal was the extent of attorney fees the plaintiff was entitled to for having to force compliance by filing a lawsuit.

3. On appeal, the court ruled that the plaintiff was entitled to attorney fees from the date the lawsuit was filed through the conclusion of the lawsuit because FOIA specifically states that an award of costs is proper where compliance with FOIA occurs only by filing a lawsuit.

H. *City of Warren v. City of Detroit*, 261 Mich. App. 165; 680 N.W.2d 57 (2004).

1. The plaintiff submitted a FOIA request seeking the formula for the rate the City used to calculate water and sewer fees. In response, the City claimed that the formula was "software," for which there is a disclosure exemption under MCL 15.232(f).

2. The court rejected the argument that where a formula is contained in a software program, the formula is inextricable and thus exempt from FOIA disclosure as a matter of law. The court determined that the plain language of the statute supported this conclusion. The burden of proving otherwise was on the City.

3. In addition, the City is obligated by statute to set its water rates "based on the actual cost of service as determined under the utility basis of rate-making" under MCL 123.141(2). It was precisely that formula that the plaintiff sought. In light of the purpose of FOIA – to facilitate the public's understanding of the operations and activities of government—the court concluded that the information the plaintiff sought was subject to disclosure.

IX. ELECTRONIC COMMUNICATION RETENTION POLICY:

A. Each municipality should adopt a policy that notifies employees about their responsibilities for retaining official email records and identifies how email should be stored. Supervisors/department heads, information technology staff, and attorneys should work together to finalize a policy that addresses technology resources and legal vulnerabilities.

Through an email retention policy, a municipality should do the following:

1. Explain the basis for the policy and why it is necessary. The policy should explain what email is and that it includes attachments and metadata. It should explain the relationship between emails, public records and FOIA and should state that emails created, used and stored on a personal computer can be public records, depending on their use.

2. Define terms such as email, retention schedules, FOIA coordinator, litigation coordinator, public record and FOIA.

3. State the responsibilities of the employee, management and the FOIA and/or litigation coordinator regarding email messages.

4. Identify different types of email messages (i.e., public records, transitory records, personal records) and explain to the employee how those emails are to be stored. The policy should provide the municipality's method for storing email messages in email folders using the live or archived section of the email program, other electronic storage method, if printing and physical storage is required or that the municipality utilizes a data management system. The policy should explain how the employee must categorize emails and how to utilize the selected storage system. If training is necessary, the training should be identified in the policy.

5. State that senders are generally considered to be the person of record for an email message. However, if recipients of the message take action as a result of the message, they should also retain it as a record.

6. Require that employees retain only the final message in a communication string that documents the contents of all previous communications. This is preferable to retaining each individual message, containing duplicate content.

7. Require that each employee evaluate the content and purpose of each email message to determine which retention and disposal schedule defines the message's approved retention period.

8. Require that employees retain email that has not fulfilled its legally mandated retention period by printing the email and placing it in the appropriate file location corresponding with the content and purpose of the email, if this is the applicable storage method.

9. Require that employees retain transactional information with the email message if there is a substantial likelihood of relevancy to ongoing or anticipated litigation.

10. Require that employees dispose of transitory, non-record and personal email messages from the email system.

11. Direct employees to dispose of email messages that document the official functions of the agency in accordance with an approved Retention and Disposal Schedule. Note that public records, including email, may not be destroyed if they have been requested under FOIA, or if they are part of ongoing or anticipated litigation, even if their retention period has expired.

12. Require employees to provide access to their email to the FOIA or litigation coordinator upon request.

13. State that email messages that are sent and received using the municipality's email system are not private and that employees are encouraged to manually delete personal appointments (such as sick leave or annual leave) from the email system after the event takes place.

14. Explain that the municipality shall ensure that its records are listed on an approved Records Retention and Disposal Schedule.

15. Explain that the municipality shall ensure that all employees with email accounts are aware of and implement the email retention policy.

16. Explain that the municipality shall notify its Information Technology Specialist (if there is one) when the accounts of former employees can be closed.

17. Explain that the municipality shall ensure that the email messages and other records of former employees are retained in accordance with approved Retention and Disposal Schedules.

18. Explain that the municipality shall notify the FOIA or litigation coordinator when it becomes involved in litigation or receives a FOIA request.

19. Explain that the FOIA or litigation coordinator shall determine whether records requested by the public are stored in the municipality's email system, regardless of whether the request seeks emails.

20. Provide that the FOIA or litigation coordinator shall notify affected employees that a FOIA request involving email was received to prevent the destruction of relevant messages.

21. To prevent the destruction of relevant messages, provide that the FOIA or litigation coordinator may, in appropriate instances, notify the municipality's Information Technology Specialist (if there is one) that a FOIA request involving email was received.

22. Provide that the FOIA or litigation coordinator shall identify all email records relevant to ongoing or anticipated litigation to which the municipality is a party.

23. Provide that the FOIA or litigation coordinator shall notify the municipality's Information Technology Specialist (if there is one) that email which is the subject of a FOIA request or related to litigation cannot be destroyed until after the case is closed, even if the applicable retention period has expired.