STEVENS & DAY LLP

ATTORNEYS AT LAW

29TH ANNUAL REFERRING ATTORNEY SEMINAR

SEGMENT 3: E-Filing in the State Courts

Laura Pioch

NOVEMBER 6, 2020

82 WINTHROP STREET, AUGUSTA, ME 04330

Session 3
Legal Potpourri: Remote Notarizations; E-Recording in the Registry; E-Filing in the State Courts; The Paperless Office; and Interesting Cases Resolved in the Past Year

Written Materials

- Maine Rules of Electronic Court Systems

- Board of Overseers of the Bar - Opinion #196: Transmission, Retrieval and Use of Metadata Embedded in Documents

STATE OF MAINE
SUPREME JUDICIAL COURT
ADOPTION OF
MAINE RULES OF ELECTRONIC COURT SYSTEMS

2020 Me. Rules 03

Effective: August 21, 2020

All of the Justices concurring therein, the following Maine Rules of Electronic Court Systems are adopted to be effective on the date indicated above. To aid in the understanding of the Rules, Advisory Notes appear after the text of certain Rules. Each Advisory Note provides pertinent information regarding the Rule, but the Advisory Note is not part of the Rule adopted by the Court.

1. The Maine Rules of Electronic Court Systems are adopted to read as follows:

PREAMBLE

These Rules of Electronic Court Systems are intended to facilitate public access to and use of the courts in the electronic environment, while providing maximum reasonable public access to court records and minimizing the risk of harm to individuals and entities involved in court proceedings. In developing these rules, the Maine Judicial Branch has carefully considered and weighed the importance of both public access and protection of privacy in court records in the context of an electronic case management and filing system.

RULE 1. SCOPE AND PRINCIPLES

(A) Scope. These rules define the scope of access to court records electronically stored by the Maine Judicial Branch and govern electronic filing and service of documents. They shall be construed to secure simplicity and fairness in administration and the elimination of unjustifiable expense and delay.

(1) These rules apply to:

(a) Parties, persons, and entities filing or requesting access to electronic court records; and

(b) All court staff and other persons conducting business on behalf of the court, including justices, judges, and magistrates, responding to requests for electronic court records.

(2) These rules do not apply to county probate courts or paper records and paper filings in existence on or made before the date these rules are implemented in the courthouse where the record is located.

(B) Principles. Public access to court records is restricted in certain instances by law. When public access to court records is not controlled by law, these rules will control public access, and every judge, justice, and magistrate applying these rules shall consider the principles listed below in doing so:

(1) Public access to records can inform and educate the public about the workings of government, support accountability, and advance public safety;

(2) Persons who use the courts have a legitimate expectation of privacy. Providing access to personal details in court records can put the parties at risk and create a disincentive to use the courts;

(3) The public can be informed of court activity without having access to all of the personal details in a court record; and

(4) When digital information or data are made accessible by the public remotely, neither the Maine Judicial Branch nor any other entity or person has the practical ability to control its dissemination or use.

RULE 2. DEFINITIONS

(A) As used in these rules, unless the context otherwise indicates, the following terms have the following meanings:

(1) "Accept" or "Acceptance" in the context of electronic filing indicates approval by the court clerk of an electronic document submitted to the electronic filing system. When a court clerk approves and accepts a document submitted for electronic filing, that electronic filing becomes part of the electronic case file.

(2) "Accessible by the public" means that a court record is open to inspection by any member of the public and may be reproduced as permitted by these rules. Under these rules, some court records may be accessible by the public only at a courthouse, and other court records may be accessible by the public both remotely and at a courthouse.

"Accessible by the public" does not mean that the court will search for records when the requester does not have information sufficient to identify the specific court records sought.

(3) "Accessible by the public only at a courthouse" means that a court record may be inspected by any member of the public only at a public access computer. Juvenile case records that are accessible by the public only at a courthouse cannot be copied electronically nor may hard copies be provided by the court clerk. All other court records that are accessible by the public only at a courthouse cannot be copied electronically, but hard copies may be provided by the court clerk. A fee may be charged for copies.

(4) "Accessible by the public remotely" means that a court record may be inspected or reproduced by any member of the public through an internet-based case management system accessible through a standard browser. Court records that are accessible by the public remotely are also accessible by the public at a courthouse.

(5) "Aggregate data" means summary information extracted, assembled, or derived from compiled data. "Aggregate data" eliminates any case- or party-identifying information such as docket numbers, names, personally identifying information, and addresses.

(6) "Bulk data" means an electronic collection of data composed of information from multiple records, whose primary relationship to each other is their shared origin from single or multiple databases. "Bulk data" is different from multiple records.

(7) "By law" means by federal or state law or regulation, court rule, including these rules, or administrative order.

(8) "Case management system" or "CMS" means an electronic document repository maintained, administered, and managed by the Maine Judicial Branch to track information and manage cases.

(9) "Child protection matter" means any child protection matter filed under Title 22 of the Maine Revised Statutes.

(10) "Civil case" means any case that is not a criminal case subject to Rule 5, a juvenile case subject to Rule 6, or a family matter, child protection matter, or protection order case subject to Rule 7.

(11) "Clerical error" means information in the court record that is obviously incorrect and that occurred as a result of a mistake made by court staff.

(12) "Compiled data" means information that is derived from the selection, collection, or reformulation of all or some of the information from the records of more than one case or judicial proceeding.

(13) "Conventional filing" and its variants mean a process in which a filer submits a paper document that is then converted to electronic format by a court clerk and filed.

(14) "Conventional service" and its variants mean service accomplished by nonelectronic means such as by mail or in person in accordance with the applicable rules of civil, criminal, or appellate procedure.

(15) "Court" means the Supreme Judicial Court, the Superior Court, the District Court, and all justices, judges, and magistrates of those courts.

(16) "Court clerk" means a manager of court operations, clerk of court, deputy clerk, assistant clerk, associate clerk, administrative clerk, or staff of a clerk's office.

(17) "Court record"

(a) "Court record" means any file, document, information, or data received or maintained by a court in electronic form in connection with a specific case or proceeding, including:

(i) Pleadings, motions, briefs and their respective attachments, correspondence, and documentary evidentiary exhibits submitted with court filings;

(ii) Orders, judgments, opinions, and decrees;

(iii) Registries of actions, calendars, docket sheets, and other information created or prepared by court clerks that is related to a case or proceeding; and

(iv) Juvenile case records as defined in the Maine Juvenile Code.

(b) "Court record" does not include the following materials, even if they exist in connection with a specific case or proceeding:

(i) Information gathered, maintained, or stored by a governmental agency or other entity to which any employee of the Maine Judicial Branch has access but that is not part of a court record or file or is part of the court record but is prohibited from release by law;

(ii) Notes, memoranda, and drafts thereof, and any other material prepared or collected by a justice, judge, or magistrate or other court staff at the direction of a judicial officer and used for a judicial settlement conference, in recording the judicial officer's notes of a proceeding, or in researching or preparing orders, judgments, opinions, or decrees;

(iii) Internal draft working documents, reports, or data analysis prepared for or by a justice, judge, magistrate, other court staff, bail commissioner, or justice of the peace

related to court practices, schedules, work assignments, and procedures;

(iv) Legal work product, including drafts, and other records or reports of any attorney, law clerk, or other person employed by or representing the Maine Judicial Branch that are produced in the regular course of business or during representation of the Maine Judicial Branch;

(v) Records of consultative, advisory, or deliberative discussions pertaining to the rendering of decisions or the management of cases;

(vi) Discovery materials served through the EFS;

(vii) Exhibits submitted at or filed in preparation for trial or hearing;

(viii) Juror information; and

(ix) Any other documents or information not expressly defined as court records, including administrative records or reports maintained by the Maine Judicial Branch.

(18) "Courthouse" means any facility in which a State of Maine District Court or Superior Court is housed. "Courthouse" does not include county probate courts.

(19) "Electronic case file" means the dataset that includes any document, information, data, or other item created, collected, received, or maintained by the Maine Judicial Branch in connection with a specific case that is readable through the use of an electronic device. The electronic case file does not include anything that is not a court record as defined in these rules.

(20) "Electronic document" means the electronic form of pleadings, notices, motions, warrants, orders, exhibits, briefs, judgments, writs of execution, and other records accepted by a court clerk for filing. Electronic documents include documents filed in digitized format or converted to digitized format by a court clerk.

(21) "Electronic filing" means the electronic transmission of a document in electronic form to the court through the electronic filing system. An electronic filing under these rules does not include the submission or transmission of documents to a court through other electronic means such as email, facsimile, or external USB drives.

(22) "Electronic filing system" or "EFS" means the system approved by the Maine Judicial Branch for the filing and service of electronic documents.

(23) "Electronic service" means the electronic transmission of a document or information to a party or a party's attorney. Under these rules, electronic service does not include service of process or a summons or warrant to gain jurisdiction over persons or property.

(24) "Electronic notification message" means an automatic electronic message generated by the CMS and sent to all attorneys or parties in a specific case to denote the receipt of a filing.

(25) "Family matters" means cases or proceedings, including post-judgment proceedings, for the following:

(a) Divorce;

(b) Annulment or judicial separation;

(c) Parental rights and responsibilities, including the establishment or enforcement of a child support obligation;

(d) Paternity or any type of parentage, including actions to enforce or obtain remedies for noncompliance with a gestational carrier agreement;

(e) Grandparent or great-grandparent visitation; and

(f) Adoption, guardianship, name change, or emancipation of a minor.

(26) "Inspection" means only visual inspection of court records without photocopying, photographing, or otherwise reproducing those records.

(27) "Juror information" means the following for all jurors and prospective jurors:

(a) Names;

(b) Telephone numbers, addresses, including email or other electronic addresses, and other contact information;

(c) Social Security numbers;

(d) Dates of birth;

(e) Source lists;

(f) Seating charts;

(g) Qualification questionnaires;

(h) Information obtained by special screening questionnaires or in *voir dire* proceedings that personally identifies jurors; and

(i) All other personally identifying information of a juror or information from which a juror's identity could be learned.

(28) "Nonpublic" means access is restricted or prohibited by law.

(29) "Personally identifying information" means information that can be used to distinguish, detect, discover, or trace an individual, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

(30) "Protection order case" means any protection from abuse case or any protection from harassment case.

(31) "Public"

(a) "Public" means the following:

(i) Any person, business, media organization, or entity; and

(ii) A government agency or commission for which there is no existing federal or state law, court rule, or court order defining that agency's access to court records.

