International Municipal Lawyers Association

2013 Annual Conference
San Francisco, California

Work Session IX: Open Meetings Act: Electronic Records
(Electronic Records / Electronic Advances / Open Meetings Act)

Public Information Acts and their Adaptation (or lack thereof) to Electronic Documents

Hilary Ruley
Assistant Solicitor
Baltimore, Maryland

©2013 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2013 Annual Conference, held September 29 – October 2, 2013 in San Francisco, CA. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Public Information Acts and their Adaptation (or lack thereof) to Electronic Documents

Contents

I. Introduction page 3

II. How are e-mails treated? page 3

III. When is an electronically stored dataset a record? page 7

IV. When is a government "capable" of extracting electronic data? page 10

V. Is metadata part of a public record? Should it be? page 15

VI. Conclusion page 23

Public Information Acts and their Adaptation (or lack thereof) to Electronic Documents

I. Introduction

> "We find ourselves in the situation akin to that of a court being asked to apply the laws governing transportation adopted in a horse and buggy world to the world of automobiles and air transportation."[1]

Attorneys must interpret current government records laws to determine if a particular electronic document must be disclosed. There is no consensus among jurisdictions about which electronic documents are subject to disclosure. Although many states look to the federal law as a guide, it has not addressed every aspect of electronic records, nor is it always possible to model the federal approach in states that have different statutory schemes. The most common record, the e-mail, is not even mentioned by name in many state records laws. Other electronic records, such as databases, are problematic because there is usually a difference between the vast amount of electronic information stored in a government computer and the reports that the software programs on that computer are able to produce from that database. Is a requestor entitled to a copy of the entire database or just the particular data complications (*i.e.* reports) utilized by the government in its operations? Even when a jurisdiction determines that a particular electronic record is subject to disclosure, there is rarely any guidance on whether the metadata associated with that record must also be disclosed. Attorneys assisting government clients in answering requests for electronic records must face common questions: how are e-mails treated? When is an electronically stored dataset a record? Is the government "capable" of extracting electronic data? Is metadata part of a public record? Should it be? This paper will address each of these common questions so that attorneys can better assist government clients in responding to requests for electronic records.

II. How are e-mails treated?

The most commonly thought of electronic document is an e-mail. Yet, not all public information act statutes specifically list e-mails as records of the government. The federal Freedom of Information Act ("FOIA" codified at 5 USC §551 *et. seq*.) certainly captures e-mails as public records. *See, e.g., United Am. Fin., Inc. v. Postmaster General Potter*, 531 F. Supp. 2d 29, 44-45 (D.D.C. 2008). Although some states specifically include e-mails in the definition of a record,[2]

---

[1] *Howell Educ. Ass'n MEA/NEA v. Howell Bd. of Educ.*, 789 N.W.2d 495, 499 (**Mich**. Ct. App. 2010).

[2] *See, e.g.*, **Cal**. Gov. Code §6252(g); **Colo.** Rev. Stat. §§24-72-202, 24-72-204.5; **Fla**. Stat. §§119.001(12), 668.6076; **Ga**. Code §§50-18-71(f), (g); **Ill**. Comp. Stat. §140/2(c); **Mo**. Stat. §610.025; **Mont**. Code §§2-6-101(2), (3); **R.I**. Gen. Laws §38-2-2(4); **Tenn**. Code. §10-7-512(b); **Wyo**. Stat. §§9-2-401(v), 16-4-201(v), (x); *see also* **Tex**. Gov't Code §552.146 (listing certain

many public records laws are silent on whether e-mails are included, instead defining records broadly to include information in any format.[3] A court or a state's attorney general usually finds that e-mails are captured within these broad definitions.[4]

Nevertheless, the absence of a statutory provision squarely addressing this common electronic document can be problematic. For example, in Alabama, the statutory definition of a record subject to public review is "all written, typed or printed books, papers, letters, documents and maps." Ala. Code §41-13-1. Although it also includes, "any other public record authorized by law" it does not specifically provide that e-mails are included. Although a recent case suggests that e-mails could be received in response to a records request, *see Tenn. Valley Printing Co. v. Health Care Auth.*, 61 So. 3d 1027, 1029 (Ala. 2011), without a legislative pronouncement on whether e-mails are records subject to disclosure, the matter is left to judicial interpretation. This gives very little guidance to attorneys tasked with instructing a client about where to search for documents responsive to a request for information. However, because the clear national trend is to include e-mails as public records, it behooves attorneys to instruct government clients that e-mails should be included in any search for responsive records.

Additionally, it is important to note that many courts consider e-mails as public records only if they concern public business, thereby not requiring production of a personal e-mail sent or received at a government employee's work e-mail address.[5] There is also some movement towards requiring the production

---

types of e-mails that are exempt from disclosure, implying the general rule that the others are able to be disclosed).

[3] *See, e.g.*, **Alaska** Stat. §40.25.110 *et. seq.*; **Conn**. Gen. Stat. §§1-200(5), 1-211(a); 29 **Del**. C. §10003(h); **D.C.** Code §2-502(18); **Haw**. Rev. Stat. §92F-1 *et. seq.*; **Idaho** Code §9-338, *et. seq.*; **Ind**. Code §5-14-3-2(m); **Kan**. Stat. §45-217(g); **Ky**. Rev. Stat. §61.870(2); **Louisiana** SA-R.S. §44:1(A)(2)(a); 1 **Me**. Rev. Stat. §402.3; **Md**. Code., State Gov., §10-611(g); **Mass**. Gen. Laws, Ch. 4, §7(26); R.R.S. **Neb**. §84-712.01(1); **Nev**. Rev. Stat. §239.010.4; **N.H.** Rev. Stat. §91-A:1-a.III; **N.J**.S.A. §47:1A-1.1; **N.M**. Stat. §14-3-2(f); **N.Y.** CLS, Pub Off., §86.4; **N.C**. Gen Stat §132-1(a); **N.D**. Cent. Code, §§44-04-18.2-.18.3; **Ohio** Rev. Code §149.43(F)(2)(d); 51 **Okla**. St. §§ 24A.1- 18 *et. seq.*; **Or**. Rev. Stat. §§192.410(6), 192.4301(1); 65 **Pa**. Stat. §67.101; **S.C**. Code §30-4-10; **S.D**. Codified Laws §1-27-1 *et. seq.*; **Utah** Code §63G-2-101 *et. seq.*; 1 **Vt.** Stat. §315 *et. seq.*; **Va**. Code §2.2-3700 *et. seq.*; **Wash**. Rev. Code §42.56.001 *et. seq.*; **W. Va**. Code §29B-1-1; **Wis**. Stat. §19.31 *et. seq.*

[4] *See, e.g.*, **Haw.** Off. Info. Pract., Op. Ltr. No. 04-12, 3 (2004) ("Records of e-mail communications should be treated no differently than records maintained in written form."); *Cowles Publ'g Co. v. Kootenai County Bd. of County Comm'rs*, 159 P.3d 896, 901 (**Idaho** 2007); *St. Tammany Parish Coroner v. Doe*, 48 So. 3d 1241, 1246 (**La**. Ct. App. 2010); *Reno Newspapers, Inc. v. Gibbons*, 266 P.3d 623, 625-26 (**Nev**. 2011); *McGee v. Township of East Amwell*, 7 A.3d 785, 792 (**N.J**. Super. Ct. App. Div. 2010); **New York** Comm. On Open Gov't FOIL-AO-13444 (July 10, 2002); *State ex rel. Wilson-Simmons v. Lake County Sheriff's Dep't*, 693 N.E.2d 789, 793, n.1 (**Ohio** 1998); *Easton Area Sch. Dist. v. Baxter*, 35 A.3d 1259, 1264 (**Pa**. Commw. Ct. 2012); *Hill v. Fairfax County Sch. Bd.*, 83 Va. Cir. 172, 177 (**Va**. Cir. 2011); *Forbes v. City of Gold Bar*, 288 P.3d 384, 389 (**Wash**. Ct. App. 2012).

