

Emily Bienek
121 Blackstrap Rd
Falmouth, Maine 04105
emily.bienek@maine.edu

March 26, 2019

Via email: lawcourt.clerk@courts.maine.gov

Honorable Justices of the Supreme Judicial Court
Matthew Pollack, Clerk
Maine Supreme Judicial Court
205 Newbury Street, Room 139
Portland, Maine 04101-0368

RE: Comments Regarding Drafts of the Maine Digital Court Records Access Rules

Dear Chief Justice Saufley, Senior Associate Justice Alexander, and Associate Justices Mead, Gorman, Jabar, Hjelm, and Humphrey:

Thank you for the opportunity to submit comments on the Maine Digital Court Records Access Rules. I write to you in my personal capacity and not on behalf of the University of Maine School of Law, where I am a current second year law student.

It is clear that much work and thought has gone into this transition on the part of the Court, and also on the part of the bar and the numerous interested parties. The Court must strike a difficult balance between access, privacy, and transparency. Many other states have gone before, and Maine is certainly capable of constructing a superior system that works for our legal community, the public, and the high number of unrepresented litigants in our state.

The issue I bring to your attention today is formed in part based on my own thoughts, but also on observation of the Rules Committee meetings on March 6th and the comments given by the public members. Overall, making informed, concise, and effective comments as to the Maine Digital Court Records Access Rules and any of the accompanying amendments to other rules requires an understanding of the underlying system and how it will work from both ends, the submission of information and the access to already submitted information. Without this understanding of the underlying system, comments and decisions are shots in the dark with a great potential to be over-broad, under-broad, or to miss the intended point entirely. I urge the Court to push pause on the formation of the Digital Court Records Access Rules until the Court and those involved in building Odyssey can properly inform, demonstrate, and explain the system to the interested parties.

To illustrate, there is a lot of concern about access to information and fees associated with access. It is my understanding that the court does not want to charge any fees. It is also my

understanding that submitted PDF's need to be searchable to comply with the ADA. Based on my Rules Committee observations, the Court and Committee members are not quite clear on the extent of this searchability and how that impacts access overall. Access to information comprises multiple, distinct types: 1) access by a party to their own documents, 2) ease of access and searchability within those documents, 3) access by the public within Odyssey, and 4) access by the public via the internet and search engines such as Google or Bing. This access is critical to privacy concerns and should not be viewed not as a continuum without definiteness, but as distinct, compartmentalized issues to be addressed separately. Searchability of PDF's and compliance with the ADA under the second type should not inform decisions made as to any of the other types of access. Each type of accessibility is dictated by the structure of Odyssey, and, therefore, will independently inform the formulation of distinct rules.

This is a prime example of how a lack of understanding of the underlying system leads to an inability to make a properly informed comment or decision, because without knowing how access works with regard to any of the types, no decision about the imposition of fees can be informed. For instance, as to the fourth type and internet searchability, PACER indexes the information in its system and in its PDFs on search engines (meaning, if you go to Google and type in the name of a person who has been involved in a bankruptcy case, the search results will lead you directly to their Federal court documents via PACER; this indexing of information is built into the system at its creation). To balance this very broad level of access and searchability, PACER charges fees because fees may deter some unscrupulous information seekers and it allows PACER to know who is seeking what information. On the other hand, you cannot go to Google to search the name of a person involved in legal issues in Massachusetts, because Massachusetts does not index its information on search engines the same way that PACER does. Massachusetts only allows access from within its portal and, even then, the searcher needs to know three specific types of information to gain access. In an instance like this, fees are not necessary as a check on the potentially unsavory use of information.

The stark differences in accessibility and searchability of these systems can lead one to vastly different conclusions as to whether or not fees should be imposed. Currently, without knowing which system Maine's Odyssey will look like, we cannot make decisions or comments to the best of our ability. This is only one illustration where big issues in rule-making could be solved with more information about the system; there are many others. For this very reason, because there is so much confusion, because there are still so many unanswered questions, and because various members of the public have expressed a passionate desire to know more about Odyssey before moving forward, I urge the Court to pause the rule-making and to 1) inform the public in an in-depth way as to how Odyssey will work, 2) to allow official comment as to changes in the Odyssey system itself, and 3) to provide another comment period as to the rules.

Respectfully submitted,



Emily Bienek,
Law Student

AARON M. FREY
ATTORNEY GENERAL

TEL: (207) 626-8800
TTY USERS CALL MAINE RELAY 711



STATE OF MAINE
OFFICE OF THE ATTORNEY GENERAL
6 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES:
84 HARLOW ST., 2ND FLOOR
BANGOR, MAINE 04401
TEL: (207) 941-3070
FAX: (207) 941-3075

415 CONGRESS ST., STE. 301
Portland, Maine 04101
TEL: (207) 822-0260
FAX: (207) 822-0259

14 ACCESS HIGHWAY., STE 1
CARIBOU, MAINE 04736
TEL: (207) 496-3792
FAX: (207) 496-3291

March 26, 2019

Matthew E. Pollack
Clerk of the Law Court
205 Newbury Street, Room 139
Portland, ME 04101-4125

RE: Proposed Digital Court Records Access Rules

Dear Matt:

I am responding on behalf of the Advisory Committee on Rules of Criminal Procedure to the Court's Notice of Opportunity for Comment on the proposed Digital Court Records Access Rules. I am attaching, in PDF format, both the Committee's comments and a "track changes" version of the proposed Access Rules.

Very truly yours,

/s/ Laura A. Yustak

Laura A. Yustak
Assistant Attorney General
Chair, Advisory Committee on Rules of
Unified Criminal Procedure

LY/tlc
Enclosures

Comments of the Advisory Committee on Rules of Unified Criminal Procedure to Proposed Amendments to the Maine Rules of Unified Criminal Procedure and Proposed Digital Court Records Access Rules

The Advisory Committee on the Maine Rules of Unified Criminal Procedure met on March 6, 2019 to discuss the Supreme Judicial Court's proposed amendments to the Maine Rules of Unified Criminal Procedure and the Supreme Judicial Court's proposed Digital Court Records Access Rules. The following comments are submitted on behalf of the Committee.

Specific revisions to the language of the proposed rules are made in the body of each set of proposed rules and are being submitted separately for each set of rules, along with a copy of these comments.

In general, the Committee agrees that providing the public with remote electronic access to documents associated with publicly conducted judicial proceedings will help to ensure transparency and protect the public's right of access to the courts. Where the Committee has expressed concerns, the basis lies primarily in the logistics of and resources necessary for redaction; the timing of disclosures of specific facts associated with unresolved charges that may affect trial rights of defendants and the State; and the personal nature of the circumstances and identifying information of victims and witnesses caught up in the criminal justice system. The second and third interests are recognized and protected by the Intelligence and Investigative Record Information Act, 16 M.R.S., Chapter 9.

Maine Rules of Unified Criminal Procedure

Rule 24(g) Juror Information Confidentiality

The Committee has no substantive comments regarding the proposed amended to Rule 24(g), and agrees with the proposed draft.

The Committee noted that proposed Rule 24(g) refers to Title 14, Court Procedure—Civil, Chapter 305: Juries. Although several provisions within Chapter 305 refer to grand and traverse jurors or juries, the Committee raised the question as to whether Title 14, Chapter 305 should be amended, perhaps with a general provision at the beginning of the chapter to indicate its applicability to criminal proceedings where the context requires, or whether a

cross-reference should be added to Title 15, Court Procedure—Criminal, Chapter 203: Juries, to reference applicable provisions within Title 14.

Rule 32(c)(3) Access to Written Presentence Report and Right to Comment

The Committee has no substantive comments regarding the proposed amendment to Rule 32, and agrees with the proposed draft.

The following comments address the interplay between the proposed amendments to M.R.U.Crim. P. 4 and 41 and the proposed DCRA Rules.

Rule 4(b) Grounds for Issuance of Arrest Warrant or Summons Rule 41(f) Issuing a Search Warrant

The Committee's understanding is that together, these rules reaffirm that warrants and affidavits will not be publicly available if impounded. The default accessibility rule would be that the arrest warrant and affidavit (and possibly the probable cause affidavit, see M.R.U.Crim. P. 4A), would be public once the warrant has been executed (or at initial appearance), unless a further impoundment is ordered, and that a search warrant and supporting materials would be public once a return is filed. With respect to both arrest and search warrants, a recalled warrant results in the materials being treated as confidential. The Committee understands that a document that is "public" will be available via remote electronic ("online") access.