(b) "Public" does not mean the following:

(i) Court staff, employees, justices, judges, and magistrates;

(ii) The parties to a specific case or proceeding, their attorneys and their attorneys' authorized agents, and persons identified by the court as having access to the court record in that case or proceeding;

(iii) Private or governmental persons, vendors, or entities that assist the Maine Judicial Branch in performing its functions and are subject to court restrictions on the use and dissemination of information from court records, including bail commissioners, justices of the peace, interpreters, and mediators;

(iv) Persons or governmental entities whose access to court records is governed by law, or by a policy set by the State Court Administrator;

(v) Persons who are authorized by law to access court records;

(vi) An alleged victim in a criminal or juvenile proceeding;

(vii) The parent, guardian, or legal custodian of an alleged victim in a criminal or juvenile proceeding when the alleged victim is a minor;

(viii) An immediate family member, parent, guardian, legal custodian, or a licensed investigator acting on behalf of an alleged victim in a criminal or juvenile proceeding when the alleged victim cannot act on his or her own behalf due to death, age, physical or mental disease, or disability; and

(ix) An attorney representing the alleged victim in a criminal or juvenile proceeding.

(32) "Public access computer" means a facility within a courthouse to access the Maine Judicial Branch's closed-loop system.

(33) "Registry of actions," formerly identified as "docket entries," means the list of case information maintained by the court clerk that contains the case caption; docket number; a chronological entry identifying the date and title of each complaint, motion, order, judgment, notice, action, or other document filed in a case; and the dates of events in the case.

(34) "Registered user" means an individual or entity with an assigned username and password authorized by the Maine Judicial Branch to access and utilize the EFS.

(35) "Seal or impound" means to restrict public access to a court record by court order. When a juvenile case record is sealed pursuant to Rule 6(G)(1), the juvenile may respond to inquiries other than from a court or criminal justice agency about the sealed juvenile case records as if the juvenile crimes had never occurred, without being subject to any sanctions.

(36) "Self-represented litigant" means a person or entity, other than an attorney, who is not represented by an attorney in a court proceeding.

(37) "User agreement" means an agreement that establishes the obligations and responsibilities of the registered user for use of the EFS.

PART ONE: RULES OF ELECTRONIC COURT RECORDS ACCESS

RULE 3. GENERAL ACCESS POLICY

(A) Electronic court records are accessible by the public except as provided by law, including these rules, or by court order.

(B) Parties and their attorneys may access all court records in their cases remotely and at the courthouse except as provided by law or court order. Alleged victims in any criminal or juvenile cases may access court records as provided by law only at a courthouse.

(C) Any file, document, information, or data received or maintained by the court before the implementation of electronic filing that become court records through scanning or other digitization are accessible as follows:

(1) Accessible remotely or at the courthouse by the parties and their attorneys; and

(2) Accessible by the public as allowed by these rules only after the court records have been redacted by the court clerk in accordance with these rules:

(a) on the court's own initiative, or

(b) upon request.

(D) Timing of access to court records accessible under these rules is determined by date of acceptance as defined in Rule (2)(A)(1). Court records become accessible upon acceptance unless otherwise provided in these rules.

(E) Whenever the accessibility of a court record changes under these rules, or by court order, the court clerk will either remove or grant electronic access within a reasonable time.

RULE 4. CIVIL CASES

(A) Date of Accessibility.

(1) No court record will be accessible by the public until three business days after acceptance by the court clerk of the filing of such record and proof of service of process on at least one defendant. The date of acceptance must be determined by application of these rules.

(2) When a complaint is filed with a motion for approval of *ex parte* attachment or trustee process, no court records will be accessible by the public, by any other party to the case, or by attorneys of record until the court rules on the motion.

(3) When a motion for approval of *ex parte* attachment or trustee process is filed after the filing of the complaint, the motions and any attachments will not be accessible by the public, by any other party to the case, or by attorneys of record until the court rules on the motion.

(B) Civil Court Records Not Accessible by the Public. Court records related to the following proceedings are nonpublic:

(1) Mental health civil commitment proceedings;

(2) Medical malpractice screening panel proceedings;

(3) Sterilization proceedings;

(4) Proceedings for extreme weapon protection orders;

(5) HIV/AIDS testing proceedings; and

(6) Minor settlement proceedings.

(C) Limitations on Accessibility of Civil Court Records in Forcible Entry and Detainer (FED), Small Claims, and Foreclosure Cases Accessible by the Public only at a Courthouse. Before the entry of a judgment, court records in forcible entry and detainer (FED), small claims, and foreclosure cases are accessible by the public only at a courthouse. Court records in FED, small claims, and foreclosure cases are accessible by the public remotely only if and after a judgment has been entered against a defendant.

(D) Civil Court Records Accessible by the Public Remotely and at a Courthouse. Court records for any civil cases not listed in (B) or (C) are accessible by the public remotely and at any courthouse, except as otherwise provided by law or court order.

(E) Nonpublic Data, Documents, and Information. The data, documents, and information listed below, when filed in civil cases, are nonpublic, except as otherwise provided by law or court order.

(1) Full names of minors;

(2) Personally identifying information, including:

(a) Residence addresses;

(b) Telephone numbers;

(c) Personal, business, or school email addresses and other electronic addresses;

(d) Financial account numbers or statements, such as those that identify loans, bank accounts, mortgages, investment accounts, credit card numbers, personal identification numbers, or similar numerical identifiers;

(e) Driver's license numbers;

(f) Other personal identification numbers, such as Social Security and employer identification numbers, passport numbers, and state identification numbers;

(g) DNA-identifying data or information; and

(h) Dates of birth.

(3) Disability accommodation requests;

(4) Names, addresses, and personally identifying information of parties protected under a protection order, restraining order, or injunction, and of alleged victims of sexual offenses, domestic violence, or stalking;

(5) Images of minors and of persons of any age subject to guardianship, conservatorship, or mental health commitment proceedings;

(6) Images depicting nudity or of a sexual nature, including sexual acts, sexual contact, or sexual touching;

(7) Immigration and visa documents and any related work authorizations;

(8) Indigency affidavits and any attachments;

(9) Exhibits, affidavits, and other materials that are filed that contain otherwise confidential information as set out in these rules;

(10) Personal financial documents, including financial statements, tax documents including W-2s, paystubs, bank statements, account statements, and payment histories;

(11) Personal health information and medical records, including HIV/AIDS testing information and results, all mental health evaluations and records, forensic evaluations, substance use evaluations and treatment records, psychological records, and intelligence test documents and results;

(12) School and education records, including discipline and scholastic achievement information and data;

(13) Birth certificates and death certificates;

(14) Trade secrets;

(15) Requests for appointment of a guardian ad litem, orders appointing guardians ad litem, and guardian ad litem reports;

(16) Reports of sexual assault kits;

(17) Juror information, except as allowed in Rule 8; and

(18) Any other information or court record to which public access is prohibited by law.

RULE 5. CRIMINAL CASES

(A) Criminal Court Records Accessible by the Public Remotely and at a Courthouse. Court records listed below in criminal cases are accessible by the public both remotely and at a courthouse except as otherwise provided by law or subdivision (B) of this rule.

(1) Complaints, indictments, informations, motions, registries of actions, court judgments and commitment documents, and sentencing orders concerning:

(a) Pending criminal charges;

(b) Criminal charges that have resulted in either a conviction or an acquittal;

(c) Criminal charges that are dismissed by court order that are not part of a plea agreement;

(d) Criminal charges that are dismissed as a part of a plea agreement that results in:

(i) A conviction or adjudication on another charge,

(ii) An admission to a probation or administrative release violation,

(iii) A deferred disposition or filing of the charge, or

(iv) A dismissal of one charge and conviction on one or more others after a deferred disposition or filing;

(e) Criminal charges that are affected by conditional pardons or commutation;

(f) Criminal charges that were dismissed by the prosecutor without any plea to a related charge or any admission to a probation or administrative release violation; or

(g) Judgments of not criminally responsible.

(2) Motions for arrest warrants and any associated affidavits, not otherwise ordered impounded by the court pursuant to M.R.U. Crim. P. 4, after the warrant has been executed. Arrest warrants for failure to appear or for failure to pay a fine are accessible by the public remotely and at a courthouse before execution;

(3) Search warrants and associated affidavits, not otherwise ordered impounded by the court under M.R.U. Crim. P. 41 or 41B, only after a criminal charge related to the case is filed; and

(4) Pleadings, registries of actions, docket sheets, and court orders or decisions.

(B) Nonpublic Data, Documents, and Information. Data, documents, and information listed below, when filed in adult criminal cases, are nonpublic, except as provided by law.

(1) Names and dates of birth of persons, other than the accused and alleged adult accomplices;

(2) Personally identifying information, including:

(a) Residence addresses, other than of the accused;

(b) Telephone numbers;

(c) Personal, business, or school email addresses and other electronic addresses;

(d) Financial account numbers or statements, such as those that identify loans, bank accounts, mortgages, investment accounts, credit card numbers, personal identification numbers, or similar numerical identifiers;

(e) Driver's license numbers;

(f) Other personal identification numbers, such as Social Security and employer identification numbers, passport numbers, and state identification numbers; and

(g) DNA-identifying data or information.

(3) Disability accommodation requests;

(4) Names, addresses, and personally identifying information of parties protected under a protection order, restraining order, or injunction, and of alleged victims of sexual offenses, domestic violence, or stalking;

(5) Images of minors and of persons of any age subject to guardianship, conservatorship, or mental health commitment proceedings;

(6) Images depicting nudity or of a sexual nature, including sexual acts, sexual contact, or sexual touching;

(7) Immigration and visa documents and related work authorizations;

(8) Court records relating to applications for court-appointed counsel, including indigency affidavits;

(9) Exhibits, affidavits, and other materials that are filed that contain otherwise confidential information as set out in these rules;

(10) Personal financial documents, including financial statements, tax documents including W-2s, paystubs, bank statements, account statements, and payment histories;

(11) Personal health information and medical records, including HIV/AIDS testing information and results, all mental health evaluations and records, forensic evaluations, substance use evaluations and treatment records, psychological records, and intelligence test documents and results;

(12) School and education records, including discipline and scholastic achievement information and data;

(13) Birth certificates and death certificates;

(14) Trade secrets;

(15) Requests for appointment of a guardian ad litem, orders appointing guardians ad litem, and guardian ad litem reports;

(16) Reports of sexual assault kits;

(17) Juror information, except as allowed in Rule 8;

(18) In criminal prosecution for an alleged violation of a protection from abuse or harassment order, any identifying or residence information that is confidential under 19-A M.R.S. § 4008 or 5 M.R.S. § 4656;

(19) "Confidential criminal history record information," as defined by the Maine Criminal History Records Information Act, 16 M.R.S. §§ 701-710, except for information accessible by the public pursuant to Rule 5(A);

(20) Court records in grand jury proceedings;

(21) Presentence reports, including attachments and evaluation reports; and

(22) Any other information or court record to which public access is prohibited by law.