[5] *See, e.g., Griffis v. Pinal County*, 156 P.3d 418, 421 (**Ariz**. 2007); *Pulaski County v. Ark. Democrat-Gazette, Inc.*, 260 S.W.3d 718, 725 (**Ark**. 2007); *State v. City of Clearwater*, 863 So. 2d

of e-mails concerning public business that are on a private device. *See, e.g., City of Champaign v. Madigan et. al.*, 2013 IL App (4th) 120662, 2013 Ill. App. LEXIS 481 (Ill. App. Ct. 2013). In this recent Illinois case, the City of Champaign argued that the personal e-mails, texts and twitter posts sent from a private device by one individual were not records of a public body and therefore were not subject to disclosure under Illinois' public records law. *Id*. at *P30 - *P33, 2013 Ill. App. LEXIS 481 at **15-**18. The Court held that one councilmember is not a public body if he or she receives or sends a message about public business from a personal device at home, which makes that communication not subject to disclosure under the Illinois record law. *Id*. at *P40 -*P42, 2013 Ill. App. LEXIS 481 at **22-**24. However, the court held that if a councilmember is sending or receiving a message about public business from a personal device while engaged in a council meeting with a quorum present, then the message is subject to the records law. *Id*. at *P42, 2013 Ill. App. LEXIS 481 at **24-**25. Similarly, if that message received at home is forwarded to a quorum of councilmembers, the message would also be subject to the records law. *Id*. at *P41, 2013 Ill. App. LEXIS 481 at **24. Any messages about public business, sent at any time, from a publicly issued device were subject to the records law. *Id*. at *P41, 2013 Ill. App. LEXIS 481 at **24. This requires government attorneys to determine what device sent the message, whether the message concerns public business, and whether a quorum was present when the message was sent.

It remains to be seen if other governments adopt a similarly detailed analysis to determine if e-mails that originate from a personal device are subject to public records laws. Currently, the trend appears to be that an e-mail is considered subject to the public records laws only if the government has the ability to search for it. Kansas, for example, has taken the approach that an e-mail is subject to the law only if it is maintained on a government owned computer or device such that the government can access it. *See, e.g.*, 2002 Kan. AG Op. 2002-1, 2002 Kan. AG LEXIS 6, *8-*9. In Georgia, a request for "electronic messages, whether in the form of e-mail, text message or other format" should contain information "reasonably calculated to allow the recipient of the request to locate the messages sought," which would include the specific name and title of the person whose messages are sought and "to the extent possible, the specific databases to be searched." Ga. Code §50-18-7(g). E-mails existing only on back-up tapes are not defined as public records in Georgia, likely because they are difficult to retrieve. *Griffin Indus. v. Ga. Dep't of Agric.*, 720 S.E.2d 212, 216 (Ga. Ct. App. 2011). Similarly, Kentucky's attorney general has opined that the government does not need to search for deleted e-mails unless the requesting party can show they were deleted in violation of Kentucky's record retention laws. Ky. OAG 06-ORD-022, p.6, 8-9; *accord State ex rel. Toledo Blade Co. v.*

149, 152-53 (**Fla**. 2003); 2002 **Kan**. AG Op. 2002-1, 2002 Kan AG LEXIS 6, *8-*9; *Howell Educ. Ass'n MEA/NEA v. Howell Bd. of Educ.*, 789 N.W.2d 495, 500 (**Mich**. Ct. App. 2010); *AP v. Canterbury*, 688 S.E.2d 317, 320 (**W. Va**. 2009); *Schill v. Wis. Rapids Sch. Dist.*, 786 N.W.2d 177, 183 (**Wis**. 2010).

Seneca County Bd. of Com., 899 N.E.2d 961, 972 (Ohio 2002)(if the applicant establishes that e-mails were deleted against the government's records retention policy, the court may evaluate whether the government should pay for a forensic scan of the computer to retrieve them).

Some states have addressed disclosure of e-mails from the public to elected officials. For example, in Delaware, e-mails sent to or from a member of the Delaware General Assembly are not subject to Delaware's records law. 29 Del. C. §10002(l)(16). In contrast, some states require that governments post a notice warning the public that e-mail addresses can be disclosed in response to a request for public information. *See, e.g.*, Fla. Stat. §668.6076. In some states personal (non-governmental) e-mail addresses will be kept confidential. *See, e.g.*, 5 Ill. Comp. Stat. §140/2(c-5); Minn. §13.601(c)(3)(whether an e-mail address is subject to disclosure depends on whose e-mail it is). In Maryland, the General Assembly considered several bills in its last session concerning e-mail addresses of citizens that contact the government. One bill would have mandated a notice on websites that e-mail addresses used to contact the government were subject to disclosure in a public records request, similar to Florida's requirement. 2013 Maryland SB 844. Another bill exempted from disclosure the part of a record containing an e-mail address "that was provided for the purpose of or in the course of communicating with a unit or instrumentality of the State or of a Political Subdivision" unless that e-mail address was "the only way to identify the person in interest," in which case the government must disclose the address. 2013 Maryland SB 845. The inherent problem in that approach, however, was that it would turn a request for a record containing an e-mail address into a laborious search of all of the custodian's records to determine if that same e-mail address was listed anywhere else. Additionally, it would require custodians to determine the purpose behind the electronic communication with the government. Neither of these two bills passed the Maryland General Assembly, and it is unclear if there is momentum to revive them in the next session.

There likely will be a revival of 2013 Maryland Senate Bill 880, which would have exempted from disclosure a database of e-mail addresses provided to the government "for the purpose of or in the course of communicating with a unit or instrumentality of the State or of a Political Subdivision." An individual e-mail address in the database could be disclosed in response to a public information act request if it was provided to the government in the course of an existing (or in seeking to establish) a business or contractual relationship. This bill was introduced because politicians found themselves in the uncomfortable position of releasing their database of constituent e-mail addresses (likely gathered when citizens sought to be on a newsletter mailing list) to opponents during election time. Assuming a version of this bill is introduced at the next Maryland General Assembly session, it will need to address the same burden that 2013 Senate Bill 845 created, namely requiring the government to determine if an e-mail address found in one record was the only way that the person communicated with the government.

E-mails are commonplace in government business and most jurisdictions recognize that they should be searched when responding to a request for public records. Some jurisdictions also address disclosure of e-mails contained on private devices and e-mails to government employees from members of the public.

III. When is an electronically stored dataset a record?

The well respected Sedona Conference, a non-profit organization studying the policies and practices involved with complex legal issues, distinguishes between "information" (defined as everything from thoughts to telephone message slips) and "records" (a subset of information that an organization decides has value, such as a particular spreadsheet). *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, Second Edition, November 2007, p. 2-3.[6] For example, an electronic database may include much information, but the software program that contains that database may print only certain reports of useful subsets or arrangements of that information. Is the entire electronic database a record or is it merely the reports that the software program can generate? Determining whether and/or when information is a "record" requires "fixing points in time when the data should be considered to be a record." *Id*. at 3. No single professional standards organization has comprehensively defined when a grouping of electronic information should be considered a record. *Id*. at 4 (citing ANSI-American National Standards Institute, AIIM-Association for Information and Image Management, ARMA-International Association of Records Managers and Administrators and ISO-International Organization for Standardization).

The federal government is clear that a record includes any electronic information. 5 USC §552(a)(3)(C); 5 USC §552(f)(2)(A); *see e.g., Yeager v. DEA*, 678 F.2d 315, 321 (D.C. Cir. 1981)("computer-stored records, whether stored in the central processing unit, on magnetic tape or in some other form, are still 'records' for purposes of the FOIA")(citation omitted). This includes the raw statistical data that is the basis of any reports. 5 USC §552(e)(3). Under FOIA, the source code (data created by the computer program and visible on the computer screen) is considered part of the record. *See, e.g., Boyd v. BATF*, 496 F. Supp. 2d 167, 171 (D.D.C. 2007)(the source code "relates to the software applications that identify how the displayed record was retrieved: specifically, the software program mapping code, the routing codes within the program that allows the query to move from screen to screen, and the codes that allow movement to other programs from the displayed screen."). These source codes are "data displayed on screen prints," making them different from the metadata that would

[6] A Project of the Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production, Copyright 2007 The Sedona Conference, available at https://thesedonaconference.org/publication/Managing%20Information%20%2526%20Records (cited with permission).

not be seen by the computer user. *Id*. The source code may be redacted if it falls into an existing exemption, usually if it would aid in the unauthorized access to the computer system. *Id*.; *accord Lewis-Bey v. DOJ,* 595 F. Supp. 2d 120, 131 (D.D.C. 2009).

As noted in the discussion on e-mails, many state record laws do not mention electronic information specifically, instead defining a record broadly to include information in any form. Alabama, highlighted in the discussion on e-mails for its markedly outdated definition of a public record, convened an open records committee in 2005 and 2006, tasked with proposing a draft of a new law. Ala. Code §§36-12-40; 41-13-1. So far there have been no legislative changes.