Because supporting materials such as affidavits are public under current rules, unless impounded, and are often made available by mainstream media in high-profile cases, the proposed rules simply expand access to records that are already public. However, the Committee expressed concerns about the breadth and immediacy of remote electronic access to supporting materials even if those materials are redacted to protect the information identified in proposed DCRA Rule 5. There was no consensus amongst the Committee members as to precisely how to resolve the concerns expressed by its members associated with increased breadth and immediacy of access, but all wished to relay them to the Court. Those concerns and possible options for addressing them follow.

General concerns identified by the Committee include the following:

1. Detailed factual allegations will be available online concerning as-yet uncharged suspects.
2. Supporting affidavits regularly include full names of suspects, witnesses and victims. Under the proposed DCRA rules, names of victims and witnesses would be available online, except for full names of minors. Committee members had concerns about negative consequences associated with widespread publication of such information, including bullying or shaming of victims and witnesses identified in affidavits and supporting materials.
3. Dates of birth of victims and witnesses are found throughout affidavits in support of warrant requests and probable cause affidavits. Concerns mentioned by the Committee include identity theft. There was no consensus regarding whether there should be a bright line rule requiring redaction of month and date of birth.
4. Names and dates of birth of juveniles charged in proceedings open pursuant to the Juvenile Code would be available online. Proposed DCRA Rule 5(a); 15 M.R.S. §§ 3307-08. Although the consensus was not absolute, generally, the Committee did not support the identity of juveniles charged with juvenile crimes being available via remote electronic access. The potential for negative effects of widespread publicity and bullying or shaming of juveniles runs counter to the philosophy underlying Maine's Juvenile Code to rehabilitate and educate juveniles within the juvenile justice system.
5. Online access to pleadings in a case that is subsequently resolved by means of a disposition classified as confidential criminal history record information (e.g., acquittal; dismissal that is not part of a plea agreement) sets up potential inconsistencies between the events preceding final disposition and the final disposition itself (e.g., an indictment may remain public after an acquittal, which becomes confidential). There was some discussion on this point: The State Bureau of Identification understands and has historically implemented the Criminal History Record Information Act (CHRIA), 16 M.R.S., Chapter 7, to make criminal history underlying and associated with

confidential final dispositions similarly confidential, and thus does not disseminate, in response to requests from the public, the fact of charges associated with confidential final dispositions. Clarifying legislation may be required to ensure that the Court and the SBI are consistent in their implementation of the CHRIA.

6. How will documents submitted to the court be reviewed for compliance with proposed Rule 5?
7. What is the process envisioned under proposed DCRA Rule 9? Should redacted (public) documents be submitted alongside complete documents that are submitted under seal for the court's review? In the alternative, should the complete, unredacted document be submitted to the court accompanied by a motion to seal or protect, with a request for an order giving the party sufficient time to redact appropriate portions of the document in the event that it becomes public?
8. Redaction of affidavits and supporting materials will require substantial resources from prosecution and law enforcement.
9. Motions to impound may become the norm, demanding increased resources from the Court and the parties. This concern militates in favor of a bright-line rule regarding access.

Proposals to address specific concerns:

1. With respect to juvenile proceedings, the Committee recognizes that there are legislative proposals pending that may revise public access to these proceedings. One possible approach to online access to juvenile proceedings may be to make access available at the courthouse but not online, consistent with the Court's proposal for PFA proceedings, until a date certain, to give the Legislature opportunity to act in this area and with an understanding of the increased public access to juvenile proceedings that will result from the Court's digital records system, which was not the practice at the time of the enactment of the current provisions regarding access to records of juvenile court proceedings.

2. Proposals for online access to arrest warrant (M.R.U.Crim. P. 4) and probable cause affidavits (M.R.U.Crim P. 4A) included the following:
 - a. Make the documents available online immediately upon execution or at initial appearance, consistent with the Court's proposal, and redacted to protect the information designated in proposed DCRA Rule 5.
 - b. Provide parties with a time-limited opportunity to request further sealing or redaction at the time the document would otherwise become public. The Committee suggests that whenever unredacted documents are filed with the court under seal and subsequently become publicly accessible, the Court would have the discretion to give parties a period of time to redact the documents in order to comply with proposed DCRA Rule 5.
 - c. Delay online access until a designated period of time after a triggering event. There was no consensus as to whether the triggering event should be the filing of the complaint or indictment, or final disposition of the charge, and what the time period should be.

3. Proposals for online access to search warrant materials (M.R.U.Crim. P. 41) were similar to the approach outlined for arrest and probable cause affidavits.
 - a. Make the documents available online immediately upon return of the warrant materials, consistent with the Court's proposal, and redacted to protect the information designated in proposed DCRA Rule 5.
 - b. Provide parties with a time-limited opportunity to request further sealing or redaction at the time the document would otherwise become public. The Committee suggests that whenever unredacted documents are filed with the court under seal, the Court would have the discretion to give parties a period of time to redact the documents in order to comply with proposed DCRA Rule 5.

- c. Delay online access until a designated period of time after a triggering event. The triggering event might be the filing of the return, the filing of a charge, or resolution of a charge.
4. One proposal would distinguish pleadings from supporting materials such as affidavits so as to extend online access to criminal and juvenile pleadings (with appropriate redactions under DCRA Rule 5) but retain the current approach of making supporting affidavits available at the courthouse—again, similar to the approach the Court proposes for PFA records.

Respectfully submitted,

Laura Yustak, Chair, on behalf of
Advisory Committee on Maine Rules of Unified Criminal Procedure

1 STATE OF MAINE
2 SUPREME JUDICIAL COURT
3 **PROPOSED**
4 MAINE DIGITAL COURT RECORDS ACCESS RULES
5

6 **PREAMBLE**
7

8 These rules implement the recommendations of the privacy workgroup
9 regarding public access to court records created or maintained by the Maine
10 Judicial Branch. Given the extent and breadth of information contained in court
11 records and the growing understanding of the dangers associated with online
12 aggregation and/or dissemination of personal information, it is fundamentally
13 necessary that the new format through which court records are available be
14 tailored to ensure that there is an appropriate balance between access and
15 privacy.

16 In weighing the competing interests associated with the public's right of
17 access to the courts, the legitimate expectations of privacy held by those who
18 choose or are required to come to court to resolve disputes and seek justice,
19 and the need for effective court administration, the following principles have
20 been adopted in these rules:

- 21 1. The public has a general right of access to court records in both civil
22 and criminal cases and proceedings, unless otherwise restricted by
23 federal or state law, court rule, or administrative order;
24
- 25 2. Public access to court records informs and educates the public about
26 the workings of the courts and acts as a mechanism for oversight and
27 accountability;
28
- 29 3. The protection of personal privacy is also critical, and the public right
30 of access to court records is not absolute. Certain private, personal
31 information contained in court records need not be made public in
32 order to promote the interests served by access to court records;
33
- 34 4. Therefore, access to court records, including remote electronic access,
35 should be encouraged and facilitated to the extent it is consistent with
36 the preservation of legitimate privacy interests and with state and
37 federal laws.

38 Pursuant to those principles, these rules provide for access to court records
39 in a manner that:

- 40 • provides maximum reasonable accessibility to court records,
- 41 • supports the role of the judiciary,
- 42 • promotes governmental accountability,
- 43 • contributes to public safety,
- 44 • minimizes the risk of harm to individuals,
- 45 • protects individual privacy rights and interests,
- 46 • makes effective use of limited court resources,
- 47 • protects proprietary business information,
- 48 • minimizes reluctance to use the court to resolve disputes,
- 49 • provides excellent customer service,
- 50 • does not unduly interfere with the function of the Judicial Branch to
- 51 administer justice to litigants,
- 52 • protects individuals from the use of outdated or inaccurate information,
- 53 and
- 54 • contributes to the body of knowledge of effective practices of courts.

55 *****

56
57
58 **RULE 1. PURPOSE AND APPLICABILITY**
59

60 The purpose of these rules is to provide a comprehensive framework for
61 public access to digital state court records maintained or created by the Maine
62 Judicial Branch. The rules apply to litigants and all other persons and entities
63 seeking access to digital state court records and to judicial officers and court
64 personnel responding to requests for access. These rules apply to all court
65 records and data that are accessible as digital records in the Maine Judicial
66 Branch's digital case management system. Except as otherwise explicitly stated
67 in these rules or by court order, remote access to digital state court records as
68 provided in these rules shall be co-extensive with access to such records at
69 courthouses. The county probate courts are not included in the scope of these
70 rules.
71

RULE 2. DEFINITIONS

As used in these rules, unless the context otherwise indicates, the following terms have the following meanings.