RULE 6. JUVENILE CASES

(A) Juvenile Case Records that are Nonpublic. There is no public access to the juvenile case records listed below:

(1) Juvenile petitions and orders of adjudication that are not open to inspection pursuant to subdivision (B);

(2) Juvenile case records of an alleged or adjudicated offense that would be a Class D or E crime or a civil violation if committed by an adult;

(3) Juvenile case records for a juvenile offense that is dismissed by the court;

(4) Any other juvenile case records where the Legislature has explicitly closed the proceedings; and

(5) Any other juvenile case records that are not explicitly identified as public by law. If there is any ambiguity as to the level of access to a juvenile case record, the juvenile records are nonpublic unless determined otherwise by court order.

(B) Juvenile Petitions and Orders of Adjudication Accessible by the Public. Upon request, the following juvenile case records will be printed by the court clerk and provided for inspection by the public in paper form at a courthouse:

(1) Juvenile petitions alleging murder, felony murder, or manslaughter; and

(2) Orders adjudicating a juvenile of an offense that would constitute murder, or a Class A, B, or C crime if committed by an adult.

(C) Juvenile Case Records that are Accessible to Alleged Victims.

(1) Access for Alleged Victims. Juvenile case records that are open to inspection by an alleged victim pursuant to 15 M.R.S. § 3308(2) will be printed by the clerk and provided for inspection in paper form at a courthouse.

(2) Alleged Victim Defined. For purposes of this rule, alleged victim of the juvenile crime includes:

(a) The alleged victim;

(b) If the alleged victim is a minor, the parent or parents, guardian, or legal custodian of the alleged victim; or

(c) If the alleged victim cannot act on the alleged victim's own behalf due to death, age, physical or mental disease or disorder or intellectual disability or autism or other reason, an immediate family member, guardian legal custodian of the alleged victim or a licensed professional investigator under Title 32, Chapter 89.

(D) Enhanced Access to Juvenile Case Records. Juvenile case records are accessible at the courthouse, and upon request, are accessible remotely by the following:

(1) The juvenile's parent, guardian, or legal custodian;

(2) An agency to which legal custody of the juvenile was transferred as a result of adjudication;

(3) The Department of Health and Human Services prior to adjudication if commitment to the Department of Health and Human Services is a proposed disposition; and

(4) The Victims' Compensation Board established in 5 M.R.S. § 12004-J(11) if a juvenile is alleged to have committed an offense upon which an application to the board is based.

(E) Access to Juvenile Case Records as Allowed by the Court. Whenever the court grants access to juvenile case records pursuant to 15 M.R.S. §§ 3308(4), (5), or (7), or 3308-A, the records may be accessed in the format allowed by the court.

(F) Nonpublic Juvenile Case Data, Documents, and Information. Even when filed in otherwise public juvenile case records, the data, documents, and information listed below are nonpublic:

(1) Names and dates of birth of persons, other than the accused and alleged adult accomplices;

(2) Personally identifying information, including:

(a) Residence addresses;

(b) Telephone numbers;

(c) Personal, business, or school email addresses and other electronic addresses;

(d) Financial account numbers or statements, such as those that identify loans, bank accounts, mortgages, investment

accounts, credit card numbers, personal identification numbers, or similar numerical identifiers;

(e) Driver's license numbers;

(f) Other personal identification numbers, such as Social Security and employer identification numbers, passport numbers, and state identification numbers; and

(g) DNA-identifying data or information.

(3) Disability accommodation requests;

(4) Names, addresses, and personally identifying information of parties protected under a protection order, restraining order, or injunction, and of alleged victims of sexual offenses, domestic violence, or stalking;

(5) Images of minors and of persons of any age subject to guardianship, conservatorship, or mental health commitment proceedings;

(6) Images depicting nudity or of a sexual nature, including sexual acts, sexual contact, or sexual touching;

(7) Immigration and visa documents and related work authorizations;

(8) Court records relating to applications for court-appointed counsel, including indigency affidavits;

(9) Exhibits, affidavits, and other materials that are filed that contain otherwise confidential information as set out in these rules;

(10) Personal financial documents, including financial statements, tax documents including W-2s, paystubs, bank statements, account statements, and payment histories;

(11) Personal health information and medical records, including HIV/AIDS testing information and results, all mental health evaluations and records, forensic evaluations, substance use evaluations and

treatment records, psychological records, and intelligence test documents and results;

(12) School and education records, including discipline and scholastic achievement information and data;

(13) Birth certificates and death certificates;

(14) Trade secrets;

(15) Requests for appointment of a guardian ad litem, orders appointing guardians ad litem, and guardian ad litem reports;

(16) Reports of sexual assault kits;

(17) Documents concerning the issue of the juvenile's competency unless and until there is a decision finding the juvenile competent to stand trial;

(18) Any information in an order of adjudication or other document about determination of Special Immigrant Juvenile Status;

(19) Presentence reports, including attachments and evaluation reports; and

(20) Any other information or court record to which public access is prohibited by law.

(G) Sealing or Impounding Public Juvenile Case Records.

(1) Sealing of juvenile case records of a person adjudicated to have committed a juvenile crime.

(a) Pursuant to 15 M.R.S. § 3308(8), a person adjudicated to have committed a juvenile crime may petition the court to seal from public inspection all juvenile case records pertaining to the juvenile crime and its disposition, and to any prior juvenile case records and their dispositions if:

(i) At least 3 years have passed since the person's discharge from the disposition ordered for that juvenile crime;

(ii) Since the date of disposition, the person has not been adjudicated to have committed a juvenile crime and has not been convicted of committing a crime; and

(iii) There are no current adjudicatory proceedings pending for a juvenile or other crime.

(b) The court may grant the petition if it finds that the requirements of subdivision (G)(1)(a) are satisfied, unless it finds that the general public's right to information substantially outweighs the juvenile's interest in privacy.

(c) Section 3308(8)(C) of Title 15 controls which persons have access to the sealed juvenile case records. Whenever access is allowed under this subdivision, the juvenile case records shall be accessible remotely and at the courthouse.

(d) If juvenile case records are sealed pursuant to subdivision (G)(1)(a) of this rule, the juvenile may respond to inquiries other than from the courts and criminal justice agencies about that person's juvenile crimes, the juvenile case records of which have been sealed, as if the juvenile crimes had never occurred, without being subject to any sanctions.

(2) The procedure for sealing juvenile case records pre-adjudication shall be governed by Rule 10(A)(2). It is the responsibility of the filing party to ensure that sealed or impounded juvenile case records are submitted to the court in accordance with Rule 12.

RULE 7. FAMILY MATTERS, CHILD PROTECTION MATTERS, AND PROTECTION ORDER CASES

(A) No court records are accessible by the public remotely.

(B) No court records are accessible by the public in the following proceedings:

(1) Child protection matters;

(2) Adoptions;

(3) Guardianships of minors;

(4) Name changes for minors;

(5) Petitions for court-authorized abortions for minors;

(6) Emancipations of minors; and

(7) Assisted reproduction matters, including noncompliance with gestational carrier agreements.

(C) Court Records in Family Matters, Child Protection Matters, and Protection Order Cases Accessible by the Public only at a Courthouse. Court records listed below are accessible by the public at a courthouse except as provided by law or subdivisions (B) or (D) of this rule.

(1) Protection from abuse cases;

(2) Protection from harassment cases; and

(3) The following family matters:

(a) Divorce, annulment, or judicial separation;

(b) Parental rights and responsibilities, including the establishment or enforcement of a child support obligation;

(c) Establishment of parentage including complaints for de facto parenthood; and

(d) Grandparent or great-grandparent visitation.

(D) Nonpublic Records. The documents listed below, when filed in family matters and protection order cases, are nonpublic, except as provided by law.

(1) Social Security Confidential Disclosure Form;

(2) Disability accommodation requests;

(3) Images of minors and of persons of any age subject to guardianship, conservatorship, or mental health commitment proceedings;

(4) Images depicting nudity or of a sexual nature, including sexual acts, sexual contact, or sexual touching;

(5) Immigration and visa documents and related work authorizations;

(6) Indigency affidavits and any attachments;

(7) Exhibits, affidavits, and other materials that are filed that include otherwise confidential documents as set out in this Rule;

(8) Personal financial documents, including child support affidavits and worksheets, financial statements, tax documents including W-2s, paystubs, bank statements, account statements, qualified domestic relations order, and payment histories;

(9) Personal health and medical records, including HIV/AIDS testing documents, all mental health evaluations and records, forensic evaluations, substance use evaluations and treatment records, psychological records, and intelligence test documents and results;

(10) School and education records, including discipline and scholastic achievement reports;

(11) Birth certificates and death certificates;

(12) Documents containing trade secrets;

(13) Requests for appointment of a guardian ad litem, orders appointing guardians ad litem, and guardian ad litem reports;

(14) Reports of sexual assault kits;

(15) Affidavit for confidential address or contact information, and any identifying or residence information that is confidential under 19-A M.R.S. § 4008, 5 M.R.S. § 4656, or M.R. Civ. P. 102;

(16) Family and probate matter summary sheet; and

(17) Any other court record or document to which public access is prohibited by law.

RULE 8. JUROR INFORMATION

(A) Trial Juries.

(1) No Public Access. All juror information regarding trial jurors or prospective trial jurors is confidential and is not accessible to anyone, except as provided by statute, these Rules, or applicable rules of procedure.

(2) Limited Access by Party or Attorney During Jury Service. During the period of service of a jury pool, juror information is accessible only:

(a) To attorneys of record, their agents, and self-represented litigants for cases for which jurors are being selected from the jury pool;

(b) For purposes of conducting *voir dire* examination;

(c) At the courthouse where *voir dire* examination takes place; and

(d) On the condition that the authorized recipient of the juror information provides a written, signed certification that the recipient will comply with all requirements of 14 M.R.S.