Other state records laws specifically include electronic information as a type of record subject to public disclosure absent an applicable exemption.[7] Some jurisdictions take care to protect certain types of electronic information from mandatory disclosure.[8] Additionally, there is a growing body of case law, and an increasing number of statutes, addressing whether or not the software programs themselves are considered electronic records, with mixed results.[9]

---

[7] *See, e.g.*, **Ariz.** Rev. Stat. §41-151.18; **Ark**. Code §§25-19-103; 25-19-108 (specifically including computer databases); **Cal**. Gov. Code §6252; **Colo.** Rev. Stat. §24-72-202(7); **Conn**. Gen. Stat. §1-211(a); **D.C**. Code §2-502(18); **Ga**. Code §50-18-70(b)(2); **Idaho** Code §9-337(16); 5 **Ill**. Comp. Stat. §140/2(c); **Ind**. Code §5-14-3-2(m); **Iowa** Code §22.1.3.a; **Kan**. Stat §45-217(g); **Ky**. Rev. Stat. §61.870(2); **Louisiana** SA-R.S. §44:1(A)(2)(a); 1 **Me**. Rev. Stat. §402.3; **Mass**. Gen. Laws, Ch. 4, §7(26); **Mich**. Comp. L. §15.232(e); **Minn**. §13.02, Subd. 7; **Miss**. Code §25-61-3; **Mo**. Stat. §610.010(6); **Mont**. Code §2-6-110; R.R.S. **Neb**. §§84-712.01(1), 84-1202(3); **N.H.** Rev. Stat. §91-A:1-a.III; **N.J**.S.A. §47:1A-1.1; **N.Y.** CLS Pub. Off. §86.4; **N.C**. Gen. Stat. §132-1(a); **N.D**. Cent. Code, §44-04-18.2-.3; **Ohio** Rev. Code §149.43(F)(2)(d); 51 **Okla**. St. §24A.3.1; **Ore**. RS §§192.410(6); 192.430(1); 65 **Pa** .Stat. §67.102; **R.I**. Gen. Laws §38-2-2(4); **S.D**. Codified Laws §1-27-1.1; **Tenn**. Code §10-7-503(a)(1)(A); **Tex**. Gov't Code §552.002(b),(c); **Utah** Code §63G-2-103(22); 1 **Vt.** Stat. §316(h); **Va**. Code §2.2-3701; **W. Va**. Code §§29B-1-2(5), 29B-1-3(3); **Wis**. Stat. §19.32(2).

[8] *See, e.g.*, **Ark**. Code §25-19-105(b)(11)(security information and passwords are exempt from disclosure); **Iowa** Code §22.1.7.40 (prevents disclosure of IP address of the person requesting a record); 65 **Pa**. Stat. §67.708(computer source data that can jeopardize computer security does not need to be disclosed).

[9] *See, e.g., Sierra Club v. Superior Court,* 125 Cal. Rptr. 3d 913, 916-917 (**Cal**. Ct. App. 2011)(computer software itself is not a public record and therefore access to it can require a license); **Colo.** Rev. Stat. §24-72-202(7)(software itself is not a public record); **Iowa** Code §§22.2; 22.7.33 (government need not give any access to data processing software it developed); **Nev.** AGO 89-1 (1989)(software itself is not a government record); *Matter of TJS of N.Y., Inc. v. New York State Dept. of Taxation*, 89 A.D.3d 239, 242 (**N.Y**. App. Div. 2011)("software that enables an agency to manipulate data is a record pursuant to FOIL in the same way that a written manual describing a series of procedures would be subject to disclosure."); **N.Y**. Comm. on Open Gov't FOIL-AO-12920 (August 30, 2001)(software developed with municipal funds is itself a record subject to disclosure so long as other exemptions do not apply); **N.Y**. Comm. on Open Gov't FOIL-AO-12366 (October 30, 2000)(software that is a mere delivery system is itself not subject to disclosure)("the application is essentially a tool that enables assessors and others to use data; it is not data itself and, therefore, in my opinion, it could not be characterized as a 'record'"); **N.C**. Gen. Stat. §§132-6.1(c), 132-6.1(d)(3),(4)(software and computer programs are defined to exclude, "the original data, or any analysis, compilation, or manipulated form of the original data produced by the use of the program or software."); **N.D**. Cent. Code, §44-04-18.4.2.c(7)(software

Whether or not electronic records are specifically addressed in state statues, courts and attorneys general are called upon to interpret what types of electronic data are covered under state records laws.[10] An interesting approach exists in Ohio, where the Court held:

> Computer tapes *qua* computer tapes are not public records. To the contrary, a public record is simply a record kept in the course of business of a public institution. Expression in a tangible medium, be it on paper, magnetic tape, or magnetic disk, does not transform that medium into a public record, nor is it necessary that the expression be in a particular medium for it to be a public record. 5 R.C. 149.43 requires the message, not the medium, to be disclosed. It is only when the method of expression enhances the message that we require agencies to disclose more than just a literal representation on paper.

State ex rel. Margolius v. City of Cleveland, 584 N.E.2d 665, 670 (Ohio 1991).

Courts will continue to interpret what types of electronic information are subject to disclosure. Most recognize that information cannot be shielded from

---

with independent economic value is considered a trade secret), **N.D**. Cent. Code, §44-04-18.5(computer program developed by government is exempt from public records law); 51 **Okla**. St. §24A.10.B.3(can keep computer software confidential but not the data it contains); **Ore**. RS §192.501(15)(computer program developed or purchased by government is exempt from public records law); **Utah** Code §63G-2-301(3)(l)(allows government to share the data in the program but not the computer program itself).

[10] *See, e.g., Commission on Peace Officer Standards & Training v. Superior Court of Sacramento County*, 165 P.3d 462, 467, n3 (**Cal**. 2007)(information in computer database covered under California public records law); *Lucarelli v. Freedom of Info. Comm'n*, 43 A.3d 237, 241 (**Conn**. App. Ct. 2012)(voice mails are subject to public records law but are not required to be kept or transcribed); *Fromer v. Freedom of Info. Comm'n*, 875 A.2d 590, 595-596 (**Conn**. App. Ct. 2005)(power point presentations were not records kept by public body but instead were personal records); **Haw.** Off. Info. Pract., Ltr. No. 90-35, 2, 5 (1990)(government records include electronic records); *American Federation of State, County & Municipal Employees (AFSCME) v. County of Cook*, 555 N.E.2d 361, 364 (**Ill**. 1990)(computer tapes are subject to public records law); *Wichita Eagle & Beacon Publ. Co. v. Simmons*, 50 P.3d 66, 79 (**Kan**. 2002); Ky. OAG 95-ORD-12; **La**. Atty. Gen. Op. No. 1990-330; *Prince George's County v. Wash. Post Co.*, 815 A.2d 859, 885-886 (**Md**. Ct. Sp. App. 2001)(database fields that were created by a consultant but used by the government were subject to public records law and not presumptively proprietary); 01/02 Op. Attn'y Gen. **Mass**. No. 1 (2001)(information in computer database was covered by public records law); *Payne v. Grand Rapids Police Chief*, 443 N.W.2d 481, 485 (**Mich**. Ct. App. 1989); *City of Warren v. City of Detroit*, 680 N.W.2d 57, 62 (**Mich**. Ct. App. 2004); *MacKenzie v. Wales Twp.*, 635 N.W.2d 335, 339 (**Mich**. Ct. App. 2001); *Flagg v. City of Detroit*, 252 F.R.D. 346, 356 (E.D. **Mich**. 2008)(text messages are subject to public records law); *Minnesota Medical Asso. v. State*, 274 N.W.2d 84, 88 (**Minn**. 1978)(information on computer tapes are subject to public records law); **Minn**. A.G. Op. 90-0032; **Minn**. A.G. Op. 05-0612; *Hemeyer v. KRCG-TV*, 6 S.W.3d 880, 882 (**Mo**. 1999)(videotape is subject to public records law); *Menge v. Manchester*, 311 A.2d 116, 118-119 (**N.H**. 1973); *State ex rel. Gambill v. Opperman*, 135 Ohio St. 3d 298, 302 (**Ohio** 2013); *Seago v. Horry County*, 663 S.E.2d 38, 43 (**S.C**. 2008); *O'Neill v. City of Shoreline*, 240 P.3d 1149, 1153 (**Wash**. 2010).

disclosure simply because it exists on a computer and has not yet been printed by a government employee. But that is just one (mostly settled) aspect of electronic records. Jurisdictions are now grappling with where the information itself ends and the software begins. This distinction matters in some jurisdictions, like Ohio, where disclosure is limited to information that is viewable in hard copy. Other jurisdictions treat software as government information that must be disclosed to the public, unless it is proprietary. An example is GIS (Geographic Information Systems) software that correlates the information it stores to a spatial reference point, for example, the location of parking meters, their hours of operation and fees charged. The government employee inputs a list of all of the parking meters and fees, but the software converts that information into a useful, interactive map. Is the map subject to disclosure, or just the underlying list? Courts can answer this question by using standard principles of statutory construction to determine what the word "software" means in the public records statute. *See, e.g.*, *Sierra Club v. Superior Court*, 302 P.3d 1026, 1029, 1031 (Cal. 2013). This will lead to a review of dictionary definitions, legislative history and public policy. *Id*. at 1032-39. However, it is important that courts and legislatures also consider what information is feasible for the government to extract from the electronic record and produce in response to a records request.