(a) “Accessible by the public” means that a court record may be inspected or copied by any member of the public. A fee may be required for the inspection or copying.

(b) “Aggregate data” means summary information extracted, assembled, or derived from compiled data. “Aggregate data” eliminates any case or party-identifying information such as case numbers, names, and addresses.

(c) “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.

(d) “Clerical errors” are errors or omissions appearing in a court record that are patently evident, and that occur as a result of court personnel’s action or inaction.

(e) “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.

(f) “Court Clerk” means a Manager, Clerk of Court, Deputy Clerk, Assistant Clerk, or Associate Clerk.

(g) “Court record”

(1) “Court record” means any file, document, information, or data received or maintained by a state court in digital form in connection with a particular case or proceeding, including, but not limited to:

(A) Pleadings, motions, briefs and their respective attachments, and evidentiary exhibits;

111 (B) Any order, judgment, opinion, or decree; and
112

113 (C) Any registry of actions, calendar, or other information
114 created or prepared by court clerks or staff that is related to
115 a case or proceeding.
116

117 (2) For purposes of these rules, “court record” does not include the
118 following materials, even if they exist in connection with a
119 particular case or proceeding:
120

121 (A) Unfiled discovery materials;
122

123 (B) Information gathered, maintained, or stored by a
124 governmental agency or other entity to which the court has
125 access but that is not part of the case record or file;
126

127 (C) Notes, memoranda, and drafts thereof, and any other
128 material prepared or collected by a judicial officer or other
129 court personnel at the direction of a judicial officer and used
130 in the process of a judicially assisted settlement conference,
131 in recording the jurist’s notes of a proceeding, or in the
132 preparation of a decision or order;
133

134 (D) Internal draft working documents prepared for or by a
135 judicial officer or other court personnel related to court
136 practices and procedures;
137

138 (E) The identity of any justice of the Supreme Judicial Court,
139 other than a justice sitting as a publicly designated single
140 justice in a particular matter, assigned to prepare a written
141 decision or opinion if the decision or opinion has not yet been
142 issued;
143

144 (F) The legal work product and other records of any attorney,
145 law clerk, or other person employed by or representing the
146 Judicial Branch that are produced in the regular course of
147 business or during representation of the Judicial Branch;
148

149 (G) Records of consultative, advisory, or deliberative
150 discussions pertaining to the rendering of decisions or the
151 management of cases; or
152

153 (H) Any other court records maintained by the Judicial
154 Branch not expressly defined as court records.
155

156 **(h) “Family matter proceedings”** include cases or proceedings for
157 divorce, annulment, or judicial separation; parental rights and responsibilities,
158 including but not limited to the establishment or enforcement of a child support
159 obligation; paternity or any type of parentage (including actions to enforce or
160 obtain remedies for noncompliance with a gestational carrier agreement¹);
161 grandparent visitation; or the adoption, guardianship, or emancipation of a
162 minor.
163

164 **(i) “Nonpublic case, document, information, or data”** means any case,
165 document, information, or data to which public access is restricted pursuant to
166 federal or state law, court rule, or administrative order.
167

168 **(j) “Public”**

169 (1) “Public” includes:

170 (A) Any person, business, or entity;
171

172 (B) A government agency or commission for which there is
173 no existing federal or state statute, court rule, or court order
174 defining that agency’s access to court records; and
175

176 (C) Media organizations.
177

178 (2) “Public” does not include:
179
180
181

¹ We intend to ask the Legislature to make nonpublic any case and proceeding involving the establishment of parentage by assisted reproduction (19-A M.R.S. §§ 1921–1929), noncompliance with a gestational carrier agreement (19-A M.R.S. §§ 1931–1939), and the emancipation of a minor (15 M.R.S. § 3506-A).

182 (A) Judicial Branch staff, including court employees,
183 Administrative Office of the Court employees, and judicial
184 officers;

185
186 (B) The parties to a specific case or proceeding, their lawyers,
187 or persons identified by the court as having access to the
188 court record in that case or proceeding;

189
190 (C) Private or governmental persons, vendors, or entities
191 that assist the Judicial Branch in performing its functions;

192
193 (D) Persons or governmental entities whose access to court
194 records is governed by another statute, court rule, or court
195 order, or by a policy set by the State Court Administrator; or

196
197 (E) Persons who are authorized by statute, court rule, or
198 administrative order to access court records.

199
200 **(k) “Registry of actions,”** formerly identified as “docket entries,” means
201 the list of case information maintained by the Court Clerk that contains the case
202 caption; docket number; a chronological entry identifying the date and title of
203 each complaint, motion, order, judgment, notice, or other document filed in a
204 case; and the dates of events in the case.

205
206 **(l) “Sealed or impounded case, document, or information”** means any
207 public case, document, or information that has been sealed or impounded from
208 public access by order of a court.

209
210 **RULE 3. GENERAL ACCESS POLICY**

211
212 **(a)** Court records as defined in these rules are open for public inspection
213 and copying except as otherwise provided by federal or state law, court rule,
214 court order, or administrative order.

215
216 **(b)** Restrictions on inspection or copying pursuant to these rules shall
217 not be applicable to named parties or attorneys of record in a specific case or
218 judicial proceeding, except for restrictions pursuant to Rule 7 of these rules, or
219 unless otherwise restricted or limited by statute, court rule, court order, or
220 administrative order.

221
222 (c) Unless otherwise ordered by the court, a digital court record
223 accessible to the public shall be available no later than three business days after
224 it is received, filed, or entered in the Registry of Actions by the court clerk.

225
226 **RULE 4. [RESERVED FOR RULE GOVERNING**
227 **ACCESS TO AGGREGATE, BULK, AND COMPILED DATA]**

228
229 *[Neither the effective date nor the final content of Rule 4 has been established.*
230 *The Judicial Branch will undertake a review of the operational capacity of the*
231 *Odyssey case management system and the resources of the Judicial Branch*
232 *eighteen months after the case management system has been fully operational at*
233 *all court locations before promulgating rules relating to dissemination of*
234 *aggregated, compiled, or bulk data.]*

235
236 **RULE 5. SPECIFIC INFORMATION EXCLUDED FROM PUBLIC ACCESS**

237
238 In all cases, the following information is not accessible by the public:

239
240 (a) Names and dates of birth of minors (first names and initials may be
241 public), except in juvenile actions to the extent that public access is permitted
242 by statute;

Commented [YL1]: Should complete dates of birth of adults, including victims and witnesses, be public?

243 (b) Any images of minors;

244
245 (c) Any images depicting nudity, ~~or~~ sexual acts, ~~or~~ sexual contact, or
246 corpses;

247
248 (d) Personally identifiable information, including, but not limited to:

249 (1) Home addresses;

Commented [YL2]: Addresses of defendants appear on charging documents. Should these be excluded from the rule, or also specifically identified as not accessible?

250 (2) Telephone numbers;

251 (3) Personal email addresses;

252 (4) Social Security and employer identification numbers;

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

263
264 (6) Driver's license numbers;

265
266 (7) Other personal identification numbers, such as passport
267 numbers and state identification numbers; and

268
269 (8) DNA-identifying data or information.

270
271 (e) Cases, documents, or information sealed by court order issued
272 pursuant to Rule 7 of these rules;

273
274 (f) All personal health information and medical records, including, but
275 not limited to, all mental health evaluations and records, forensic evaluations,
276 and substance use evaluations and treatment records;

277
278 (g) Psychological and intelligence test documents and results;

279
280 (h) School records, including scholastic achievement information and
281 data;

282
283 (i) HIV/AIDS testing information;

284
285 (j) Death certificates;

286
287 (k) Immigration documents;

288
289 (l) "Confidential criminal history record information," as defined by the
290 Maine Criminal History Records Information Act, Title 16, chapter 7;

291
292 (m) Information and documents relating to applications for
293 court-appointed counsel, including *in forma pauperis* affidavits;

294
295 (n) Documents involving a protection from abuse order or some other
296 protective order that would reveal the identity or location of a protected person
297 under the order;

Commented [YL3]: And Medical Examiner records
confidential pursuant to Title 22, Ch. 711? [Not discussed
by full Committee]

298
299 **(o)** Identifying information in a protection from harassment case, when
300 it is alleged that the health, safety, or liberty of a party or minor child would be
301 jeopardized by disclosure of the personally identifiable information;

302
303 **(p)** The names of jurors, their juror qualification forms, and any
304 personally identifiable juror information;

305
306 **(q)** Witness subpoenae that extend to privileged or protected
307 documents;

308
309 **(r)** Arrest warrants and associated affidavits to the extent such material
310 is not accessible to the public pursuant to Rule 4 of the Maine Rules of Unified
311 Criminal Procedure;

312
313 **(s)** Probable cause affidavits to the extent such material is not accessible
314 to the public pursuant to Rule 4A of the Maine Rules of Unified Criminal
315 Procedure;

316
317 **(ts)** Subpoenae *duces tecum* that extend to privileged or protected
318 documents;

319
320 **(ut)** Search warrants and associated affidavits to the extent such material
321 is not accessible to the public pursuant to the Maine Rules of Unified Criminal
322 Procedure, Rule 41; and,

323
324 **(vz)** Presentence reports, including attachments.