§ 1254-A(7) to (9), and all applicable rules of procedure now or hereafter promulgated by the Maine Supreme Judicial Court, and will return all juror information, and related materials, to the clerk at the conclusion of the case in the trial court, on penalty of contempt.

(3) After Jury Service Motion and Affidavit Required. After expiration of the period of service for all trial jurors in the pool, public access to jurors' names may be requested only by motion to the court with an affidavit stating the basis for the request. The court may grant the motion, subject to appropriate conditions to protect juror privacy, only upon a determination that the disclosure is in the interests of justice. The factors the court may consider in determining if the disclosure is in the interests of justice include, but are not limited to, encouraging candid responses from jurors, the safety and privacy interests of jurors, and the interests of the media and the public in ensuring that trials are conducted ethically and without bias.

(4) Use of Juror Information. Dissemination and use of juror information is subject to and controlled by 14 M.R.S. §§ 1254-A and 1254-B.

(B) Grand Juries. Information about grand jurors and prospective grand jurors is accessible only by the court or court clerk.

RULE 9. PROCEDURES FOR ACCESS TO ELECTRONIC COURT RECORDS

(A) Remote Access. Court records that are accessible by the public remotely may be inspected and reproduced at any time as permitted by these rules. Remote access to court records may require a user account, registration by the user, the payment of fees as provided elsewhere in these rules, and any other procedures and payments that are reasonably necessary for administration of the system as determined by the Supreme Judicial Court.

(B) Courthouse Access. All court records accessible by the public may be inspected and reproduced at a courthouse as follows:

(1) Computer access. Members of the public may access a public access computer during regular courthouse business hours, subject to technical difficulties or system maintenance. The court clerk may set reasonable limits on the time and volume of access to the public access computer to protect the court clerk's office from undue disruption and to promote access to the public access computer for all users. There is no fee to use the public access computer. A fee may be required for printouts of electronic court records from a public access computer as provided in Rule 14.

(2) Request for assistance from the court clerk. Requests for help searching for and finding court records at a courthouse will be made at the court clerk's office. Such requests will be handled administratively and will not require a court order. The court clerk may ask the requesting person to complete a written request for the court record. If a request does not provide information sufficient to identify the record sought, the court clerk may decline to provide the requested assistance. The court clerk may set reasonable limits on the time spent helping the public with court records requests to protect the court clerk's office from undue disruption.

(C) Access to Exhibits Submitted with Court Filings. Exhibits submitted with court filings that are accessible by the public under these rules and are included in the definition of court records under Rule 2(A)(17) may be reproduced, subject to payment of fees and charges as provided in Rule 14. The rules do not address electronic access to trial and hearing exhibits because under Rule 34(C) trial and hearing exhibits are not part of the electronic case file even if filed electronically with the court.

(D) Available Formats for Reproduction.

(1) Printout. Court records that are accessible by the public under these rules may be printed subject to the payment of fees and charges as provided in Rule 14.

(2) Audio or audiovisual recordings of public court proceedings. Audio or audiovisual recordings of public court proceedings that are received or maintained by the Maine Judicial Branch in electronic format in connection with a particular case or proceeding are accessible by the public only by court order, except as provided by

law. A fee may be charged for access to or reproduction of audio or audiovisual recordings as provided in Rule 14.

(3) Transcripts of public court proceedings. Transcripts of public court proceedings that are received or maintained by the Maine Judicial Branch in electronic format in connection with a particular case or proceeding are accessible by the public. A fee may be charged for access to transcripts, as provided in Rule 14.

(E) Requester's Self-Service Duplication of a Court Record Not Permitted. Use of a smart phone or other electronic imaging device or any other means to duplicate or store copies of electronic court records is not permitted.

RULE 10. SEALING OR IMPOUNDING PUBLIC CASES OR COURT RECORDS

Cases or court records sealed or impounded under this rule are not accessible by the public.

(A) Procedure for Sealing or Impounding.

(1) The procedure for sealing or impounding juvenile case records is controlled by Rule 6(G).

(2) The procedure for sealing all cases or court records other than post-adjudication juvenile case records is as follows:

(a) Any party or any person or entity that has standing to do so may file a motion to seal or impound a case that would otherwise be accessible to the public. Such a motion must be accompanied by an affidavit stating the basis upon which the movant has standing, and the reason for the request to seal or impound, including a statement describing the harm that is alleged will occur should the motion be denied. The motion and all attachments shall be labeled "NONPUBLIC" when filed.

(b) Any party or any person or entity that has standing to do so may file a motion to seal or impound a court record that is

already accessible by the public, or would be accessible by the public if filed. Such a motion must be accompanied by an affidavit stating the basis upon which the movant has standing, and the reason for the request to seal or impound, including a statement describing the harm that is alleged will occur should the motion be denied. The motion and all attachments shall be labeled "NONPUBLIC" when filed.

(c) The person filing the motion must serve the motion to seal or impound on all parties unless the motion is filed *ex parte*.

(d) Upon acceptance by the court clerk of a motion to seal or impound, neither the motion nor any related documents will be accessible by the public, pending the court's ruling on the motion. The court clerk shall not docket the filing of the motion on the registry of actions until the court has ruled on the motion.

(e) Upon acceptance by the court clerk of an *ex parte* motion to seal or impound, neither the motion nor any related documents or related entries on the registry of actions will be accessible by the public or by any other party, pending the court's ruling on the motion.

(f) The court may seal or impound a case or a court record from public access if it finds that a reasonable expectation of privacy substantially outweighs the public interest in public access to the case or court record. In weighing a reasonable expectation of privacy against the public interest in access to the case or court record, the court will consider the following factors:

(i) An individual's personal safety, health, or well-being,

(ii) An individual's substantial personal, business, or reputational interest, and

(iii) The public's interest in access to information in the court record.

(g) If the court grants a motion to seal or impound a case, no existing court records in that case or any court records subsequently filed are accessible by the public.

(B) Handling of Sealed or Impounded Court Records. It is the responsibility of the filing party to ensure that sealed or impounded court records are submitted to the court in accordance with Rule 12.

Advisory Note

In determining whether to grant a motion to seal or impound, courts should be guided by the recognition that "the courts of this country recognize a general right to inspect and copy public records and documents." *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597 (1978). As courts have noted, however, this "general availability of court documents . . . is subject to 'countervailing interests [that] heavily outweigh the public interests in access.'" *Carey v. Me. Bd. of Overseers of the Bar*, 2018 ME 73, ¶ 11, 186 A.3d 848 (quoting *Rushford v. New Yorker Magazine, Inc.*, 846 F. 2d 249, 253 (4th Cir. 1988)).

RULE 11. OBTAINING ACCESS TO SEALED OR IMPOUNDED CASES OR COURT RECORDS AND TO CERTAIN NONPUBLIC CASES OR COURT RECORDS

(A) Scope. This rule applies to motions for access to

(1) Sealed or impounded cases or court records; or

(2) Cases or court records made nonpublic by law where that law authorizes the court to allow access in specific circumstances.

(B) How Access is Requested. Any person seeking access to sealed or impounded or nonpublic cases or court records may file a motion for access in accordance with applicable court rules of procedure. A nonparty who files a motion for access will be considered a party in interest for the limited purposes of the motion brought under this rule.

(C) Procedure for Service when Addresses are Confidential.

(1) In criminal cases, when the defendant is required to serve a motion for access on an alleged victim of a crime or a witness who testified at trial, service shall be on the office responsible for prosecuting the case, which shall send or forward the notice or motion to the alleged victim or witness;

(2) Except as set forth in subdivision (C)(1), when serving a motion for access on a party or affected nonparty whose name or address is confidential, the movant must state prominently in the caption of the motion for access, "Confidential Party: Court Service Requested" or "Confidential Affected Nonparty: Court Service Requested." The court clerk will provide a copy of the motion to the party or affected nonparty by any method permitted in the rules of procedure, in a way that does not reveal the confidential information.

(3) The court may waive this service requirement on motion or at any time on its own initiative if it finds that good faith efforts to locate the person to be served are not likely to be successful or could endanger that person's health, safety, or well-being.

(D) Opportunity to be Heard. The movant, the parties, and the affected persons will have an opportunity to be heard. The court will consider written submissions and, in its discretion, may hold a hearing.

(E) Standard to Obtain Access.

(1) Previously sealed or impounded cases or court records. A motion for access to previously sealed or impounded cases or court records may be granted only if the court finds that the previous court order impounding or sealing the case or court record must be amended because new information about the need for public access to the case or court record convinces the court that the need for public access now substantially outweighs a party's reasonable expectation of privacy.

(2) Nonpublic Records. A motion for access to nonpublic cases or court records will be considered only if the motion includes explicit legal authority for public or limited nonparty access to those cases or court records. If there is no explicit standard for review, then access will

be granted only upon a showing of extraordinary circumstances that require the cases or court records to be made available.

(F) Extent of Access if Motion Granted. If the court allows access, it may impose reasonable conditions to protect the privacy interests at issue. Cases or court records made accessible to a specific movant are not accessible by the public until the court orders otherwise.

(G) Access in Motions Practice. A motion to allow access, the response to such a motion, and the order ruling on such a motion must be written in a manner that does not disclose information from sealed or impounded cases or court records. Motions and responses are sealed or impounded until the court orders otherwise.

(H) Appeal. A party, party in interest, or affected nonparty may appeal from a court order regarding access to a case or a court record under these rules in accordance with the Maine Rules of Appellate Procedure.

(I) Effective Date. The effective date of any order in a proceeding under this rule granting access will be suspended for a period of three days following entry of the order and the case or the court record at issue will remain nonpublic during this three-day period.

If any party to the proceeding files an appeal from the order in compliance with the applicable rules of appellate procedure before the end of the three-day period, the cases or court records at issue will not be accessible by the public or the party during the pendency of the appeal.

RULE 12. IDENTIFICATION AND HANDLING OF SEALED, IMPOUNDED, OR NONPUBLIC CASES, COURT RECORDS , DATA, DOCUMENTS, AND INFORMATION

It is the responsibility of the filing party to ensure that sealed, impounded, or nonpublic cases, court records, data, documents, and information are redacted before submission, or otherwise submitted to the court in accordance with these rules.

(A) For all cases or court records designated as sealed, impounded, or nonpublic, every filing must be clearly and conspicuously marked, "NONPUBLIC."

(B) When a document or other filing that is nonpublic or that has been sealed or impounded is submitted to the court in a public case, that document or filing must be clearly and conspicuously marked, "NONPUBLIC."