IV. When is a government "capable" of extracting electronic data?

The commentary to Rule 1.1: Competence in the ABA Model Rules of Professional Conduct has been changed recently to reflect that to "maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." *See* Comment 8, ABA Model Rule 1.1. Changing technology usually increases the type and amount of information that computer and Smart Phone users can extract from their electronic files. In the context of requests for electronic records, laws must strike a balance between what is theoretically possible to retrieve and what is cost effective for the government to be required to produce. The balance struck in many records laws was crafted by legislators when records were predominantly in hard copy, and production charges reflected the amount of paper and ink used and the time to search files. The few states that have addressed the format of production for electronic records are split about whether or not the requestor can demand to receive an electronic record in a particular format.

FOIA requires production of a record in any format requested "if the record is readily reproducible by the agency in that form or format." 5 USC §552(a)(3)(B). Some states take a similar approach, requiring records to be produced in the format requested when feasible.[11] Naturally, whether or not an

[11] *See, e.g.*, **Ark**. Code §25-19-105(d)(2)(B)(production "in any medium in which the record is readily available or in any format to which it is readily convertible with the custodian's existing software"); **Cal**. Gov. Code §6253.9(f)(do not have to produce "in the electronic form in which it is held by the agency if its release would jeopardize or compromise the security or integrity of the

agency can "readily" or "easily" produce an electronic record in a particular format is fact specific, leaving much for courts to interpret.[12] Although there is a body of case law discussing what types of electronic information is feasible for the government to produce, this amounts to little guidance for attorneys in states where the courts have not yet addressed this issue. However, the cases of other jurisdictions can be cited to bolster the argument that the process used by the client is reasonable.

Some states allow the government to decide whether or not to produce the electronic record in the requested format.[13] Other states mandate that if a record is kept electronically, then it must be produced in an electronic format, either in the one in which it is kept, or another format.[14] A subset requires production only in the electronic format in which the record is kept by the government.[15]

---

original record or of any proprietary software in which it is maintained"); 5 **Ill.** Comp. Stat. §140/6(a); **Mo**. Stat. §610.029(make electronic records available in useable format if possible); **N.Y.** CLS, Pub. Off., §§87.5(a), 89.3(a), **N.Y**. Comm. on Open Gov't FOIL-AO-12559 (March 6, 2001)("assuming that the conversion of format can be accomplished, that the data sought is available under FOIL, and that the data can be transferred from the format in which it is maintained to a format in which it is requested, an agency would be obliged to do so"); **N.C**. Gen. Stat. §132-6.2(a)("Persons requesting copies of public records may elect to obtain them in any and all media in which the public agency is capable of providing them."); **N.D**. Cent. Code, §44-04-18.4("Access to an electronically stored record under this section, or a copy thereof, must be provided at the requester's option in either a printed document or through any other available medium. A computer file is not an available medium if no means exist to separate or prevent the disclosure of any closed or confidential information contained in that file."); **Ore**. Rev. Stat. §192.440(3)(available in form requested if possible, and if not in form kept); **R.I**. Gen. Laws §38-2-3(g), (h), (k); **Tex**. Gov't Code §552.228; **Wyo**. Stat. §16-4-202(d)(ii), (iv).

[12] *See, e.g., Blaylock v. Staley*, 732 S.W.2d 152, 153 (**Ark**. 1987)(held magnetic tape to be a record but could not determine if it could be copied); **Haw.** Off. Info. Pract., Op. Ltr. No. 90-35, 3 (1990)(whether a record can be routinely complied under government's existing programming capabilities is a factual question, which can be determined, at least in part, by whether the agency itself compiles information in this manner); **Haw.** Off. Info. Pract., Op. Ltr. No. 90-22 (1990)(computer tapes can be given out in electronic form); **Haw.** Off. Info. Pract., Op. Ltr. No. 92-12, 7 (1992)(electronic mailing list must be provided on computer disk upon request, "unless doing so might significantly risk damage, loss or destruction of the original record."); *Matter of Hearst Corp. v. State*, 882 N.Y.S.2d 862, 867 (**N.Y**. Sup. Ct. 2009)(quoting the legislative history)("When an agency has the ability to retrieve or extract a record or data maintained in a computer storage system with reasonable effort, it shall be required to do so."); **N.Y**. Comm. on Open Gov't FOIL-AO-7595 (March 4, 1993)(not required to reprogram to get computer records); *Cummings & Associates, Inc. et. al. v. Oklahoma City, et. al.*, 849 P.2d 1087, 1090 (**Okla**. 1993)(do not need to develop special computer program to extract data); *Mechling v. Monroe*, 222 P.3d 808, 847, 850 (**Wash**. App. 2009)(provide in electronic format when feasible).

[13] *See, e.g.*, 29 **Del**. C. §10003(l); **Ind**. Code §5-14-3-2(m); **Iowa** Code §§22.2; 22.7.33 (access to a geographic computer database can be on terms acceptable to the government); *St. Tammany Parish Coroner v. Doe*, 48 So. 3d 1241, 1246 (**La**. Ct. App. 2010)(nothing in the law "specifically prohibits reproduction of public records by electronic format."); *Hawkins v. N.H. Dep't of Health & Human Serv.*, 788 A.2d 255, 258 (**N.H**. 2001)(not required to compile data into format requested); **N.M**. Stat. §§14-3-15.1, 14-3-18(E), 14-3-18(G)(electronic database information need only be printed in hard copy, but requestor can pay for an electronic copy or the agency may allow access to the database itself).

[14] *See, e.g.*, **Cal**. Gov. Code §6253.9(a); **D.C**. Code §2-532(a-1)(must produce in format requested "provided that the person shall pay the costs of reproducing the record in that form or format.");

Arkansas is a typical example of a hybrid approach: requiring production in the requested format where feasible but also permitting the government to agree to produce a record in any format. Ark. Code §25-19-109 (custodian can agree to summarize or provide electronic info "in a particular manner or medium and may agree to provide the data in an electronic format to which it is not readily convertible.").[16]

Some states make legislative pronouncements that encourage the production of electronic records in any electronic format or in a particular

---

Fla. Stat. §119.01(2)(f)("An agency must provide a copy of the record in the medium requested if the agency maintains the record in that medium"); **Ga**. Code §50-18-71(f)(produce in format requested "or in a standard export format such as a flat file electronic American Standard Code for Information Interchange (ASCII) format, if the agency's existing computer programs support such an export format"); **Haw.** Off. Info. Pract., Op. Ltr. No. 90-35, 3 (1990)("As long as the information is physically maintained in the format requested by a person, the agency must make copies of the government record in the format requested."); Op. Iowa AG 88-3-6(l), 1988 Iowa AG LEXIS 24, *6, 1988 WL 1583205 (**Iowa** A.G.)(government "should make available a copy of its master computer tape if that is the form in which the requestor wants to receive the information."); **Ky**. Rev. Stat. §61.874(2)(electronic records must be produced in standard electronic format, defined as ASCII format, unless "the public agency maintains electronic public records in a format other than ASCII, and this format conforms to the requestor's requirements, the public record may be provided in this alternate electronic format."); *Farrell v. City of Detroit*, 530 N.W.2d 105, 109 (**Mich**. Ct. App. 1995)(computer version of real property records required, not print out); **Minn**. §13.02, Subd. 3(e)(electronic data must be provided in electronic form if government can reasonably do so); **Miss**. Code §25-61-10(1)(must make an electronic copy in ASCII or other form, or the government can make the software itself available to view the data); **Utah** Code §63G-2-201(12)(electronic record must be produced in electronic form if requested so long as the electronic copy does not "disclose other records that are exempt from disclosure; or may be segregated to protect private, protected, or controlled information from disclosure without the undue expenditure of public resources or funds"); *WIREdata, Inc. v. Vill. of Sussex*, 751 N.W.2d 736, 759 (**Wis**. 2008)(government can provide a copy in any appropriate format, which can be PDF).

[15] *See, e.g.*, *Rhea v. Dist. Bd. of Trs. of Santa Fe College*, 109 So. 3d 851, 855 (**Fla**. Dist. Ct. App. 2013); Op. Att'y Gen. **Fla**. 1997-39(no requirement to provide in medium not used); 1 **Me**. Rev. Stat. §408-A.7 (provide electronic records as printed document or format in which it is kept, at requestor's option, so long as confidential information in electronic document can be shielded); R.R.S. **Neb**. §84-712(3); **Nev**. Rev. Stat. §239.010.4 (can get record in any medium in which it is readily available); **N.J**.S.A. §47:1A-5(d); **S.D**. Codified Laws §1-27-4(only need to provide electronic record in the format in which it is stored); 1 **Vt.** Stat. §316(h); **Va**. Code §2.2-3704.G; **W. Va**. Code §29B-1-3(3).