325
326 **RULE 6. COURT RECORDS IN SPECIFIC CASE TYPES AND PROCEEDINGS**
327 **EXCLUDED FROM PUBLIC ACCESS**

328
329 Some court records are not accessible to the public because federal or
330 state law, or court rule, or administrative order prohibits disclosure of the
331 information. Court records that are not accessible to the public include, but are
332 not limited to, court records in the following case types and proceedings:

333 **(a)** Adoption proceedings;

334 **(b)** Child protection proceedings;

- 337
- 338 **(c)** Mental health civil commitment proceedings;
- 339
- 340 **(d)** Juvenile proceedings, to the extent that the records are not open to
- 341 public inspection;
- 342
- 343 **(e)** Medical malpractice screening panel proceedings;
- 344
- 345 **(f)** Sterilization proceedings;
- 346
- 347 **(g)** Proceedings for a court-authorized abortion for a minor;
- 348
- 349 **(h)** Grand jury proceedings;
- 350
- 351 **(i)** Noncompliance with gestational carrier agreement proceedings
- 352 (legislation to be proposed this session);
- 353
- 354 **(j)** Emancipation of a minor proceedings (legislation to be proposed this
- 355 session);
- 356
- 357 **(k)** Protection from Abuse records, although otherwise publicly available
- 358 at a courthouse, will not be available on the internet;
- 359
- 360 **(l)** Appeals from the denial, suspension or revocation of concealed
- 361 handgun permits, unless such confidentiality is waived.

Commented [YL4]: 25 MRS 2006. Question: Should confidentiality be limited to the record or include the pleadings as well?

363 All other family matter proceedings except that, pursuant to Rule 10 of these
364 rules, in some family matter proceedings, the summary complaint, summary
365 answer, registry of actions, and summary of judgment will be accessible to the
366 public.

367
368 **RULE 7. IMPOUNDING OR SEALING PUBLIC CASES, DOCUMENTS, OR**
369 **INFORMATION FROM PUBLIC ACCESS**

370
371 **(a) Procedure for impounding or sealing.** Any party to a court case or
372 any person or entity that has standing to do so may file a motion to have a public
373 case, document, or information impounded or sealed from public access. Such
374 a motion must be accompanied by an affidavit stating the basis upon which the
375 movant has standing, and the reason for the request to seal or impound,

376 including a statement describing the harm that is alleged will occur should the
377 motion be denied. As soon as a motion to impound or seal is filed, the public
378 case, document, or information that is the subject of the motion shall be
379 impounded or sealed, pending the court's ruling on the motion.

380
381 In weighing a reasonable expectation of privacy against the public
382 interest in the transparency of court records, the court shall consider whether
383 an individual's personal safety, health, or well-being, or a substantial personal,
384 business, or reputational interest outweighs the public interest in the
385 information in the court records.

386
387 **(b) Handling of impounded or sealed cases, documents, or**
388 **information.** It is the responsibility of the filing party to ensure that any
389 impounded or sealed cases, documents, or information are submitted to the
390 court in accordance with Rule 9.

391
392
393 **RULE 8. OBTAINING ACCESS TO IMPOUNDED OR SEALED CASES,**
394 **DOCUMENTS, OR INFORMATION**

395
396 **(a)** A party to the case or proceeding or a member of the public, as defined
397 in Rule 2(j)(1), may request access to a public case, document, or information
398 impounded or sealed from public access by court order issued pursuant to Rule
399 7 of these rules by filing a motion in accordance with the Maine Rules of Civil
400 Procedure, the Maine Rules of Unified Criminal Procedure, the Maine Family
401 Division Rules of Procedure, or the Maine Rules of Appellate Procedure. A
402 nonparty seeking access to an impounded or sealed public case, document, or
403 information shall be considered a party in interest for the limited purposes of
404 the motion brought pursuant to this rule.

405
406 **(b)** When a court receives a motion for access to any public case,
407 document, or information that has been impounded or sealed from public
408 access by court order, it must:

409
410 (1) Provide notice of the motion for access to all affected persons
411 or parties; and

412
413 (2) Provide the moving party or party in interest and the affected
414 persons or parties an opportunity to be heard.

415
416 **(c)** The motion shall be granted upon a showing of good cause. In
417 determining whether good cause has been shown to grant the motion, the court
418 shall consider the public access and privacy interests served and whether the
419 moving party or party in interest has demonstrated that:

420
421 (1) Extraordinary circumstances exist that require the impounded
422 or sealed materials to be made available or

423
424 (2) The public interest in disclosure outweighs any potential harm
425 in disclosure.

426
427 **(d)** If the court allows access, it may impose any reasonable conditions to
428 protect the privacy interests at issue.

429
430 **(e)** A party or party in interest that seeks to appeal from a trial court
431 order granting or denying access to impounded or sealed cases, documents, or
432 information pursuant to this rule shall file an appeal of that order in accordance
433 with the Maine Rules of Appellate Procedure. While that appeal is pending,
434 there shall be no stay of the underlying action unless the appealing party has
435 sought and obtained a stay from the trial court.

436
437 **RULE 9. IDENTIFICATION AND HANDLING OF SEALED, IMPOUNDED, OR**
438 **NONPUBLIC CASES, DOCUMENTS, INFORMATION, AND DATA**

439
440 It is the responsibility of the filing party to ensure that sealed,
441 impounded, or nonpublic cases, documents, and information are redacted
442 and/or submitted to the court in accordance with this rule.

443
444 **(a)** For any cases designated as sealed, impounded, or nonpublic by
445 federal or state law, court rule, court order, or administrative order, every filing
446 must be clearly and conspicuously marked, "NOT FOR PUBLIC DISCLOSURE."

447
448 **(b)** When any document or other filing that is nonpublic or has been
449 impounded or sealed is submitted to the court in a public case, that document
450 or filing must be clearly and conspicuously marked, "NOT FOR PUBLIC
451 DISCLOSURE."

452

453 (c) No categories of information or data that are designated as sealed,
454 impounded, or nonpublic by federal or state law, court rule, court order, or
455 administrative order shall be submitted to any court as part of a public
456 document. Where required, an active financial account number may be
457 identified by the last four digits when the financial account is the subject of the
458 litigation and cannot otherwise be identified.

459
460 (d) If any filed document does not comply with the requirements of these
461 rules, a court shall, upon motion or its own initiative, order the filed document
462 returned, and that document shall be deemed not to have been filed. A court
463 may impose sanctions on any party or person filing a noncompliant document.

464
465 **RULE 10. SUMMARY INFORMATION ACCESSIBLE BY THE PUBLIC IN SOME**
466 **FAMILY CASES OR PROCEEDINGS**

467
468 In cases or proceedings for divorce, annulment, or judicial separation;
469 parental rights and responsibilities, including but not limited to the
470 establishment or enforcement of a child support obligation; and de facto
471 parenthood, the public may access the summary complaint, summary answer,
472 registry of actions, and summary of the judgment.

473
474 **RULE 11. FEES**

475 Reasonable fees established by the Judicial Branch may be imposed for
476 providing public access to court records and data, as allowed by these rules. A
477 fee schedule shall be in writing and publicly posted.

478
479
480
481 **RULE 12. CORRECTING CLERICAL ERRORS IN COURT RECORDS**

482
483 (a) A party, or the party's attorney, seeking to correct a clerical error in a
484 court record may submit a written request for correction to the custodian of
485 the court record, using the form designed and published by the Administrative
486 Office of the Courts.

487
488 (b) The requesting party shall specifically state on the request form the
489 information that is alleged to be a clerical error and shall provide sufficient
490 facts, including supporting documentation, that corroborate the requesting
491 party's allegation that the information in question is erroneous.

492
493 **(c)** The requesting party shall send copies of the request to all parties to
494 the case.

495
496 **(d)** Within 21 days after receipt, the custodian shall respond in writing to
497 the requesting party and all parties to the case in one of the following manners:

498 (1) The request does not contain sufficient information and facts to
499 determine what information is alleged to be in error, and no further
500 action will be taken on the request.