(C) No records, documents, or information designated as sealed, impounded, or nonpublic will be submitted to the court as part of a public document.

(D) If a filed document does not comply with the requirements of these rules, a court may, upon motion or its own initiative, order the filed document returned, and that document may be deemed not to have been filed. A court may impose sanctions on any party or person filing a noncompliant document.

RULE 13. COMPILED, AGGREGATE, AND BULK DATA

Except in extraordinary circumstances, compiled, aggregate, and bulk data are not court records accessible by the public. Requests for compiled, aggregate, and bulk data may be submitted to the State Court Administrator or designee. In deciding whether to grant the request, the State Court Administrator or designee will consider staffing resources, technical barriers, and any applicable administrative order. No access to compiled, aggregate, or bulk data will be considered until all regions have been fully converted to the EFS.

RULE 14. ACCESS FEES

The court may charge reasonable fees for providing access to court records pursuant to these rules. For persons other than parties or their attorneys, a fee may be required for inspecting or copying any court records. If the court finds that the request for access is reasonable and the person making the request is without sufficient funds to pay for access to the court records, the

court shall order the fee be waived. A fee schedule will be published and publicly posted.

RULE 15. CLERICAL ERRORS

(A) To correct a clerical error in a court record, a party must submit a request in writing to the court clerk.

(B) A request to correct a clerical error must state:

(1) The information that the party claims is wrong, and

(2) Enough facts to support the claim that the information is wrong.

The request will include supporting documents as needed to prove there is a clerical error in the court record and to correct it.

(C) The requesting party must send copies of the request to all parties to the case.

(D) Within 21 days after receiving a request, the court clerk will respond in writing to all parties to the case in one of the following ways, stating that:

(1) A clerical error does exist in the court record, and the information in question has been corrected;

(2) A clerical error does not exist in the court record;

(3) The request does not state enough information or facts to determine what information is claimed to be wrong, and no further action will be taken on the request;

(4) The request does not relate to a court record covered by these rules, and no further action will be taken on the request; or

(5) The request has been received, and an additional period, up to 35 days, is needed to complete a review of the request.

(E) Any party may seek review of the court clerk's response. A request for review must be submitted to the court clerk within 14 days after the mailing date of the court clerk's response. The request to review the court clerk's response will be reviewed by the justice, judge, or magistrate who presided over the case.

RULES 16 TO 30. [RESERVED]

PART TWO: RULES OF ELECTRONIC FILING AND SERVICE

RULE 31. GENERAL CONDITIONS FOR FILING AND SERVICE

(A) Purpose and Applicability. These rules establish procedures governing the electronic filing and service of all documents and pleadings to and from all the courts within the Maine Judicial Branch. Upon implementation of electronic filing in each of the courts, electronic filing of all documents shall be mandatory in accordance with Rule 33 of these rules. These rules shall be construed liberally to promote the administration of justice.

(B) Conditions of Electronic Filing. To have access to the EFS, each filing party agrees to, and must:

(1) Register for access to the EFS;

(2) Comply with the registration conditions when using the EFS; and

(3) Maintain one or more working email addresses at which the filer agrees to accept email notification and service from the EFS.

(C) Forms. Forms developed by the Maine Judicial Branch are the official court forms and, if an applicable court form exists, it must be used.

RULE 32. ELECTRONIC CASE FILE

(A) Electronic Case File. The electronic case file is the sole repository of all court records filed in a case for the duration of the case and the applicable retention period under the records retention schedule of the Maine Judicial Branch. Each document filed in a case shall be entered into the electronic case file and, after entry in compliance with these rules, shall be the sole official court record of the filing.

(B) Acceptance. Submitted documents become part of the electronic case file only upon acceptance by the court clerk.

(C) Conversion Discrepancies. Any party has 70 days from the date of acceptance or until the final hearing on the complaint, whichever occurs first, to file a motion to correct any error caused by the conversion process.

(D) Retention of Conventionally Filed Documents After Conversion. The court will retain a conventionally filed document in its original format for 70 days following conversion by the court clerk. After 70 days, the court clerk may destroy the conventionally filed document, unless:

(1) The filer requests the return of the conventionally filed document before the expiration of the 70-day period; or

(2) The filer challenges the accuracy of the converted document before the expiration of the 70 days and retention of the conventionally filed document is necessary to resolve the dispute.

Advisory Note

Documents served through the EFS but not filed with the court are not in the electronic case file.

RULE 33. USE OF THE ELECTRONIC FILING SYSTEM

(A) Registration. To use the EFS, a filing party must register as a user and execute a user agreement. Executing a user agreement constitutes consent to receive electronic notice and electronic service of all documents

through the EFS, except for service of process, warrants, and summonses, which shall be served in accordance with M.R. Civ. P. 4 and M.R. Crim. P. 4.

(B) Required Use of the EFS. Except as provided in subdivision (C), use of the EFS in all case types is mandatory for required electronic filers. "Required electronic filers" are:

(1) Attorneys acting on behalf of a party or themselves in a court case;

(2) State, county, and municipal filers except for Maine Law Enforcement, meaning all officers defined in 25 M.R.S. § 2801-A, and Bail Commissioners, as defined in 15 M.R.S. § 1023; and

(3) Self-represented litigants filing or intending to file more than six cases that are filed and are not emergency cases in the current calendar year. For purposes of this subdivision, emergency cases are protection from abuse or harassment requests, mental health requests, requests for emergency guardianship of a minor, and three-party child protection petitions.

(C) Good Cause Exceptions. A required electronic filer may be excused from mandatory use of the EFS only upon motion and a showing of good cause. Good cause means circumstances that would render electronic filing such a hardship that the required electronic filer would be denied access to the court. For the limited purpose of seeking an exception to mandatory electronic filing and service, a required electronic filer may file a motion conventionally. If the court grants a motion for a good cause exception, the court shall establish the scope of the exception. The court may amend or revoke the good cause exception on its own initiative or upon motion of a party.

(D) Contact Information. A filer who is not required to use the EFS must provide the court with a mailing address for service of documents, and must notify the court in writing of any change of mailing address. If the filer has alleged in an affidavit or pleading under oath that the health, safety, or welfare of the filer or a minor child would be jeopardized by disclosure of the address, then the clerk shall seal the address from the public and all other parties.

(E) Elective Use of the EFS. Even where use of the EFS is not required, a filer in a case may elect to register and use the EFS in compliance with subdivision (A). After electing to use the EFS, the filer must file, serve, and accept service electronically for the duration of the case, unless excused by the court upon a motion and showing of good cause.

(F) Misuse of the EFS. Misuse occurs when any user attempts to harm, disrupt, alter, or interfere with the EFS or any records maintained in the system, or attempts to use or access information on the system without proper authorization. Misuse of the EFS might subject the user to criminal prosecution. Misuse may also result in suspension or loss of a user's registration or any other penalty that may be imposed by the court. Misuse of the EFS by attorneys may constitute a violation of the Maine Rules of Professional Conduct. Attorneys are responsible for any misuse of the EFS by third parties whom the attorney has authorized or directed to use that attorney's individual or firm EFS account.

Advisory Note

The following are examples of what may a qualify for a "good cause" exception for Required Electronic Filers under Rule 33(C): disability; limited English proficiency; electrical or internet outages; disaster; lack of internet access or safe internet access; or oversize exhibits such as maps and blueprints.

The scope of the good cause waiver is in the discretion of the court and may be by case, by filing, or by time period.

RULE 34. DOCUMENT REQUIREMENTS

(A) Requirements for Documents Filed Electronically

(1) Document Type and Format. A document submitted electronically to the court must be in the form of a Portable Document Format (PDF), be directly converted to PDF rather than scanned (if possible), and not exceed 50 megabytes. A document that exceeds the size limit must be broken down and submitted as separate files that do not exceed 50 megabytes each. Separate files under this section must include

in the "Comments to Court" field for each submission a description that clearly identifies the part of the document that the file represents.

(2) Documents Must be Submitted Separately. All documents must be submitted individually as separate files with the same submission. The filer must include in the "Filing Description" field a description that clearly identifies each document. For each separate document submitted, the detailed caption title, filing description in the EFS, and .pdf file title must be substantially identical.

(3) Consolidated Cases. When a court consolidates two or more cases for purposes of court events, including hearings, but retains separate docket numbers, a party electronically filing a document that is applicable to all of those cases must electronically file and serve the document in each case, using appropriate case docket numbers.

(4) Additional Technical Format Requirements. All electronic documents shall be self-contained and must not contain live links to external papers or websites.

(B) Documents or Materials Not Filed in Electronic Format

(1) Materials that are required to be filed with the court and that cannot be converted into electronic format, such as videotapes, radiographs, and other items that are not intelligible when scanned, may be filed conventionally. The filing party shall file a Notice of Conventional Filing that shall be docketed into the EFS to denote that a conventional filing has been made and that the material is being held in the clerk's office. The filing party shall serve the materials conventionally, if required.

(2) Documents or materials that must be filed conventionally include:

(a) Documents subject to *in camera* inspection, including those produced by the Department of Health and Human Services pursuant to 22 M.R.S. § 4008;

(b) A record or image that is barred from electronic transmission or storage by law, including sexually explicit images of a minor;

(c) Proposed orders drafted by attorneys during court proceedings; and

(d) Anything else required to be filed conventionally by court order.

(C) Trial and Hearing Exhibits. Trial and hearing exhibits shall not be part of the electronic case file, but shall be received, held, and retained by the court until all opportunities for appeal have been exhausted and as required by law or court order.

Advisory Note

Rule 34(A)(2) requires that each electronic document be filed as a separate electronic file. However, separate electronic documents may be filed within the same submission. For example, a filer initiating a parental rights and responsibilities case would file the complaint and child support affidavit as separate documents within the same submission.

When a large document is submitted in separate files, each submission should be identified with a description in the "Comments To Court" field such as, for example, "Motion for Summary Judgment, part 1 of 2".

RULE 35. TIME OF FILING, SERVICE, AND RESPONSE

(A) Availability of Electronic Filing System. The EFS will receive electronic documents except when the system is unavailable due to scheduled or other maintenance.

(B) File Date. A "day" begins at 12:00 a.m. and ends at 11:59 p.m. in the time zone where the courthouse is located. For a document that is electronically submitted between 12:00 a.m. and 11:59 p.m. in the time zone where the courthouse is located on Monday through Friday, the "file date" will be the day it is submitted. If a document is submitted on a Saturday, Sunday,

or legal holiday, the file date will be the next business day. For any questions of timeliness, the time and date registered by the EFS will be determinative. For a document electronically submitted, the file date will apply for purposes of meeting the statute of limitations or any other filing deadlines, even if the document is accepted by the clerk on a later date, except as provided in subdivision (D) of this rule. A conventionally filed document is deemed submitted when presented to the court clerk.