[16] *See also* **Conn**. Gen. Stat. §1-211(a)("requires production of electronic records "on paper, disk, tape or any other electronic storage device or medium requested by the person, including an electronic copy sent to the electronic mail address of the person making such request, if the agency can reasonably make any such copy or have any such copy made."); 29 **Del**. C. §10003(l); 1994 **Kan**. AG Op. No. 94-104; 1994 **Kan**. AG LEXIS 95, *2-*3 ("If the records are mandatorily open and already available in database format, the public agency must provide those records in such format upon request. The agency is not required to acquire or design a special program to produce information in a desired form, but has discretion to allow an individual who requests information to design or provide a computer program to obtain the information in the desired form.").

electronic format.[17] Additionally, some states require that records be kept in an easily reproducible electronic form, even going so far as to prevent governments from utilizing software that impedes the ability to produce an electronic record in an electronic form. For example, in Connecticut, a Court held that the government violated the law by purchasing a system that restricted public access to information and ordered the government to pay to have a computer reprogrammed, at a cost of $14,000, so that the requested information could be provided in electronic form. *Office of Health Care Access v. Freedom of Info. Commission*, 2005 Conn. Super. LEXIS 962, *4, *30 (Conn. Super. Ct. 2005)(unreported); *see also* 1 Me. Rev. Stat. §414 (when government purchases software it must consider maximizing access and protecting confidentiality).

Standing in stark contrast to this trend towards production of electronic records in electronic form, is Ohio, which allows copying of computer records if the requestor shows paper records are insufficient and pays the copying costs. *State ex rel. Margolius v. City of Cleveland*, 584 N.E.2d 665, 669 (Ohio 1991). "[I]t should be the rare instance in which a party making such a request would be able to demonstrate a need for the record stored on a magnetic medium in lieu of a paper copy." *Id*. at 669-670.[18]

Frequently, the cost of producing an electronic record is borne by the requesting party.[19] Some states even encourage or require that electronically

---

[17] *See, e.g.*, **Alaska** Stat. §40.25.115(a)("A public agency is encouraged to make information available in usable electronic formats to the greatest extent feasible."); **Md**. Code, State Gov., §10-620(a)(i)(electronic record must be produced in a "searchable and analyzable electronic format" if it exists in that manner and can be produced without revealing information subject to redaction); **Mo**. Stat. §§610.029, 109.190(although security of computer system cannot be compromised, a format that insures electronic copying is preferred but a photocopy can be provided).

[18] *Accord State ex rel. Recodat Co. v. Buchanan*, 546 N.E.2d 203, 205 (**Ohio** 1989)(no right to electronic documents in electronic form); *see also State ex. rel. Kerner v. State Teachers Retirement Board*, 695 N.E. 2d 256, 274 (**Ohio** 1998)(agency does not need to reprogram computer to extract electronic data).

[19] *See, e.g.*, **Ark**. Code §25-19-109(costs over two hours borne by requesting party); **Cal**. Gov. Code §6253.9(b)(if production of electronic record in electronic form requires computer programming, that cost can be passed on to requestor); *Hartford Courant Co. v. Freedom of Info. Comm'n*, 801 A.2d 759, 765-766 (**Conn**. 2002)(requestor bears cost of any reprogramming of computer system required to produce a record in electronic form); 29 **Del**. C. §10003(h); **D.C**. Code §2-532(f)(1)(personnel time to reprogram computers over eight hours is unreasonable); **Fla**. Stat. §119.01(2)(f)(agency may charge a fee for substantial manipulation or programming); **Haw.** Off. Info. Pract., Op. Ltr. No. 05-06, 6 (2005)(no obligation to purchase software to enable government to make the necessary redactions in a computer database to keep the appropriate data fields confidential, unless requestor is willing to pay for that software, in which case the custodian must make the redactions and provide the rest of record electronically); **Ind**. Code §§5-14-3-3.5, 3.6 (some records can be made available by third party vendors under contract with the government for a fee); *Johnson v. City of Pineville*, 9 So. 3d 313, 320 (**La**. Ct. App. 2009)(citizen entitled to electronic copies if he pays for electronic copying); 1 **Me**. Rev. Stat. §408-A.7.A; **Tex**. Gov't Code §§552.231, 552.272(can charge to program or manipulate data or deny request if doing so would interfere with government operations); **Utah** Code §63G-2-203(2)(iii); *accord Graham v. Davis County Solid Waste Mgmt. & Energy Recovery Special Service District*, 979 P.2d 363, 372 (**Utah** Ct. App. 1999)("An agency may, however, assess fees in conjunction with a

stored government information be available via an internet portal.[20] In contrast, Delaware's attorney general opined that a media request for access to a computer case-management database by giving the media the ability to log-in at their desktops, was unprecedented. 1994 Del. Attn'y Gen. Op., 94-I011. Interestingly, though, a request for information in Delaware can be filed on-line via a web portal. 29 Del. C. §10003.[21]

Alaska requires that electronic information "provided in printed form shall be made available without codes or symbols, unless accompanied by an explanation of the codes or symbols." Alaska Stat. §40.25.110(i). This furthers the general policy of government record disclosure laws to increase public understanding of government affairs.

Kentucky's legislature has declared that it will formulate the policy that governs the relationship between open records laws and "coordination of strategic planning for computerized information systems." Ky. Rev. Stat. §61.8715. However, the myriad of Kentucky attorney general's opinions on how to treat requests for information from electronic databases shows how difficult it can be to

---

record request that involves extracting materials from a larger document or source and compiling them in a different form."); *but see* **Ga**. Code §50-18-71(f)("An agency shall not refuse to produce such electronic records, data, or data fields on the grounds that exporting data or redaction of exempted information will require inputting range, search, filter, report parameters, or similar commands or instructions into an agency's computer system so long as such commands or instructions can be executed using existing computer programs that the agency uses in the ordinary course of business to access, support, or otherwise manage the records or data."); *Sage Info. Servs. v. Humm*, 977 N.E.2d 895, 900 (**Ill**. App. Ct. 2012)(charge for electronic reproduction can only be the cost of the electronic media on which it is placed, not a per-page fee).

[20] *See, e.g.*, **Ark**. Code. §25-19-105(f), (g)(software must allow electronic access and severability of non-exempt information); **Ind**. Code §5-14-3-2(e)("enhanced public access" allows access "by means of an electronic device other than an electronic device provided by a public agency in the office of the public agency" or by "compilation or creation of a list or report that does not result in the permanent electronic storage of the information"); **Ind**. Code §§5-14-3-8.3, 8.5 (funds established to maintain enhanced public access generally, and for electronic maps, specifically); **Ky**. Rev. Stat. §61.874(6)(government can make the record available via online access if the parties agree and this can be by contract, but must provide those same terms of access to all future requestors); *accord* **Ky**. OAG 05-ORD-25, p. 2-3; **Minn**. §13.02, Subd. 3(b)(electronic data stored electronically can be inspected by remote computer access); *Crutchfield v. N.M. Dep't of Taxation & Revenue*, 106 P.3d 1273, 1280 (**N.M**. Ct. App. 2004)(separate law concerning access to electronic government databases by commercial users); **N.C**. Gen. Stat. §132-10 (government must make access to GIS records available to public, but can condition copies on agreement that the copy will not be resold or used commercially, but media and real estate agents can use in their work); **Tenn**. OAG 01-021 (Feb., 8, 2001)(if record is accessible only by computer, then the government must provide means of accessing that record on-site).

[21] *See also Jersawitz v. Hicks*, 448 S.E.2d 352, 353 (**Ga**. 1994)(clerk of court was not required to create a new program to provide public access to real estate deed records by personal computers because access by disk was sufficient); 2009 **Kan**. AG Op. No. 2009-14, 2009 Kan. AG LEXIS 17, *7; *accord* 1995 **Kan**. AG Op. No. 95-64, 1995 Kan. AG LEXIS 71, *15 (allowing remote computer access through a third party doesn't relieve the government of its duty to make electronic records available in electronic form if possible); *but see* 65 **Pa**. Stat. §67.704(government can give electronic access to documents if it wants to do so).

craft a coherent policy.[22] Those opinions may create more confusion than help, especially where attorneys are addressing similar but not identical fact patterns. Attorneys may look to the trends developing in other jurisdictions before advising clients on an appropriate approach to extracting electronic information from a government computer, Smart Phone or other device.

V. Is metadata part of a public record? Should it be?

Metadata is "data about data." It is the information stored in an electronic document that is *not* visible on the screen. The term is used to describe the information created by a computer software program (application metadata, such as deleted text, format changes) and the computer itself (system metadata, such as date the file was saved, location of the file). It reveals additional facts about the electronic document that a requestor would not see if receiving a paper document or viewing the document on screen (*e.g.*, where the files are stored, who has access to them, when they were created, what edits were made and when). Public records laws rarely address this type of information that most people do not realize is being gathered and attached to the electronic document. For example, when a citizen asks for a paper copy of a permit, the names of government employees that have access to the filing cabinet containing the permits is not automatically disclosed. However, producing an electronic copy of a permit with its associated metadata will likely reveal which government employees are authorized to access the electronic permit file, along with a host of other information. This is information that most legislators never contemplated when drafting public records laws.