501
502 (2) The request does not concern a court record that is covered by
503 this policy, and no further action will be taken on the request.

504
505 (3) A clerical error does exist in the court record, and the
506 information in question has been corrected.

507
508 (4) A clerical error does not exist in the court record.

509
510 (5) The request has been received, and an additional period not
511 exceeding 35 days is necessary to complete a review of the request.

512
513
514 **(e)** A requesting party may seek review of the custodian's response
515 under subsections (d)(1)-(4) within 14 days after the mailing date of the
516 response on a form that is designed and published by the Administrative Office
517 of the Courts.

518
519 The request shall be reviewed by the judge(s) who presided over the
520 case.

521
522
523 **Drafters' Notes - 2019**

524 Rule 1 explains the purpose and the applicability of the rules. Most court
525 records that are accessible to the public will be available on the Judicial Branch
526 website. Records of Protection from Abuse actions, however, will be available
527 to the public only at court houses. This limitation on access is required by 18
528 United States Code, Section 2265(d)(3). Rule 2 provides definitions, and Rule 3
529 explains the Judicial Branch's general policy of access.

530
531 Rule 4, when promulgated, will establish the rules for public access to
532 aggregate, bulk, and compiled data.
533

534 Rule 5 lists categories of information contained in court records that are
535 not accessible to the public. In some contexts, access to most of the categories
536 of information identified as nonpublic in Rule 5 was already restricted through
537 statutes, court rules, or administrative orders. Each subsection in Rule 5
538 describing documents or information protected by law and not available for
539 public inspection is further explained below:

540 (b) and (c) Private images as described in Title 17-A, section 511-A,
542 subsection 1 are not available for public inspection;

543 (d)(5) Financial statements in family cases are not available for public
544 inspection pursuant to M.R. Civ. P. 108(d)(3), and records of personal
545 financial information submitted in mediation on the Foreclosure
546 Diversion program are confidential pursuant to Title 14, section 6321-A,
547 subsection 4;

548 (f) Health and medical records are confidential pursuant to Title 1,
549 section 402, subsection 3, paragraph H, the Health Insurance Portability
550 and Accountability Act of 1996, PL 104-191, and 42 United States Code,
551 Section 290dd-2; and Title 22, section 1711-C;

552 (g) Psychological and intelligence test documents and results are
553 confidential pursuant to the Family Educational Rights and Privacy Act,
554 20 United States Code, Section 1232g, and Title 34-B, section 1207;

555 (h) School records, including scholastic achievement data on
556 individuals are confidential pursuant to the Family Educational Rights
557 and Privacy Act, 20 United States Code, Section 1232g, and 34 Code of
558 Federal Regulations, Part 99;

560 (i) HIV/AIDS testing information is not, pursuant to Title 5, section
561 19203, *et seq.*, available for public inspection unless an exception
562 contained in that statute applies;
563
564

565 (j) Death certificates are not available for public inspection pursuant
566 to Title 22, section 2706; certain records of the Office of Medical
567 Examiner are confidential pursuant to Title 22, section 3022.

568
569 (k) Immigration documents are confidential pursuant to the Privacy
570 Act of 1974, 5 United States Code, Section 552a;

571
572 (l) “Confidential criminal history record information” is confidential
573 pursuant to the Maine Criminal History Records Information Act, Title 16,
574 chapter 7;

575
576 (m) Personal and identifying information concerning individuals with
577 court-appointed counsel is not available for public inspection pursuant
578 to Title 4, section 1806

579
580 (n) Documents in proceedings involving a Protection from Abuse
581 Order or some other protective order that would reveal the identity or
582 location of a protected person under the order are confidential pursuant
583 to 18 United States Code, Section 2265(d)(3);

584
585 (o) Identifying information in protection from harassment actions may
586 not be disclosed when it is alleged that the health, safety, or liberty of a
587 party or child would be jeopardized by disclosure of personally
588 identifiable information, pursuant to Title 5, section 4656;

589
590 (p) Juror qualification questionnaires are confidential pursuant to
591 Title 14, section 1244-A, subsections 7 through 9; juror information used
592 during the selection of jurors is confidential pursuant to Title 14, section
593 1254-B, except as allowed by section 1254-B(3); and jurors’ notes are
594 confidential pursuant to Rule 24(g) of the Maine Rules of Unified Criminal
595 Procedure and Rule 47(f) of the Maine Rules of Civil Procedure;

596
597 (q) Witness subpoenae that extend to privileged or protected
598 documents are not available for public inspection pursuant to the Maine
599 Rules of Unified Criminal Procedure, now in Rule 17(d), and Rules
600 26(b)(5) and 45(c) and (d) of the Maine Rules of Civil Procedure;

601
602 (r) Arrest warrants and associated affidavits for probable cause and
603 indictment that have not been executed are not available for public

604 inspection, pursuant to Rule 4(d) of the Maine Rules of Unified Criminal
605 Procedure;

606
607 (s) In forma pauperis affidavits are not available for public inspection,
608 except by order of court, pursuant to the Maine Rules of Civil Procedure,
609 Rule 91(a)(2);

610
611 (t) Subpoenae *duces tecum* that extend to privileged or protected
612 documents are not available for public inspection, pursuant to the Maine
613 Rules of Unified Criminal Procedure, now in Rule 17 A;

614
615 (u) Search warrants and associated affidavits ordered impounded or
616 sealed by the court or that have not yet been executed are not available
617 for public inspection pursuant to the Maine Rules of Unified Criminal
618 Procedure, now in Rule 41(f) and Rule 41B; and

619
620 (v) Presentence reports, including attachments are not available for
621 public inspection, pursuant to the Maine Rules of Unified Criminal
622 Procedure, now in Rule 32(c).

623 The categories of nonpublic information in Rule 5 include personally
624 identifiable information that must be protected from public access to ensure
625 that court records do not become a cache of valuable and dangerous
626 information for data-miners or identity thieves, and those categories that
627 protect the names and images of minors. Address and location information of
628 victims is specifically made confidential by Title 17-A, section 1176.

629
630 Rule 6 lists case types for which court records are not accessible to the
631 public. With the exceptions of subsections (j) through (l), public access for the
632 case types and proceedings identified in Rule 6 is already restricted through
633 statutes, court rules, or administrative orders, as follows:

634
635 (a) Adoption proceedings are not open to the public pursuant to Title
636 18-A, section 9-310;

637
638 (b) Child protective proceedings are not open to the public pursuant to
639 Title 22, section 4007;

640

641 (c) Mental health civil commitment proceedings are not open to the
642 public pursuant to Title 34-B, section 3864, paragraphs (5)(G) and (H);

643
644 (d) Juvenile hearings are partially closed to the public, pursuant to
645 Title 15, sections 3307 and 3308;

646
647 (e) Medical malpractice screening panel proceedings are closed to the
648 public pursuant to Title 34, sections 2853(1-A), 2854(1-A), and 2857;

649
650 (f) Sterilization proceedings are closed to the public pursuant to Title
651 34-B, section 7014;

652
653 (g) Petitions for court-authorized abortions for minors are closed to
654 the public pursuant to Title 22, section 1597-A, subsection (6),
655 paragraphs (B) and (C); ~~and~~

656
657 (h) Grand jury proceedings are closed to the public pursuant to the
658 Maine Rules of Unified Criminal Procedure, Rule 6; ~~and~~

659
660 ~~(h)~~(i) Applications for and proceedings concerning concealed handgun
661 permits are confidential pursuant to Title 25, section 2006.

Formatted: List Paragraph, Left, No bullets or numbering

662
663 Subject to the enactment of legislation and the promulgation of court
664 rules, Rule 6, subsections (j) and (k) will establish that access to digital court
665 records will be closed to the public in certain family cases and proceedings in
666 which a great deal of private information is filed with the court. Currently,
667 among the variety of family cases filed in Maine's courts, only adoption and
668 child protection matters are closed to the public; and in those cases, the public
669 is excluded by statute from all hearings and is precluded from having any access
670 to case records.

671 Although the public does have the right to know what happens in court,
672 that right does not extend to the personal information generated in family
673 cases. M.R. Civ. P. 101 already provides for orders preventing public access to
674 "identifying information" when a party alleges that "the health, safety or liberty
675 of a party or minor child would be jeopardized by disclosure" of that
676 information. The purpose of Rule 6(j) and (k) is to reflect the reality that by
677 making family case records electronically accessible, the court could be
678 jeopardizing "the health, safety or liberty of a party or minor child."