(C) Service Date of the Submitted Document. The service date of submitted documents will be the date of submission, if served pursuant to Rule 36 and the documents are accepted as filed.

(D) Acceptance or Rejection Procedure.

(1) The clerk's review of a submission for acceptance or rejection is purely ministerial.

(2) Following submission, the court clerk will accept or reject the electronic document.

(a) If the submission is accepted, it is deemed filed and is entered into the electronic case file with the file date as determined under subdivision (B) of this rule. When a submission is accepted, the court will send an acceptance notice to the parties.

(b) If the submission is rejected, the court will send a rejection notice to the submitting party and the submission shall not be entered on the registry of actions. The rejection notice shall identify the basis for the rejection.

(3) If a submission is rejected, the filing party shall serve the notice of rejection on the opposing parties.

(E) Resubmission and Relief.

(1) Requirements of Resubmission. A filer who resubmits a document under this rule must include in the "Comments to Court" field, or, if conventionally filed, in the cover letter accompanying the resubmission, the following:

(a) The words, "Resubmission of filing, original submission unsuccessful";

(b) The date of the original attempted submission;

(c) The date of the rejection notice; and

(d) A statement confirming that this is the first resubmission.

(2) File Date of Resubmitted Document.

(a) Resubmissions That Relate Back Automatically. If the filer resubmits a corrected version of the rejected document, and it is accepted by the court clerk, the file date of the resubmitted document will automatically relate back to the file date of the original submission if:

(i) it is the first resubmission, and

(ii) it is submitted within four business days after the date of the rejection notice. If notice of the rejection is provided by mail, the filer has three additional days, for a total of seven days, to resubmit the filing.

(b) Resubmissions That Relate Back with Leave of Court. If the filer resubmits the rejected document more than once or submits the rejected document more than four business days after the date of the rejection notice, the file date of the resubmitted document will only relate back to the file date of the original submission upon court approval.

(c) Response Time. If the file date relates back to the file date of the original submission, the court will adjust the schedule for responding to these documents by adding four business days to the response time. The court may also postpone a court event or provide other relief.

(3) Service Date of Resubmitted Document. The service date of resubmitted documents will be the original date of service if the resubmission is accepted.

(F) Unavailability of the Electronic Filing System and Relief.

(1) EFS Unavailable. Any filer may obtain relief if the EFS is not operating through no fault of the filer. Technical problems with the filer's equipment or attempted transmission within the filer's control will not excuse an untimely filing.

(2) Relief. Upon satisfactory proof of the system's temporary unavailability or other technical problem, the file date of the document will relate back to the file date of the first filing attempt. The court, in its discretion, may adjust the schedule for responding to any affected filings, postpone the next court event, or provide other relief. The process for resubmission of the filing shall be in accordance with subdivision (E), and may include, with the resubmission, supporting exhibits showing system unavailability.

Advisory Note

The court clerk does not review for legal sufficiency of the filing, which is clearly a judicial function. The court clerk's review is similar to that described in M.R. Civ. P. 5(f). The court clerk's review includes, for example, signatures, bar number, and required fees or waiver request.

RULE 36. SERVICE OF ELECTRONIC DOCUMENTS

(A) Applicability. All documents filed in the EFS must be served through the EFS, except the following, which must be served by conventional service:

(1) Summonses, complaints, indictments, informations, and other case initiating documents;

(2) Subpoenas;

(3) Any documents that cannot by law be served electronically;

(4) Any documents to be served on those who are not registered users; and

(5) Any documents for which a court order requires conventional service.

(B) Service Contacts. The filer must provide the name and service email address of the filer and any alternative or additional service contacts to be used by the EFS in the case. Designation of any email recipients as alternative or additional service contacts is deemed to provide consent to have electronic documents filed in the case served on those service contacts. The filer is responsible for updating contact information, and may update service contacts through the user agreement.

(C) Registered User Consent. Upon the initiation of a case, filing of responsive pleading, or submission of an entry of appearance in a case, registered users are deemed to have consented to receive electronic service of all documents through the EFS.

(D) Service Upon Registered Users. When a filer submits a document to the EFS that must be served electronically, the filer must complete service on any required service contacts at the time of submission.

(E) Conventional Service. A party who is not a registered user must be served conventionally. After a party who was not a registered user becomes a registered user, that party must be served electronically.

(F) Service of Sealed, Impounded, and Nonpublic Documents, and Documents Submitted for *In Camera* Review. Regardless of method of filing, sealed, impounded, and nonpublic documents, and documents submitted for *in camera* review must not be served on service contacts or conventional service recipients, either through a hyperlink or paper copies.

If the documents are filed electronically, the EFS will generate a notice to all service contacts in the case. If the documents are filed conventionally, the filer must serve notice that the documents were filed conventionally.

If the court orders that the documents filed are accessible to the public, the court will provide a hyperlink to or paper copies of the documents to the service contacts and any recipients of conventional service.

(G) Certificate of Service. A certificate of service must be filed with the court only when documents are served conventionally, in accordance with the applicable procedural rules.

(H) Service of Documents by the Court.

(1) Service of documents by the court on registered users will be made electronically to all service contacts in a case.

(2) Service of documents by the court on those who are not registered users, including rejection notices of submissions filed conventionally, will be made by conventional service.

(I) Service of Discovery. Service of discovery documents through the EFS is permitted but not required. Discovery documents served through the EFS are not court records and are nonpublic.

Advisory Note

Under this rule, electronic service of a complaint, indictment, or information on a criminal defendant prior to arrest is not required.

RULE 37. ELECTRONIC SIGNATURES AND DOCUMENT AUTHENTICITY

(A) Types of Electronic Signatures. The three forms of electronic signature allowed under this rule are defined as follows:

(1) "Facsimile signature" means a captured image incorporated in the document;

(2) "Scanned signature" means a signature affixed by the signer in ink on the signature line of a paper document and scanned with the document for electronic filing; and

(3) "Typographical signature" means a signature block with the name of the signer typed on the signature line preceded by "/s/".

(B) Signatures of Justices, Judges, Magistrates, and Clerks. Any document that is signed by a justice, judge, magistrate, or court clerk and filed electronically must bear either a facsimile signature or a scanned signature.

(C) Signatures of Court Reporters. A court reporter's signature on any document or transcript prepared by a court reporter for inclusion in the court record must be a facsimile signature, a scanned signature, or a typographical signature.

(D) Signatures of Registered Users. The username and password required to submit documents to the EFS shall serve as that registered user's signature. The electronically filed document shall bear a facsimile or a typographical signature along with the typed name, address, email address, and telephone number of the registered user and, if the registered user is an attorney, the attorney's bar number.

(E) Penalty of Perjury, Acknowledgment, Notarization, and Attestation.

(1) Any party and any attorney representing a party who is filing any document consisting of or containing statements, affirmations, or averments made by the party that are otherwise required to be sworn under oath, acknowledged, attested, or notarized may file the document without oath or notarization provided that, in lieu of an oath, the party affixes the party's typographical or facsimile signature immediately below a declaration using the following language: "I swear under penalty of perjury that the above statements are true and correct. I understand that these statements are made for use as evidence in court and that I am subject to prosecution for perjury punishable by up to 5 years in prison and a fine of up to $5,000.00 if I give false information to the court."

(2) A document electronically filed or served using the EFS that is required by law to include a signature of a nonparty and to be signed under penalty of perjury or to be notarized, acknowledged, or attested may be filed electronically provided that the declarant, notary public, and any other necessary party or witness have properly signed in ink the paper form of the document and the executed document is converted for filing in a format that accurately reproduces the original signatures and contents of the document. By electronically filing the

document, the attorney or self-represented litigant attests that the document and signature are authentic.

(F) Documents Requiring Signature of Opposing Parties. A document to be filed electronically requiring the signatures of opposing parties must be signed by all parties in accordance with these rules. By electronically filing the document, the attorney or self-represented litigant attests that the document and signature are authentic.

(G) Certification. By electronically filing or submitting a document using the EFS or presenting a filing to a court clerk that is converted and filed, the filer is certifying compliance with the signature requirements of these rules. Signatures on the electronic document shall have the same legal effect as the signatures on the original document.

(H) Retention of Original Documents with Signatures of Anyone Other than the Filer. By electronically filing a converted document, the filer certifies that the converted document is an accurate image of the original. A filer who converts a paper document with the handwritten signature of anyone other than the filer to an electronic format for filing shall retain the original document in paper form for two years after the later of the entry of final judgment or the conclusion of an appeal and shall provide the original document upon request by the court. This rule does not affect other retention periods required by law.

RULE 38. NONPUBLIC COURT FILINGS

(A) Burden on Parties. Parties are responsible for omitting or redacting nonpublic information in documents filed into the EFS, whether filed electronically or conventionally. With the exception of *in camera* reviews, the court will not review any document to ensure compliance with this rule and is not responsible or liable for the inclusion of nonpublic information in any filed document.

(B) Documents Containing Nonpublic Information.

(1) Omission or Redaction. When documents containing nonpublic information are necessary for the adjudication of a case, the

filing party must ensure that nonpublic information is appropriately omitted or redacted in the filing and that the nonpublic information is submitted in a separate document along with the filing. When a separate document is filed containing nonpublic information, the user must include in the "Comments to Court" field the designation "NONPUBLIC" followed by the name of the court filing (e.g. "NONPUBLIC, Motion to Continue").

(2) Access. A document designated as "NONPUBLIC" in accordance with subdivision (B)(1) of this rule will be accessible only as provided in these Rules.

(3) Review. Upon motion, the court may consider any matter relating to submissions designated as "NONPUBLIC" in the EFS.

(C) Filing Sealed or Impounded or Nonpublic Documents. Sealed or impounded or nonpublic documents must be filed and handled in compliance with Rule 12. The filer must include in the "Comments to Court" field the designation "NONPUBLIC".

(D) Motion to Seal or Impound. Motions to seal or impound documents must be made in compliance with Rule 6 or Rule 10.