What types of metadata should be considered part of an electronic document and subject to disclosure is an emerging area of public records law. Attorneys often look to publications from The Sedona Conference to shed guiding light on legal issues created by electronic information. The Sedona Conference has produced a thorough description of metadata, highlighting the differences between application and system metadata. *See The Sedona Principles (Second Edition), June 2007: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, p. 3-4;[23] *see also Microsoft Office*

---

[22] *See, e.g.*, **Ky**. OAG 03-ORD-214, p. 9 (government may tailor its electronic database to the format requested and recoup costs, or it may produce in the standard format); **Ky**. OAG 03-ORD-04, p. 8-9 (although programming was not required to produce the select parts of database requested, the government should have then produced the whole database upon subsequent request even if this required redaction of some of the information); **Ky**. OAG 02-ORD-48, p. 5-6 (government not required to provide electronic information from database by culling it by hand when there is no software search function, or by allowing total database access when some of the information is protected); **Ky**. OAG 00-ORD-8, p.3 (government can allow person to see print out instead of inspect original record where it would divert on-site agency computers away from government duties to be used only for record inspection); **Ky**. OAG 99-ORD-68, p. 4 (government not required to create a separate program to put database information in a certain form).

[23] A project of The Sedona Conference Working Group on Electronic Document Retention & Production, Copyright 2007, The Sedona Conference, <http://www.sos.mt.gov/Records/

Online: Find and Remove Metadata (Hidden Information) in Your Legal Documents, (discussing the types of metadata created by Microsoft Office programs).[24] However, The Sedona Conference acknowledges that the metadata associated with electronic information is frequently altered (when a document is accessed or printed, for example) and recommends that an organization give careful thought to when it makes sense to retain such metadata, cautioning that courts can require it in discovery if it has been preserved, or require it to be preserved.[25]

Yet, neither the Sedona Conference nor the Microsoft publications make any definitive pronouncement on whether (and at what point) metadata is part of an electronic record. A requestor can ask the government for an electronic document, with its metadata, as of a certain date and time. However, it may be impossible for a government, without great expense, to reveal the metadata at all, let alone metadata that was coupled with the electronic document at an earlier time. Until this becomes easily technologically feasible, those governments that choose to include metadata as part of an electronic record will likely consider the relevant metadata to be the metadata associated with the record at the time it is accessed for production to the requestor.

Currently, most jurisdictions are completely silent in both statutes and case law on whether metadata is part of a public record, even though many of them address metadata in the context of civil discovery.[26] Only a few jurisdictions explicitly include some type of metadata in a record subject to production under public records laws. *See, e.g., Lake v. City of Phoenix*, 218 P.3d 1004, 1007-08 (Ariz. 2009)(includes application metadata, not system metadata, in the information that must be produced with an electronic record). Arizona's highest court has explained its reasoning for the inclusion:

> The pertinent issue is not whether metadata considered alone is a public record. Instead, the question is whether a "public record" maintained in an electronic format includes not only the information normally visible upon printing the document but also any embedded metadata . . . It would be illogical, and contrary to the policy of openness underlying the public records laws, to conclude that public entities can withhold information embedded in an electronic document, such as the date of creation, while

---

committees/erim_resources/A%20%20Sedona%20Principles% 20 Second%20Edition.pdf> (cited with permission).

[24] <http://office.microsoft.com/en-us/assistance/HA010776461033.aspx>

[25] *See The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (Second Edition)*, Comment 3f, p. 28-30, a project of The Sedona Conference Working Group on Electronic Document Retention & Production, Copyright 2007, The Sedona Conference, https://thesedonaconference.org/publication/Managing%20Information%20%2526%20Records (cited with permission).

[26] *See, e.g., Hawaii v. Hawaii Gov't Employees Assoc, et. al.*, 2013 Haw. App. LEXIS 135, * 28 (**Haw**. Ct. App. 2013); *Aequitas Solutions v. Anderson*, 2012 Del. Ch. LEXIS 250, *10, n.12 (**Del**. Ch. 2012).

> they would be required to produce the same information if it were written manually on a paper public record. . . . Our decision is unlikely to result in the "administrative nightmare" that the City envisions. A public entity is not required to spend "countless hours" identifying metadata; instead, it can satisfy a public records request merely by providing the requestor with a copy of the record in its native format.

Lake, 218 P.3d at 1007-08.

The approach outlined in this 2009 case demonstrates that judges did not consider confidential metadata that, if visible on the screen or in hard copy, would be exempt from disclosure. A subsequent Arizona case addressed this situation when it considered a request for the metadata attached to a legal memo from a city attorney. *Morgan v. Adams*, 2012 Ariz. App. Unpub. LEXIS 1089, (Ariz. Ct. App. 2012). The plaintiff "requested information concerning the date the memorandum was written, its title, delivery date, names of the intended recipients, delivery method, and any confirmation that it actually had been received and reviewed." *Id*. at *3. The lower court found the memo privileged attorney-client communication and held that the disclosure of the metadata would violate the privilege. *Id*. However, the appellate court mandated selective metadata redaction. *Id*. at *13-*14. The appellate court held that the privilege does not encompass "the date of the memorandum and the identity of its recipients," because these are "facts which are not part of the communication between lawyer and client." *Id*. at *13-*14 (citation omitted). Assuming that the metadata would show the information sought, the court required the production of the metadata itself, with the rest of the record redacted. *Id*. at *14. The court did not provide any advice on how to selectively show the metadata while redacting the entire contents of the electronic document that contained the privileged communication.

A Washington state court looked to these Arizona decisions for guidance when determining that a citizen was entitled to disclosure of metadata associated with an e-mail. *O'Neill v. City of Shoreline*, 240 P.3d 1149, 1151 (Wash. 2010). The original e-mail, which complained of zoning issues, was sent from one private citizen to a second. *Id*. That second citizen forwarded it to herself and blind copied several others including the Deputy Mayor and a member of City Council. *Id*. The Deputy Mayor mentioned receiving the e-mail at a subsequent meeting and a third citizen, the requestor, asked for a copy of that e-mail. *Id*. When she got home, the Deputy Mayor sent the e-mail she had gotten to her personal e-mail account but removed the "to" and "from" lines showing the e-mail had come from the second citizen and that the Deputy Mayor had been blind copied on it. *Id*. Then the Deputy Mayor forwarded this e-mail from her personal e-mail account to employees who printed it out and gave the hard copy to the requesting citizen. *Id*.

Seeing no senders or recipients, the requesting citizen sought the original chain of e-mails. *Id*. Thus, the Deputy Mayor found the original e-mail from the second citizen and sent it to the city's attorney. *Id*. The requesting citizen sought all the metadata associated with the e-mail chain. *Id*. The Deputy Mayor could not find the metadata associated with the original e-mail, assuming she had inadvertently deleted it (begging the question of how she searched for that information on her own) and so she asked the second citizen to forward her the e-mail again. *Id*. at 1152. Although this re-sent e-mail was provided to the requestor along with the identical metadata contained in the same e-mail that had gone to the Councilmember, the requesting citizen continued to seek the original metadata. *Id*.

A trial court ruled in favor of the government, but the requestor appealed and Washington's appellate court held that the metadata contained in the e-mail that went to the Deputy Mayor was a public record subject to disclosure and remanded the case for a factual finding of whether the Deputy Mayor's computer contained the metadata that she could not locate herself. *Id*. Washington's highest Court granted review and held that it agreed "with the Supreme Court of Arizona that an electronic version of a record, including its embedded metadata, is a public record subject to disclosure." *Id*. at 1154. "Metadata may contain information that relates to the conduct of government and is important for the public to know." *Id*. at 1154-55. The Supreme Court observed that the City had "the opportunity to inspect [the Deputy Mayor's] home computer's hard drive for the requested metadata. While the City has searched [the Deputy Mayor's] e-mail folder for the deleted e-mail and its associated metadata, the City has not inspected the hard drive of [the Deputy Mayor's] home computer." *Id*. at 1155. The Court held that the hard drive of the Deputy Mayor's home computer should be inspected because otherwise City employees could thwart records laws by using home computers. *Id*.