679
680 Because there is a benefit to making some limited information available
681 for review by the public in cases or proceedings involving divorce, annulment,
682 or judicial separation; parental rights and responsibilities, including but not
683 limited to the establishment or enforcement of a child support obligation; and
684 de facto parenthood, “summary” documents to be used by the parties in
685 litigating these cases, and “summary” orders containing information about the
686 court’s decisions will be made available to the public, as provided in Rule 10. In
687 addition, the public will have access to the registry of actions, a term of art for
688 what used to be known as “docket entries.” This access will allow any member
689 of the public to have sufficient information to understand and evaluate court
690 operations.

691
692 Rule 7 establishes a method for requesting the impounding or sealing of
693 public court records, Rule 8 establishes a method for seeking access to sealed
694 or impounded public court records, and Rule 9 establishes the methods for
695 identification and handling of sealed, impounded, or nonpublic cases,
696 documents, information, and data.

697
698 Rule 10 establishes a method for providing summary case record
699 information to the public in some types of family matter proceedings. The
700 Family Division will publish forms to be used by parties litigating divorce,
701 annulment, or judicial separation; parental rights and responsibilities,
702 including but not limited to the establishment or enforcement of a child support
703 obligation; and de facto parenthood, so that summary complaints and answers
704 will be available for public review. In addition, judicial officers will create
705 summaries of judgments that provide some information about the resolution of
706 the case or proceeding, including whether there was an order of shared,
707 allocated, or sole parental rights and responsibilities, whether there was an
708 award of spousal support, and whether real property was awarded to either
709 party.

710 If any party to a pending case needs additional information concerning a
711 separate divorce, annulment, or judicial separation; parental rights and
712 responsibilities, including but not limited to the establishment or enforcement
713 of a child support obligation; and de facto parenthood case or proceeding, that
714 party may request information about the separate case or proceeding through
715 discovery. If the person from whom the information is requested does not

716 agree to provide the requested information, the parties may request a
717 conference with a judicial officer. *See* M.R. Civ. P. 26(g).

718
719 Rule 11 concerns the Judicial Branch's establishment of fees to support
720 access to digital court records.

721
722 Finally, Rule 12 creates a process for correcting clerical errors in digital
723 court records. Court records are as susceptible to clerical errors and omissions
724 as any other public record. The power of the court to correct errors in its own
725 records is inherent. It is important to emphasize that this rule does not provide
726 a party who is dissatisfied with a court's order or judgment a new avenue to
727 appeal the same by alleging there is an error in the court's order or judgment.
728 Rather, this rule permits a party to "fix" information that appears in a court
729 record that is not, for one reason or another, correct.

730 Particularly in the context of internet publication of court records, a
731 streamlined process is appropriate for addressing clerical errors to allow for
732 prompt resolution of oversights and omissions. For example, to the extent that
733 a registry of actions in a court's case management system incorrectly reflects a
734 court's order, or a scanning error occurred with regard to an uploaded
735 document, such clerical inaccuracies may be promptly corrected by the
736 appropriate court staff, upon notification, without the need for a court order.
737 However, the process in Rule 12 is not to be used when the alleged inaccuracy
738 is found in an order or judgment. Parties claiming inaccuracies in orders and
739 judgments themselves must bring those inaccuracies to the attention of the
740 court that issued the order or judgment in accordance with existing procedures.



March 27, 2019

Matthew Pollack
Executive Clerk
Maine Supreme Judicial Court
205 Newbury Street Room 139
Portland, Maine 04112-0368

Re: Comments of Disability Rights Maine to Proposed Maine Digital Court
Records Access Rules

Dear Matt:

Disability Rights Maine (DRM) has a general comment to the Proposed Maine Digital Court Records Access Rules and one specific comment.

The general comment relates to the principle, expressed in the preamble to the proposed rule, that the public have access to court records created or maintained by the Judicial Branch. DRM endorses that principle. DRM also believes that public access should include access by people with disabilities. The Judicial Branch must comply with the Americans with Disabilities Act (ADA). That means that people with disabilities must be able to access digital records to the same extent as people without disabilities. I checked the websites of New Hampshire, the Rhode Island and South Dakota but did not see anything on those websites about digital access for people with disabilities. I then went to Tyler Technologies' website and found nothing about ADA compliance. DRM is asking how the Judicial Branch is going to address access for people with disabilities, including people who are blind. DRM believes that the Judicial Branch should convene a stakeholder meeting with civil legal service providers to address the issue of access, as well as other issues raised by those providers.

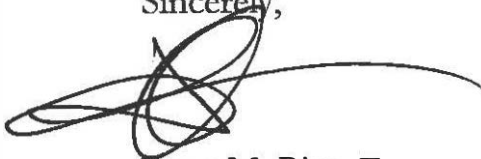
24 Stone Street, Suite 204, Augusta, ME 04330
207.626.2774 • 1.800.452.1948 • Fax: 207.621.1419 • drme.org

MAINE'S PROTECTION AND ADVOCACY AGENCY FOR PEOPLE WITH DISABILITIES

Proposed Rule 6 excludes certain specific case types and proceedings from public access. For example, according to Proposed Rule 6(c) mental health civil commitment proceedings are excluded from public access. DRM supports this exclusion. DRM also believes that 80C appeals from clinical review panels (CRP) should be excluded for the same reasons that mental health civil commitment proceedings are excluded. The decision of a CRP allowing a patient to be involuntarily treated can be appealed to Superior Court pursuant to Rule 80C of the Maine Rules of Civil Procedure. 34-B M.R.S.A. §3861(F)(1) &(2). The information contained in those filings includes personal medical and psychiatric data that should not be public.

Thank you for the opportunity to comment on the proposed rules.

Sincerely,

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

Peter M. Rice, Esq.
Legal Director

Peter J. Guffin, Esq.

ME Bar No. 3522

Comments Regarding Proposed Digital Court Records Access Rules

March 27, 2019

Chief Justice Saufley, Senior Associate Justice Alexander, and Associate Justices Mead, Gorman, Jabar, Hjelm and Humphrey:

Thank you for the opportunity to submit comments regarding the draft Digital Court Records Access Rules” (the “Rules”) recently proposed by the Maine Supreme Judicial Court (“the SJC”).

In offering the following comments, I am acting solely in my personal capacity as an interested and informed member of the Bar. I am not submitting these comments on behalf of any client or other organization.

The views expressed by me are my own and do not reflect the views of my law firm Pierce Atwood LLP, where I am a partner and chair the firm’s Privacy & Data Security practice, or the University of Maine School of Law, where I am a Visiting Professor of Practice and serve as the Co-Director of its Information Privacy Law Program.

With privacy and transparency issues of such critical importance to the citizens of Maine, it is troubling that the SJC has provided to the public and members of the Bar only scant details regarding its new digital case management system and the SJC’s plans with respect to implementation of the system.

The Rules in large part mirror many of the provisions of the now defunct Digital Court Records Access Act (the “Act”) which had been proposed by the SJC earlier this year. Echoing the comments that I submitted to the SJC on January 25, 2019 regarding the Act, I believe the Rules likewise are anything but comprehensive and represent a proposed solution for only one small piece of a much larger problem. Just like the Act, the Rules fail to address a number of privacy, transparency, data security and access-to-justice issues and raise many more issues and questions than they answer.

Having now read the many other thoughtful comments that were submitted to the SJC earlier this year regarding the Act, I know that I am not alone in these sentiments.

The SJC has not provided members of the Bar or the public with any additional information about the new digital case management system or its plans for implementation of the system in response to the issues and questions that were raised in the comments submitted regarding the Act.

Apart from the Rules, which largely govern access to the court records once they are in the system, very little is known about the electronic system and how it will work, its functions and features, capabilities and limitations, and how easily users will be able to interact with it.

Also unknown (and unknowable) at this time is how the new system will work in actual practice once it is up and running.

There is no indication that either the SJC or the National Center for State Courts (or anyone else for that matter) has conducted any comprehensive study examining the impact of implementation of digital court records systems in other states on the privacy rights and interests of individuals, including whether permitting public remote online access to court records unduly interferes with or disproportionately harms the marginalized and most vulnerable persons in our society, including the unrepresented, the poor, minorities, children, and victims of domestic abuse, sexual assault and other crimes.