RULE 39. FILING FEES

(A) Filing Fees. A filer must pay the correct filing fee by any electronic payment method acceptable to the court before the case will be allowed to proceed, subject to the following exceptions:

(1) The filer is exempt by law;

(2) The fee is waived in accordance with subdivision (B) of this rule; or

(3) The filer pays the required fee by cash or check to the court clerk within seven days after the date of the electronic submission. If the court clerk receives payment within those seven days, the file date will relate back to the date of the electronic submission.

(i) If the filing is a case initiating document and the court clerk does not receive the payment of the required fee within seven days, the case shall be dismissed without prejudice.

(ii) If the filing is other than a case initiating document and the court clerk does not receive the payment of the required fee within seven days, the court clerk shall reject the filing.

(B) Waiver of Filing Fees. Upon application to the court in accordance with M.R. Civ. P. 91, a filer may request a waiver of any filing fees contemplated by these rules.

(1) Application granted. If the application for fee waiver is granted, the file date relates back to the date of submission of the filing and application.

(2) Application denied. If the application for fee waiver is denied, the filer will have seven days from the date of denial to pay the fee. If such payment is made, the file date will relate back to the date of submission of the filing and application. If not, the court clerk shall dismiss the case or reject the filing pursuant to subdivision (A) of this rule.

Advisory Note

When an application for a fee waiver is granted, the file date is determined pursuant to Rule 35(B).

RULE 40. SANCTIONS

(A) Failure to comply with these rules may be grounds for a finding of contempt of court and imposition of sanctions.

(B) As officers of the court, attorneys are required to abide by these rules or be subject to professional discipline for any violations.

Advisory Note

Contempt of court refers to a finding in accordance with M.R. Civ. P. 66.

Dated: August 21, 2020

FOR THE COURT,*

/s/
ANDREW M. MEAD
Acting Chief Justice

ELLEN A. GORMAN
JOSEPH M. JABAR
THOMAS E. HUMPHREY
ANDREW M. HORTON
CATHERINE R. CONNORS
Associate Justices

* This Rule Adoption Order was approved after conference of the Court, all Justices concurring therein.

Opinion #196 can be found online at the Board of Overseers of the Bar's website at: https://www.mebaroverseers.org/attorney_services/opinion.html?id=63337

Opinion #196: Transmission, Retrieval and Use of Metadata Embedded in Documents

Issued by the Professional Ethics Commission

Date Issued: October 21, 2008

Question

Bar Counsel has asked for the Commission's opinion concerning the application of the Bar Rules to the ethical duties of lawyers involving the transmission, retrieval and use of metadata embedded in documents which may reveal client confidences or other legally privileged information ("confidential information"). The issue gives rise to two questions: first, whether it is ethical for an attorney receiving electronic documents (the "receiving attorney") to make efforts to uncover embedded metadata that contains confidential information not intended to be communicated by the attorney transmitting the document (the "sending attorney"); and second, whether the sending attorney has an ethical duty to take reasonable measures to remove metadata containing confidential information before document transmission. Applying the principles of Bar Rules 3.2(f)(3) and (4),[1] 3.6(h)(1) and (2),[2] and 3.6(a),[3] the Law Court's reasoning in Corey v. Norman, Hanson & DeTroy,[4] this Commission's Opinions 172 (2000), 194 (2007) and 195 (2008), as well as opinions from other states following the lead of New York, we draw the following conclusions:

1. Without authorization from a court,[5] it is ethically impermissible for an attorney to seek to uncover metadata, embedded in an electronic document received from counsel for another party, in an effort to detect confidential information that should be reasonably known not to have been intentionally communicated.
2. A sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information.

Discussion

Lawyers today routinely make use of electronic document transmission, including in communications to opposing counsel. Such documents often contain metadata, which is peripheral information electronically embedded within the document but often not seen by and sometimes not even known to those who produce or read it. [6] Much metadata is mundane and legally inconsequential, lodged within the document by the software and identifying the date and time that the document was produced and the version of the software utilized. Some of this data may be accessed with as little effort as resting the cursor upon, or right clicking, the document icon. However, purposeful efforts to 'mine' metadata in a document may allow a receiving attorney to glean information that was clearly never intended to be communicated by the sending

attorney. The revelation of such metadata could result in the disclosure of client confidences, litigation and negotiation strategy, legal theories, attorney work product and other legally privileged and confidential information. Due to the rapid advance and general opaqueness of some computer technology, it may not be reasonably possible for an attorney to know all the types of metadata that might be embedded in a document or the extent to which such data may be subject to being probed by someone using extraordinary but technologically available methods.

A number of other jurisdictions have considered these questions. While there are inconsistent approaches taken regarding the ethical duties of receiving attorneys in probing documents for metadata containing confidential information, there is greater harmony among the jurisdictions with respect to the duties of sending attorneys to take reasonable measures to minimize the prospect that such data will be inadvertently transmitted. In this Opinion, the Commission adopts a balanced view, articulating reasonable ethical duties on both the receiving and sending attorneys.

Duties of Receiving Attorneys in Probing Documents for Metadata Containing Confidential Information

In the first major bar ethics opinion on the subject, relying principally upon a lawyer's ethical duty to refrain from dishonest, fraudulent, or deceitful conduct, New York determined that "Lawyers may not ethically use available technology to surreptitiously examine and trace email and other electronic documents." NY Bar Ethics Op. 749 (2001). Citing a 1992 ABA opinion, New York concluded that "the strong policy in favor of confidentiality outweighs what might be seen as the competing principles of zealous representation…." "No such balance need be struck here because it is a deliberate act by the receiving lawyer, not carelessness on the part of the sending lawyer, that would lead to the disclosure of client confidences and secrets."

Three years later, in an opinion discussed below focused on the duties of sending attorneys, New York renewed its ethical admonition to receiving attorneys: "Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets." NY Bar Ethics Op. 782 (2004).

Generally following New York's lead, Florida concluded that "A lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. A lawyer who inadvertently receives information via metadata in an electronic document should notify the sender of the information's receipt." "It is the recipient lawyer's concomitant obligation, upon receiving an electronic communication or document from another lawyer, not to try to obtain from metadata information relating to the representation of the sender's client that the recipient knows or should know is not intended for the recipient." FL Bar Ethics Op. 06-02 (2006).

Emphasizing "the strong public policy in favor of preserving confidentiality as the foundation of the lawyer-client relationship," Alabama followed the New York analysis in finding that "the receiving lawyer also has an ethical obligation to refrain from mining an electronic document." "The disclosure of metadata contained in an electronic submission to an opposing party could lead to the disclosure of client confidences and secrets, litigation strategy, editorial comments,

legal issues raised by the client, and other confidential information." AL Bar Ethics Op. 2007-02 (2007).

In contrast to the New York rule, some jurisdictions have adopted a view that more or less liberates receiving attorneys from ethical considerations in probing metadata in electronic documents, thereby placing upon the sending attorney the entire burden of cleansing the document of any possible, embedded client confidences or other privileged information. This view is based upon the fact that no bar rule specifically addresses the issue, together with the difficulty in prescribing permissible conduct in the context of rapidly changing technology.

Thus, recognizing that "metadata is ubiquitous in electronic documents" and that its model rules "do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents," the ABA opinion placed the sole ethical obligation on the sending attorney: "A lawyer who is concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata, or who wishes to take some action to reduce or remove the potentially harmful consequences of its dissemination, may be able to limit the likelihood of its transmission by 'scrubbing' metadata from documents or by sending a different version of the document without the embedded information." ABA Ethics Op. 06-442 (2006).

Following the ABA view, Maryland concluded that "there is no ethical violation if the recipient attorney… reviews or makes use of metadata without first ascertaining whether the sender intended to [send it]." MD Bar Ethics Op. 2007-09 (2007). Likewise, Colorado rejected New York's and adopted a variation of the ABA's view, emphasizing the responsibilities of the sending lawyer "to guard against the disclosure of metadata containing Confidential Information" and "to ensure that he or she is reasonably informed about the types of metadata that may be included in an electronic document or file and steps that can be taken to remove metadata if necessary." [7] Generally absolving the receiving attorney of ethical responsibilities in probing metadata embedded in the document ("[T]here is nothing inherently deceitful or surreptitious about searching for metadata"), Colorado reasoned that the lawyer "who receives electronic documents or files generally may search for and review metadata." However, Colorado went on to create a complex and perhaps impractical set of requirements for the parties to such communications: "If a Receiving Lawyer knows or reasonably should know that the metadata contain … Confidential Information, the Receiving Lawyer should assume that the Confidential Information was transmitted inadvertently unless the Receiving Lawyer knows that confidentiality has been waived. The Receiving Lawyer must promptly notify the Sending Lawyer," in which case "the lawyers may, as a matter of professionalism, discuss whether a waiver of privilege or confidentiality has occurred." If, however, before examining the metadata, "the Receiving Lawyer receives notice from the sender that Confidential Information was inadvertently included, the Receiving Lawyer must not examine the metadata and must abide by the sender's instructions regarding the disposition of the metadata." CO Bar Ethics Op. 119 (2008).

Two other jurisdictions have adopted variations on the New York and ABA views. Acknowledging that there is no specific rule determining the ethical obligations of attorneys in this particular context, Pennsylvania arrived at what seems a default. "[E]ach attorney must…

'resolve [the issue] through the exercise of sensitive and moral judgment guided by the basic principles of the Rules' and determine for himself or herself whether to utilize the metadata contained in documents and other electronic files based upon the lawyer's judgment and the particular factual situation." "The utilization of metadata by attorneys receiving electronic documents from an adverse party is an emerging problem. Although a transmitting attorney has tools at his or her disposal that can minimize the amount of metadata contained in a document he or she is transmitting, those tools still may not remove all metadata." PA Bar Ethics Op. 2007-500 (2007).The District of Columbia has articulated yet another approach: "A receiving lawyer is prohibited from reviewing metadata sent by an adversary only where he has actual knowledge that the metadata was inadvertently sent." (emphasis added). "[W]e believe that mere uncertainty by the receiving lawyer as to the inadvertence of the sender does not trigger an ethical obligation by the receiving lawyer to refrain from reviewing the metadata…. Where there is such actual prior knowledge…, the receiving lawyer's ethical duty of honesty requires that he refrain from reviewing the metadata until he has consulted with the sending lawyer to determine whether the metadata includes privileged or confidential information." DC Bar Ethics Op. 341 (2007).