In *Matter of Irwin v Onondaga County Resource Recovery Agency*, 72 A.D.3d 314, 316 (N.Y. App. Div. 2010), New York's Appellate Court considered whether metadata associated with electronic photographs of the plaintiff emptying leaves at a county compost site, which had been sent to subscribers of a government e-newsletter, needed to be disclosed under the state's public information law. The Court noted that a request for all computer records associated with the images he sought included a request for the metadata. *Id*. at 319. The court then gave a sweeping definition of metadata and defined three recognized types: application, system and embedded. *Id*. at 320-321. The Court explained that generally there are two ways to produce metadata: with the document itself by producing it in native form, or in a TIFF file with the metadata contained in a separate file. *Id*. at 321 -322. Producing records in paper form or as a picture (PDF) contains no metadata. *Id*. at *321-322. The court noted that at issue was the "system metadata" (i.e. "file names and extensions, sizes, creation dates and latest modification dates") of the photographs and the Court held that those were public records subject to disclosure. *Id*. at 314, 319. The Court

constrained its holding to the facts at bar, stating specifically that it was not addressing whether other types of metadata were subject to disclosure. *Id*. at 322.

New York's commission on Open Government, which issues opinions on record request matters, has held that software that is a mere delivery system is itself not subject to disclosure. Comm. on Open Gov't FOIL-AO-12366 (October, 2000)("the application is essentially a tool that enables assessors and others to use data; it is not data itself and, therefore, in my opinion, it could not be characterized as a 'record'"). Reading this 2000 Open Government Commission opinion with *Irwin* leads to the conclusion that both the data on the computer screen and the metadata buried in the program must be disclosed unless another exemption applies. However, the programming code that makes the information accessible is not subject to disclosure. Although this is detailed guidance for attorneys representing governments in New York, it requires those governments to separate the electronic information into its component parts.

Although New York, Washington and Arizona clearly include some types of metadata in any request for an electronic record, other jurisdictions require that the metadata be specifically requested for it to be included: meaning that a request for electronic information does not automatically include the associated metadata.[27] Another handful of jurisdictions explicitly excludes metadata from the definition of a record or exempts it entirely from disclosure. The Colorado records statute says that a copy, photograph or print-out is a sufficient way to produce an electronic record. Colo. Rev. Stat. §24-72-205. This effectively removes any obligation to produce the metadata associated with that electronic record. *See Tax Data Corp. v. Hutt*, 826 P.2d 353, 357 (Colo. Ct. App. 1991)(providing "the information in a manner identical to viewing the same information on a computer screen" is sufficient.). Maryland allows, but does not require, the government to fully redact ("scrub") all metadata. Md. Code, State Gov., §10-620(a)(2)(iii).

The aforementioned jurisdictions are clear on how to treat metadata in public record requests. Other jurisdictions, including the federal government, are just beginning to address metadata contained in electronic records.[28] In a 2001

---

[27] *See, e.g., Citizens for Responsibility and Ethics in Government v. Department of Education*, 905 F.Supp. 2d 161, 171, 172 (D.**D.C**. 2012)(court declined to impose a rule that metadata must be produced to satisfy a FOIA request); *State ex rel. McCaffery v. Mahoning county Prosecutor's Office*, 976 N.E.2d. 877, 884 (**Ohio** 2012)(not entitled to metadata in requests for public information unless specifically requested); *Maese v. Davis County*, 273 P.3d 949, 950 -51 (**Utah** Ct. App. 2012)(court did not need to reach question of whether metadata was required to be disclosed because it was not specifically sought in original request).

[28] *See, e.g.*, 5 **Ill**. Comp. Stat. §140/1 (Illinois "General Assembly further recognizes that technology may advance at a rate that outpaces its ability to address those advances legislatively," and therefore its public records laws should be interpreted to favor disclosure unless withholding furthers the public policy articulated in a particular exemption.); **Minn**. Stat. §13.15(requires the government to tell people about how certain metadata "created, collected, or maintained about a person's access to a government entity's computer" will be disseminated); **N.H**. Rev. Stat. §91-A:4.V(confidential metadata can be removed and the record placed in "common file format" so

FOIA case, the federal court hinted that key information may be contained in the metadata of government records and that such information should not be withheld if it exists:

> At various points in the commentary, dates have been produced in unredacted form. Other pages have no dates. Defendants do not have the obligation to create new information in response to FOIA requests. However, it seems unlikely that so many of these daily reports were created without identifying dates. For example, the reports' metadata may have contained the date on which they were created; or perhaps they were archived according by date [sic]. Defendants may not withhold this information if it exists.

Families for Freedom v. United States Customs & Border Prot., et. al., 837 F. Supp. 2d 287, 303-04 (S.D.N.Y. 2001). That court did not resolve, however, whether the government was required to identify what metadata is actually embedded in the document, and how extensive any search for metadata must be.

In the more recent case, *Judicial Watch, Inc. v. USAF*, 2012 U.S. Dist. LEXIS 49717 (D.D.C. 2012), the Air Force argued that the metadata associated with an electronic version of a letter was that information attached to its PDF version (that was e-mailed to the plaintiff) and not its original Word version. *Id*. at *3-*4. The Court held that the request for metadata included both the metadata associated with the PDF and the Word document. *Id*. at *5. The Court then allowed the parties to brief the question of whether the metadata is public record. *Id*. at *6. Twenty days after the ruling, the case settled. *Id.*, <www.pacer.gov>, 11-cv-00932 (D.D.C.), doc. #21.

In a Montana case, *State v. Saksa*, 2012 MT 210N (Mont. 2012)(unreported), a criminal defendant argued that metadata associated with a CD had been altered. In a concurring opinion, a Supreme Court of Montana justice suggested that law enforcement enact procedures to protect metadata in government documents. *Id*. at *P13. He noted that metadata was discoverable in federal court, likely would be held to be discoverable in state court, and that he foresaw that, "the rule will eventually be that the preservation of digital evidence includes the preservation of the associated metadata." *Id*.

Yet, since so many jurisdictions are silent on whether metadata must be produced as part of a public record, attorneys can be left guessing as to whether a court would require the production of their government client's metadata. One way to make an educated guess about how a particular jurisdiction may treat metadata associated with an electronic government record is to review the jurisdiction's treatment of severability of exempt and non-exempt information in

---

that confidential information is not revealed, creating the inference that non-confidential metadata is likely part of the record).

the electronic context.[29] For example, Arkansas requires that software allow severability of electronically stored information that is exempt from production from the non-exempt portions. Ark. §25-19-105(f), (g). An Arkansas court or its attorney general may therefore conclude that metadata created by a computer program be disclosed if it does not otherwise fall under an exemption. This is because there is an existing expectation that electronic data is treated just as paper records are treated, requiring segregation of information that is allowed to be viewed from the information exempt from disclosure. If governments are already required to segregate electronic information that is visible on the screen into exempt and non-exempt information, courts may find it reasonable that the same be done for information that cannot be seen.

The problem with this approach, however, is that while it may be feasible to separate the electronic information that is visible on the screen and produce only that which is required to be disclosed, it may not be easy to do that with the metadata. For example, if a government keeps a document in a spreadsheet, the computer user can simply hide or delete columns in the electronic document, and then save it as a separate file. The recipient would receive an electronic copy of that separate file containing only the information that is required to be disclosed. But while most computer users can cut, paste and save, it would be rare to find the computer user that knows how to delete the document's metadata. Although some users may know how to delete metadata in its entirety, selective metadata redaction usually requires separate software for each computer program.

The difficulty posed by selective redaction of metadata has been highlighted in a recent Connecticut case, *Pictometry Int'l Corp. v. Freedom of Info. Comm'n*, 59 A.3d 172, 176 (Conn. 2013). Although an earlier Connecticut case held that GIS data in electronic form had to be produced with the associated metadata showing "when the data was input, what source was used, who input the date, the accuracy of the data, and how often the data is updated," it did not need to address selectively redacting any of that metadata because it held it was all subject to disclosure. *Dir., Dep't of Info. Tech. v. Freedom of Info. Comm'n*, 874 A.2d 785, 788, n.2 (Conn. 2005). However, in 2013, Connecticut's highest court

[29] *See, e.g.*, **Fla**. Stat. §119.011(13)("'Redact' means to conceal from a copy of an original public record, or to conceal from an electronic image. . ."); Code of **Haw.** Rules §2-71-31(b)(2)(B)(allows agencies to charge for segregating information that needs to be redacted from an electronic record); **Ind**. Code §5-14-3-6(requires separation in electronic records of information that can be disclosed from that which cannot, but can charge the requestor the cost of requisite programming); 2009 **Kan**. AG Op. No. 2009-14, 2009 Kan. AG LEXIS 17, *9 (government providing electronic records to a third party must remove information that cannot be disclosed prior to removal); **Ky**. OAG 95-ORD-43(required to redact exempt information from computer records); **N.D**. Cent. Code, §44-04-18.4; **Ohio** Op. Attn'y Gen. 2004-045 at 20 (required to redact confidential information in electronic record as it would in any other record); **Tenn**. Code §10-7-503(a)(5)(contemplates redaction from electronic record); **Tex**. Gov't Code §552.272(d)(contemplates that data may have to be manipulated to separate out confidential information); **Utah** Code §63G-2-204(5)(h)(if segregating information requestor is entitled to inspect from that which is not subject to inspection requires computer programming, then response can be delayed).

considered the disclosure of electronic photographs and their associated metadata, which included "the time that the image was captured, the angle at which it was captured and the latitude, longitude and altitude of the camera. The metadata is entered into Pictometry's proprietary software, which is protected by federal copyright and state trade secret laws." *Pictometry*, 59 A.3d at 176. The request "encompassed the metadata embedded in the computerized images. It also became clear that [the requestor] believed that the images stripped of the associated metadata would be useless to him." *Id*. at 181. The court held that the government can be ordered to redact exempt information and produce nonexempt computer records in another electronic form. *Id*. But the Connecticut Court also held that if the government could not produce the images stripped of the metadata, it was an abuse of discretion to order them to do so. *Id.* at 182.