For example, I am not aware of any detailed studies examining the following:

Harms/Remedies

- the nature and number of cybersecurity incidents in state court systems
- the nature and efficacy of courts' incident response plans
- the types of privacy harms to individuals resulting from public remote online access to digital court records
- the types of privacy protections that have been put in place to mitigate the risk of security incidents and misuse of personal data
- the effectiveness of those privacy protections
- the types of remedies that have been made available for individuals to seek relief or redress for actual or potential privacy harms resulting from public disclosure or misuse of personal data

Unrepresented Litigants/Access-to-Justice/Protection of Non-Parties

- how filings by unrepresented litigants are being managed
- the resources being made available to assist unrepresented litigants
- how courts are educating the public about protection of personal information
- how courts are handling situations in which litigants and other individuals do not have a bank account or other electronic payment method
- how courts are facilitating the protection of information in court records
- how non-party sensitive personal information is being protected

If such studies exist, they may be useful in informing the SJC as to how to calibrate the balance between privacy and transparency. If such studies do not exist, I urge the SJC to consider conducting (or requesting that the NCSC or some other organization conduct) one or more such studies.

Only after the system has been in operation for period of time will the SJC be able to assess its effect on the privacy rights and interests of individuals, including whether permitting public remote online access to court records will unduly interfere with or disproportionately harm the marginalized and most vulnerable persons in our society.

It is telling that the SJC has chosen to hit the pause button on establishing rules governing access to aggregate, bulk, and compiled data. From a transparency perspective, the latter data is the very kind of valuable information which the public needs to be able to keep a watchful eye on the workings of the Maine Judicial Branch.

In electing to punt and to reserve judgment on the effective date and content of Rule 4, the SJC explained:

The Judicial Branch will undertake a review of the operational capacity of the Odyssey case management system and the resources of the Judicial Branch eighteen months after the case management system has been fully operational at all court locations before promulgating rules relating to dissemination of aggregated, compiled, or bulk data.

The SJC's hitting the pause button on promulgating rules relating to dissemination of aggregated, compiled, or bulk data, raises the obvious question:

Why do the Rules treat transparency into the operations and performance of the SJC differently than it treats transparency into the private, personal information of Maine citizens?

Facts and details matter. By creating public remote online access rules prematurely in the abstract and in a vacuum without having the benefit of seeing the full picture in terms of how the system works in actual practice, the SJC runs the significant risk of not getting it right in terms of balancing the competing interests of privacy and transparency.

It is imperative that the SJC get it right, as the stakes are quite high with regard to protection of the rights of affected individuals as well as the integrity of the SJC as an institution.

For these reasons, I urge the SJC likewise to hit the pause button on promulgating rules relating to public remote online access to the private, personal information of Maine citizens for at least eighteen months after the case management system has been fully operational at all court locations.

Carpenter v. United States

That digital is different, requiring us to recalibrate the rules for determining what is public vs. private, is one of the biggest takeaways from the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

Noting the deeply revealing nature of cell-site location information ("CSLI"), its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the Court held that the Fourth Amendment applies to the government's search of CSLI.

Writing for the majority, Justice Roberts observed:

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today.

Id. at 2219.

Carpenter also reminds us that “[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, ‘what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.’” *Id.* at 2217 (citing *Katz v. United States*, 389 U. S., at 351–352).

Based on this line of reasoning it follows that persons have a legitimate expectation of privacy in information revealed in court records, and that a person does not surrender all privacy rights by venturing into the courthouse.

Constitutional Right to Privacy

As a threshold matter, the SJC must answer the question whether the Rules impermissibly invade an individual’s constitutionally protected zone of privacy.

In *Whalen v. Roe*, 429 U.S. 589 (1977), the Supreme Court, recognizing a constitutional right of privacy, articulated two different kinds of interests to be afforded protection. The first is “the individual interest in avoiding disclosure of personal matters,” and the second is “the interest in independence in making certain kinds of important decisions.”

Without question, both of these privacy interests are impaired by the Rules. Together these issues should be of paramount concern to the SJC. If individuals have to give up control over dissemination of their private, personal information, individuals may be discouraged from going to court and may decline to seek justice and relief through the courts.

The issue in *Whalen* was whether the State had satisfied its duty to protect from unwarranted disclosure the sensitive, personal information of individuals which was being collected and used by the State in the exercise of its broad police powers. Finding that the State’s “*carefully designed program include[d] numerous safeguards intended to forestall the danger of indiscriminate disclosure,*” the Court held that there was no impermissible invasion of privacy. However, it was careful to limit its holding to the specific facts presented.

A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the

enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure [429 U.S. 589, 606] of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.

429 U.S. at 605-606.

Justice Brennan's concurring opinion in *Whalen* also is instructive:

The New York statute under attack requires doctors to disclose to the State information about prescriptions for certain drugs with a high potential for abuse, and provides for the storage of that information in a central computer file. The Court recognizes that an individual's "interest in avoiding disclosure of personal matters" is an aspect of the right of privacy, ante, at 598-600, and nn. 24-25, but holds that in this case, any such interest has not been seriously enough invaded by the State to require a showing that its program was indispensable to the State's effort to control drug abuse.

*The information disclosed by the physician under this program is made available only to a small number of public health officials with a legitimate interest in the information. As the record makes clear, New York has long required doctors to make this information available to its officials on request, and that practice is not challenged here. Such limited reporting requirements in the medical field are familiar, ante, at 602 n. 29, and are not generally regarded as an invasion of privacy. Broad dissemination by state officials of such information, however, would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests. See, e. g., *Roe v. Wade*, 410 U.S. 113, 155 -156 (1973).*

What is more troubling about this scheme, however, is the central computer storage of the data thus collected. Obviously, as the State argues, collection and storage of data [429 U.S. 589, 607] by the State that is in itself legitimate is not rendered unconstitutional simply because new technology makes the State's operations more efficient. However, as the example of the Fourth Amendment shows, the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.

In this case, as the Court's opinion makes clear, the State's carefully designed program includes numerous safeguards intended to forestall the danger of indiscriminate disclosure. Given this serious and, so far as the record shows, successful effort to prevent abuse and limit access to the personal information at issue, I cannot say that the statute's provisions for computer storage, on their face, amount to a deprivation of constitutionally protected privacy interests, any more than the more traditional reporting provisions.

*In the absence of such a deprivation, the State was not required to prove that the challenged statute is absolutely necessary to its attempt to control drug abuse. Of course, a statute that did effect such a deprivation would only be consistent with the Constitution if it were necessary to promote a compelling state interest. *Roe v. Wade*, supra; *Eisenstadt v. Baird*, 405 U.S. 438, 464 (1972) (WHITE, J., concurring in result).*

429 U.S. at 606-607.

Many federal circuit courts have recognized the constitutional right to information privacy. See, e.g., *Barry v. City of New York*, 712 F.2d 1554, 1559 (2d Cir. 1983); *United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 577-80 (3d Cir. 1980); *Walls v. City of Petersburg*, 895 F.2d 188, 1292 (4th Cir. 1990); *Plante v. Gonzalez*, 575 F.2d 1119, 1132, 1134, (5th Cir. 1978); *Kimberlin v. United States Dep't of Justice*, 788 F.2d 434 (7th Cir. 1986); *In re Crawford*, 194 F.3d 954, 959 (9th Cir. 1999).

One court has looked to the “reasonable expectations of privacy” test to determine whether information is entitled to protection under the constitutional right to

information privacy. See *Fraternal Order of Police, Lodge No. 5, Philadelphia*, 812 F.2d 105, 112 (3d Cir. 1987).

The Third Circuit has developed the most well-known test for deciding constitutional right to information privacy cases. In *United States v. Westinghouse Electric Corp.*, 638 F.2d 570, 578 (3d Cir 1980), the court articulated seven factors that “should be considered in deciding whether an intrusion into an individual’s privacy is justified”: (1) “the type of record requested”; (2) “the information it does or might contain”; (3) “the potential for harm in any subsequent nonconsensual disclosure”; (4) “the injury from disclosure to the relationship in which the record was generated”; (5) “the adequacy of safeguards to prevent unauthorized disclosure”; (6) “the degree of need”; and (7) “whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.”

At least one court has observed that the constitutional right to information privacy “closely resembles – and may be identical to – the interest protected by the common law prohibition against unreasonable publicity given to one’s private life.” *Smith v. City of Artesia*, 772 P.2d 373, 376 (N.M. App. 1989).

Maine Constitution

Although the Maine Constitution contains no express provisions protecting an individual’s right to privacy, the Natural Rights Clause, Article I, section 1, of the Maine Constitution arguably provides the basis for recognizing privacy as an independent and distinct constitutional right.

It provides as follows:

Natural Rights. All people are born equally free and independent, and have certain natural, inherent and unalienable rights, among which are those of enjoying and defending life and liberty, acquiring, possessing and protecting property, and of pursuing and obtaining safety and happiness.