Having considered all of the approaches extant, this Commission believes that the better view is that generally expressed by New York and the jurisdictions that have followed it. While the Commission recognizes, as is the case in those jurisdictions, that no Bar Rule specifically addresses this particular situation, and the Commission is appropriately cautious in its specific application of the general proscription in Bar Rule 3.2(f)(3) and (4) on attorneys engaging in conduct involving dishonesty or prejudicial to the administration of justice, an attorney who purposefully seeks to unearth confidential information embedded in metadata attached to a document provided by counsel for another party, when the attorney knows or should know that the information involved was not intended to be disclosed, has acted outside of these broad ethical requirements. While the Commission has considered the contrary view held by the ABA and the states that have followed it, the Commission believes that Bar Rule 3.2(f)(3) and (4) would have little (and we believe quite inadequate) meaning if it were not applied in this situation. Not only is the attorney's conduct dishonest in purposefully seeking by this method to uncover confidential information of another party, that conduct strikes at the foundational principles that protect attorney-client confidences, and in doing so it clearly prejudices the administration of justice.

The Law Court's decision in Corey, while not directly addressing the Bar Rules, and the Commission's adoption of Corey in Opinion 172 (reversing Opinion 146), offer additional support for this conclusion. There, the issue was whether an attorney might retain and make use of confidential information that had been inadvertently disclosed to him by opposing counsel, the Law Court determining that he could not, based upon the shared responsibility to protect the attorney-client privilege. [8] In Opinion 172, this Commission determined that it would be a violation of the Bar Rules, in direct contravention of the holding in Corey and therefore prejudicial to the administration of justice, for an attorney to retain and make use of such information. If anything, the issue before us now is more straightforward. Unlike in Corey, here the receiving attorney is making purposeful efforts to probe for information he or she knows or should know to be confidential and not to have been knowingly communicated by opposing counsel. That such conduct is dishonest and designed to prejudice the administration of justice seems beyond dispute.

In sum, following the general analysis of New York and the other states that have adopted its view, and based upon Bar Rule 3.2(f)(3) and (4) and Corey, we find that an attorney may not ethically take steps to uncover metadata, embedded in an electronic document sent by counsel for another party, in an effort to detect information that is legally confidential and is or should be reasonably known not to have been intentionally communicated.[9]

Ethical Duties of Sending Attorneys in Taking Measures to Avoid Transmission of Metadata Containing Confidential Information

While the jurisdictions opining to date have arrived at inconsistent views in dealing with the ethical duties of document-receiving attorneys, there has been relative unanimity in dealing with those of sending attorneys. Therefore, we have no difficulty in following the consensus approach on the subject.

New York determined that sending attorneys have a duty to take reasonable measures to guard against improper disclosure of confidential information contained in metadata in documents transmitted to other parties. This conclusion was based on the rule "that a lawyer shall not 'knowingly' reveal a confidence or secret of a client." "When a lawyer sends a document by email, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information." NY Bar Ethics Op. 782 (2004).

Following New York's lead, Florida concluded that "A lawyer who is sending an electronic document should take care to ensure the confidentiality of all information contained in the document, including metadata." "It is the sending lawyer's obligation to take reasonable steps to safeguard the confidentiality of all communications sent by electronic means… and to protect from other lawyers and third parties all confidential information, including information contained in metadata." "The foregoing obligations may necessitate a lawyer's continuing training and education in the use of technology in transmitting and receiving electronic documents in order to protect client information." FL Bar Ethics Op. 06-02 (2006).

Alabama, Maryland, Colorado and Pennsylvania have all followed suit. AL Bar Ethics Op. 2007-02 (2007); MD Bar Ethics Op. 2007-09 (2007); CO Bar Ethics Op. 119 (2008); PA Bar Ethics Op. 2007-500 (2007). However, those jurisdictions following the ABA analysis (described above), in finding few or no ethical duties of the receiving attorney to refrain from probing document metadata, have placed a correspondingly heavier burden on the sending attorney to take measures to avoid the transmission of metadata containing confidential information. "The ultimate responsibility for control of metadata rests with the Sending Lawyer," who "may not limit the duty to exercise reasonable care in preventing the transmission of metadata that contain Confidential Information by remaining ignorant of technology relating to metadata or failing to obtain competent computer support." CO Bar Ethics Op. 119 (2008). Going further, the Colorado opinion suggests that attorneys should access resources exceeding those normally expected of lawyers by retaining computer experts who understand the reach of metadata and methods to avoid transmission of confidential information embedded therein.

While we stop short of embracing the full force of Colorado's advice, we agree with the other jurisdictions that attorneys are ethically required to take reasonable measures to avoid the communication of confidential information, regardless of the mode of transmission. This duty logically extends to metadata that the attorney should reasonably know may lie within an electronic document. If an attorney is in doubt, many documents can be readily converted to generic files (such as PDF) which retain little of the metadata contained in word processing documents, and of course resort can be made to paper copies where issues of metadata confidentiality are significant. Although we do not believe that an attorney's ethical duties dictate, in routine work, the retention of a computer expert for these purposes, we also do not believe it reasonable for an attorney today to be ignorant of the standard features and capabilities of word processing and other software used by that attorney, including their reasonably known capacity for transmitting certain types of data that may be confidential.

This Opinion is consistent with others the Commission has recently issued dealing with confidentiality of information in the computer era. In Opinion 195 (2008), the Commission concluded that, as a general matter and subject to appropriate safeguards, an attorney may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain client confidentiality. The issue invoked the prohibition on knowing disclosure of confidential client information under Bar Rule 3.6(h)(1) as well as the general standard requiring lawyers to "employ reasonable care and skill and apply the lawyer's best judgment in the performance of professional services" under Bar Rule 3.6(a). While we found that it is reasonable for attorneys transacting routine business through unencrypted email, some circumstances might require a more secure method of communication.

Likewise, in Opinion 194 (2007), the Commission concluded that, with appropriate safeguards, an attorney may utilize transcription and computer server backup services remote from both the lawyer's physical office and the lawyer's direct control or supervision, without violating the attorney's ethical obligation to maintain client confidentiality. The Opinion cautioned, however, that the lawyer utilizing such services has a duty to take practical measures to assure that the services are reasonably secure and appropriate for the intended purpose. [10] As here, the issue is not amenable to an unqualified answer but requires the application of a standard of reasonableness, weighing all the factors of which the lawyer should be aware.[11]

On the issue before us, we conclude that, in applying Bar Rules 3.6(h)(1) and (2) in combination with 3.6(a), the sending attorney has an ethical duty to use reasonable care when transmitting an electronic document to prevent the disclosure of metadata containing confidential information. Undertaking this duty requires the attorney to reasonably apply a basic understanding of the existence of metadata embedded in electronic documents, the features of the software used by the attorney to generate the document and practical measures that may be taken to purge documents of sensitive metadata where appropriate to prevent the disclosure of confidential information.

Footnotes

[1] Rule 3.2(f) sets forth an attorney's ethical obligations in broad terms: "A lawyer shall not:… (3) engage in conduct involving dishonesty, fraud, deceit, or misrepresentation; (4) engage in conduct that is prejudicial to the administration of justice."

[2] Rule 3.6(h)(1) sets forth an attorney's ethical obligations to maintain client confidentiality:

Except as permitted by these rules, or when authorized in order to carry out the representation, or as required by law or by order of the court, a lawyer shall not, without informed consent, knowingly, disclose or use information (except information generally known) that:

i. Is protected by the attorney-client privilege in any jurisdiction relevant to the representation;
ii. Is information gained in the course of representation of a client or former client for which that client or former client has requested confidential treatment;
iii. Is information gained in the course of representation of the client or former client and the disclosure of which would be detrimental to a material interest of the client or former client; or
iv. Is information received from a prospective client, the disclosure of which would be detrimental to a material interest of that prospective client, when the information is provided under circumstances in which the prospective client has a reasonable expectation that the information will not be disclosed.

Rule 3.6(h)(2) addresses an attorney's ethical obligation to ensure that others working on the attorney's behalf in the course of representation who are privy to confidential client information likewise maintain the client's confidences: "A lawyer shall exercise reasonable care to prevent lawyers and non-lawyers employed or retained by or associated with the lawyer from improperly disclosing or using information protected by paragraph (1) of this subdivision."

[3] Rule 3.6(a) sets forth a general standard requiring lawyers to "employ reasonable care and skill and apply the lawyer's best judgment in the performance of professional services."

[4] 199 ME 196

[5] This Opinion is not intended to deal with the extent to which relevant information may be sought in litigation through proper discovery under the guidance of a court.

[6] Although the type of metadata embedded in an electronic document varies with the software being used. and its full scope is unknown except to those with advanced computer expertise, examples include recording of the document's source, authors, editors and those offering comments, as well as changes and comments made in the course of document preparation. Some metadata may reveal client confidences and attorney work product and advice, among other confidential information.

[7] While metadata may be "ubiquitous" (to use the words of the ABA), we think that, with rapid technological advances, it may be overly simple to assume that an attorney may reasonably be able to know its full extent in all the software applications used, or that easily applied steps will

cleanse the document of all embedded information not intended to be revealed. While reasonable steps can and should be taken to minimize the amount of metadata contained in an electronic document to be transmitted to another party, and of course the document can be transmitted in paper copy if security is paramount, there is no absolute assurance that electronic transmission of documents can be undertaken in a manner that is totally immune from unwanted probing for confidential information.

[8] "In Corey, the Law Court, jurisdictionally unconstrained, has now pronounced that, as a matter of common law, the obligation to preserve the lawyer-client privilege is indeed an affirmative obligation shared by adversaries, and that the privilege cannot be inadvertently relinquished." Opinion 172.

[9] See footnote 5.

[10] As stated in Opinion 194, "[T]he primary responsibility for file integrity, maintenance, disposition, and confidentiality rests with the attorney employed by the client. See Maine Professional Ethics Commission Opinion # 74 (10/1/86)…. Rule 3.6(h)(2) implies that lawyers have a responsibility to train, monitor, and discipline their non-lawyer staff in such a manner as to guard effectively against breaches of confidentiality. Failure to take reasonable steps to provide adequate training, to monitor performance, and to apply discipline for the purpose of enforcing adherence to ethical standards is grounds for concluding that the lawyer has violated Rule 3.6(h)(2). See Maine Professional Ethics Commission Opinion #134 (9/21/93)."

[11] "With the pervasive and changing use of evolving technology in communication and other aspects of legal practice, particular safeguards which might constitute reasonable efforts in a specific context today may be outdated in a different context tomorrow. Therefore, rather than attempting to delineate acceptable and unacceptable practices, this opinion will outline guidance for the lawyer to consider in determining when professional obligations are satisfied." Opinion 194.