The difficulty with selectively extracting metadata led the Maryland General Assembly to decide that its statute would allow wholesale removal of metadata at the government's option. *See* Md. Code, State Gov., §10-620(a)(2)(iii). During legislative debate, some argued that the public should be able to receive all information that the government possesses, including the file pathways and deleted text contained in the electronic version of a document. However, metadata can contain evidence that an e-mail was sent to a certain person (blind copy) or that a document was edited in a certain way (application metadata) or accessed by someone at a specific time (system metadata). If the person blind copied, editing or accessing the document was a government attorney, for example, the metadata itself could be evidence of attorney-client communication, or attorney work product. The government should be entitled to redact that information where appropriate, just as it would in paper documents. Yet, it is technologically difficult to make these redactions without specialized software. The legislature recognized this difficulty and amended the legislation to allow government to remove the metadata entirely, instead of selectively redact metadata or requiring its wholesale production. *See* Md. Code, State Gov., §10-620(a)(2). This approach acknowledges the current technological capabilities and avoids the expense government would have to incur (purchasing software and devoting employee time) to selectively redact metadata that should not be produced to the requestor.

It appears that California, too, has recognized the difficulty in selective redaction of metadata. It distinguishes between the software itself (not subject to disclosure) and data the software contains (subject to disclosure), hinting that California would be inclined to protect from disclosure any information produced by the software, *i.e*. the metadata. 88 Ops. Cal. Atty. Gen. 153, 159 (2005). California's Supreme Court recently ruled that "although GIS mapping software falls within the ambit of this statutory exclusion, a GIS-formatted database like the OC Landbase does not. Accordingly, such databases are public records that, unless otherwise exempt, must be produced upon request at the actual cost of duplication." *Sierra Club v. Superior Court*, 302 P.3d 1026, 1029 (Cal. 2013). This ruling reinforces the separation between the information contained in the

software, which is subject to disclosure, and underlying software programming that formats the data. Courts that analyze issues presented by electronic documents by separating those documents into their components (data versus software) could use the same analysis to separate the electronic information into its components (visible versus metadata). Reviewing a jurisdiction's case law or statutory treatment of the information created by a software program could be another way to make an educated guess about how a jurisdiction that has no policy on metadata may handle a request seeking it.[30]

Until more courts and attorneys general examine requests for the metadata associated with electronic records, there will be little guidance. Analogies to how a jurisdiction treats information created by a software program or whether it requires severability of exempt and non-exempt information in the electronic context are the best tools for guiding government clients while this body of law develops.

VI. Conclusion

Jurisdictions are determining which electronic records are able to be disclosed and which are simply too costly or time consuming to make available. E-mails are the most common electronic records. While many jurisdictions do not mention them by name, they are generally captured under a broad definition of public records and required to be disclosed if their contents concern government business. There is no consensus on whether e-mails on private devices are subject to disclosure when they concern government business.

---

[30] *See e.g.*, **Colo.** Rev. Stat. §24-72-202(7)(software itself is not a public record); **Idaho** Code, §9-340D(15)(exempts proprietary computer programs from disclosure but defines those programs as "instructions or statements which permit the functioning of a computer system," and not the original data, any manipulated forms of that data or any formulas "that would be used if the manipulated forms of the original data were to be produced manually," making the latter available under public records laws); **Ky**. Rev. Stat. §§61.870(3), 61.878(software, including security features and proprietary aspects, are separate from the data it contains); **Mich**. Comp. Laws §15.232(f)(software is defined to include the code that makes it function and any proprietary information, but to exclude and make available for disclosure the information the software contains); **Mo**. Stat. §§610.021, (10), (20)(records identifying how a computer operates or its electronic codes are not open to inspection); 1996 **Neb**. Op. Att'y Gen. No. 74(except computer source codes, all computer programming and instructions are part of the public record); **Nev**. AGO 89-1 (2-6-1989)("a computer program is not a record at all."); *State ex rel. Gambill v. Opperman*, 135 Ohio St. 3d 298, 304-06 (**Ohio** 2013)(if cannot extract the electronic data and pull it away from proprietary software, then it need not be disclosed, or it can be disclosed for the cost of an outside consultant to extract it); **Ore**. Rev. Stat. §192.501(15)(software program is different than the "[a]nalyses, compilations and other manipulated forms of the original data produced by use of the program; or the mathematical and statistical formulas which would be used if the manipulated forms of the original data were to be produced manually."); **Utah** Code §63G-2-103(4)(computer program is defined to exclude "any associated documentation and source material that explain how to operate the computer program" but include mathematical or statistical formulas); **Wis**. Stat. §19.36(4)("material used as input for a computer program and material produced as a product are subject to inspection and copying, but the a computer program is not."); *accord* 75 Op. Attn'y Gen. **Wis**. 133, 1986 Wis. AG LEXIS 22, *10.

No consensus exists on what other types of electronic information should be subject to disclosure. Statutes generally favor disclosure, and commonly exclude information that may compromise the security of the computer system. There is a wide range of cases and attorney general opinions on what specific types of electronic information, from databases to text messages, are subject to public records laws. These provide sources of support for attorneys addressing novel information requests.

The trend is towards treating information stored electronically just like any other public record. But no trend has emerged in the treatment of the software that contains that information, even though many jurisdictions have addressed that question in some form. In some jurisdictions the software programs are mere delivery systems, not captured within the spirit of what was intended to be disclosed under public record laws. In other jurisdictions, software coding information is viewed as any other information and production is required, especially where the government has created the software.

These two divergent views also manifest themselves in nascent law on metadata associated with electronic records. Some jurisdictions treat the metadata just as it would any other information and require its production. Others see a stark contrast between the information that can be viewed on the screen and that which is hidden behind it. Determining what is information subject to disclosure will continue to evolve with changes in technology.

Jurisdictions will continue to evaluate what information can be extracted from electronic records. What can be copied and at what expense? What must be redacted? Should a request be deemed to include all the information visible on the screen or is metadata presumed to be included? If metadata is included, how is it copied and given to the requestor? While selectively redacting some electronic information (e.g., deleting certain columns on a spreadsheet) may be familiar to computer users, redacting the metadata is far harder. Courts and state attorneys general have not adequately addressed the additional time and special software needed to selectively redact metadata.

Attorneys advising clients on what electronic information is included and how to extract it can find similar fact patterns in other jurisdictions. Certainly many state courts find the federal government's approach persuasive. Yet, the federal government has not addressed all aspects of electronic production or metadata. Although it may be tempting to formulate a global answer to the many questions posed by producing electronic government information to the public, such an approach naively ignores all the many varied computer programs and software. A uniform approach would also require a global balance of a desire for transparency with the resources available to the government. Not every jurisdiction will have the same employees or resources to dedicate to extracting electronic information at the request of the public. Moreover, not every

jurisdiction will employ the same software programs or store the same types of information.

As Justice Ginsburg wrote in her concurring opinion in *Los Angeles Police Department v. United Reporting Publishing Corp.*, 528 U.S. 32, 43-44 (1999)(Ginsburg, J., concurring), requiring an all-or-nothing approach to records disclosure could lead to less government transparency, not more. In that case, the Supreme Court rejected a challenge to a California statute that restricted the disclosure of arrestee information to limited-purpose requestors. *Id*. Justice Ginsburg aptly noted:

> [I]f States were required to choose between keeping proprietary information to themselves and making it available without limits, States might well choose the former option. In that event, disallowing selective disclosure would lead not to more speech overall but to more secrecy and less speech. As noted above, this consideration could not justify limited disclosures that discriminated on the basis of viewpoint or some other proscribed criterion. But it does suggest that society's interest in the free flow of information might argue for upholding laws like the one at issue in this case rather than imposing an all-or-nothing regime under which "nothing" could be a State's easiest response.

This reasoning is equally compelling in the context of the disclosure of electronic documents and their metadata. Governments need to determine what it is feasible to disclose, considering time, advances in technology and the cost of redaction software. Flexibility will allow governments to provide transparency in the face of changing technology.