For the same reasons the Rules impair the privacy interests recognized in *Whalen*, they also impair affected individuals’ “natural, inherent and unalienable rights” under the Natural Rights Clause of the Maine Constitution.

The broad language of the Natural Rights Clause has no federal analogue, and it could support an argument that Maine's Constitution provides broader privacy protections for individuals than does the U.S. Constitution. The Maine Constitution has an existence independent of the U.S. Constitution. While I haven't researched the issue, I am not aware of any jurisprudence on the right to privacy under the Maine Constitution. In other jurisdictions, some state courts have found that almost identically worded provisions form the basis of state privacy claims.

In other contexts, Maine's courts have held that the Maine Constitution provides additional guarantees beyond those contained in the U.S. Constitution, as have many other states' courts, such as New Hampshire, Vermont and Massachusetts. *See e.g., State v. Sklar*, 317 A.2d 160, 169 (Me. 1974) (noting that the state constitution, but not the Federal Constitution, guarantees trial by jury for all criminal offenses and similar language of federal and state provisions is not dispositive); *Danforth v. State Dep't of Health and Welfare*, 303 A.2d 794, 800 (Me. 1973) (holding that the state constitution protects parent's right to custody of child and that parent has due process right under the state constitution to court-appointed counsel although the Federal Constitution may not guarantee that right); *State v. Ball*, 471 A.2d 347 (N.H. 1983) (analyzing state constitutional claim before turning to Federal Constitution, and concluding state constitution's limitations on search and seizure were stricter than federal limitations); *State v. Kirchoff*, 587 A.2d 988 (Vt. 1991) (stating that the Vermont Constitution provides more protection against government searches and seizures than does the Federal Constitution); and *Attorney General v. Desilets*, 636 N.E.2d 233 (Mass. 1994) (interpreting the Massachusetts Constitution's free exercise of religion clause as broader than federal protections).

In 1905, the Georgia Supreme Court recognized privacy as an independent and distinct right under the Georgia Constitution. In *Pavesich v. New England Life Ins. Co.*, 50 S.E. 68 (Ga. 1905), the Georgia Supreme Court found the state's residents to have a "liberty of privacy" guaranteed by the Georgia constitutional provision: "no person shall be deprived of liberty except by due process of law." The court grounded the right to privacy in the doctrine of natural law:

The right of privacy has its foundations in the instincts of nature. It is recognized intuitively, consciousness being witness that can be called to establish its existence. Any person whose intellect is in a normal condition recognizes at once that as to each individual member of society there are

matters private and there are matters public so far as the individual is concerned. Each individual as instinctively resents any encroachment by the public upon his rights which are of a private nature as he does the withdrawal of those rights which are of a public nature. A right of privacy in matters purely private is therefore derived from natural law. Id. At 69

At least ten state constitutions contain explicit right-to-privacy clauses, including Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington.

Conclusion

By creating public remote online access rules prematurely in the abstract and in a vacuum without knowing how the system will work in actual practice, the SJC runs the significant risk of not getting it right in terms of balancing the competing interests of privacy and transparency.

Particularly concerning is that it is unknown at this time how implementation of the system will affect the privacy rights and interests of individuals, including whether permitting public remote online access to court records will unduly interfere with or disproportionately harm the marginalized and most vulnerable persons in our society, including the unrepresented, the poor, minorities, children, and victims of domestic abuse, sexual assault, and other crimes.

It is imperative that the SJC get it right, as the stakes are quite high with regard to protection of the rights of affected individuals as well as the integrity of the Judicial Branch as an institution.

For all of the foregoing reasons, I urge the Supreme Judicial Court to hit the pause button on promulgating rules relating to public remote online access to the private, personal information of Maine citizens for at least eighteen months after the case management system has been fully operational at all court locations.

Respectfully,



Peter J. Guffin., Esq.



Matt Pollack < matt.pollack@courts.maine.gov >

Digital Court Records Access Rules

1 message

rhark@harklawoffice.com < rhark@harklawoffice.com >
To: Law Court Clerk's Office < lawcourt.clerk@courts.maine.gov >

Tue, Mar 12, 2019 at 2:59 PM

Matt:

I am writing to offer three comments on the proposed Maine Digital Court Records Access Rules.

I did note in Rule 5(d)(1), that home addresses are to be inaccessible. This is fine, but this might require revision of the court's *Civil Summary Sheet*, which asks for the addresses of the parties (I have always assumed that the Summary Sheet requires this information for two reasons: to give the court a quick means of determining whether the venue is proper; and to provide a means for contacting an unrepresented party).

In Rule 5(m), where it speaks of "...applications for court-appointed counsel including in forma pauperis affidavits[,]” the word “including” should be stricken and the word “or” should be substituted, since an application for proceeding *in forma pauperis* does not *necessarily* entail asking for court-appointed counsel, and I would think that notwithstanding that someone is not requesting court-appointed counsel, the application to proceed *in forma pauperis* probably ought not to be public.

Finally, following Rule 6(i) which addresses non-compliance with *gestational carrier agreements* (anticipating some legislation), there should be an additional provision, that addresses Birth Orders, which are required to provide for “sealing the record from the public to protect the privacy of the child and the parties...” I propose the additional provision should read as follows:

() Proceedings for Birth Orders pursuant to 19-A M.R.S. §1928.

Robert S. Hark

ATTORNEY

75 Pearl Street, Suite 209

Portland, ME 04101

PHONE (207) 773.5000 FAX (207) 772.0385

rhark@harklawoffice.com

This E-Mail may contain information that is privileged, confidential and / or exempt from discovery or disclosure under applicable law. Unintended transmission shall not constitute waiver of the attorney-client or any other privilege. If you are not the intended recipient of this communication, and have received it in error, please do not distribute it and notify me immediately by email at rhark@harklawoffice.com or via telephone at 207-773-5000 and delete the original message. Unless expressly stated in this e-mail, nothing in this message or any attachment should be construed as a digital or electronic signature or as a legal opinion



Free Legal Help for Maine's Seniors

March 27, 2019

Via electronic mail

Matthew Pollack, Executive Clerk
Maine Supreme Judicial Clerk
205 Newbury Street, Room 139
Portland, ME 04112-0368

RE: Comments by Legal Services for the Elderly on Proposed Digital Court Records Access Rules

Dear Justices of the Maine Supreme Judicial Court,

Legal Services for the Elderly (LSE) respectfully submits the following brief comments with regard to the proposed Digital Court Records Access Rules and the anticipated implementation of a statewide digital court records system. LSE is a statewide nonprofit legal aid provider that offers free, high quality legal services to Maine's socially and economically needy elderly age 60 and over.

LSE previously submitted comments on January 17 and 25, 2019. As part of those comments, LSE requested additional information about the timing, scope, and practical details of the anticipated transition to e-filing and digital court records. Thereafter, LSE attended the March 6, 2019 meeting of the Advisory Committee on the Rules of Civil Procedure. At that meeting, we were happy to learn from court administrators that following implementation of the new rules, pro se parties will continue to be able to file pleadings and other materials in paper. As we discussed previously, continuing to permit paper filing provides a means of access for parties who do not have computer/internet access or the skills necessary to effectively interact digitally with the courts.

We anticipate that e-filing and digital access to court records could provide substantial practical benefits for LSE staff and attorneys. However, we continue to have concerns about the transition to a digital court records system because we have not seen how the Court intends to address issues involving access, security, and privacy.

LSE continues to be willing to work with the Court to address these concerns and would welcome the opportunity to discuss the anticipated digital court records system at a time and place convenient for the Court.

Respectfully submitted,



Ben Jenkins
Litigation Director
Legal Services for the Elderly
136 US Route One
Scarborough, ME 04074
(207) 396-6532



MAINE ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

P.O. Box 17642
Portland, ME 04112-8642
(207) 523-9869
mainemacdl@gmail.com

March 27, 2019

2018-2019 OFFICERS

President
Hunter J. Tzovarras

President-Elect
Jamesa J. Drake

Vice President
Amber L. Tucker

Treasurer
Walter F. McKee

Executive Committee Appointee
Matthew D. Morgan

2018-2019 DIRECTORS

Justin W. Andrus
Dylan R. Boyd
Amy L. Fairfield
Heather Gonzales
Devens Hamlen
Scott F. Hess
Stacey D. Neumann
Logan E. Perkins
Neil Prendergast
Luke S. Rioux
Heather M. Seasonwein
Adam P. Sherman
Adam Swanson
Robert T. Van Horn

EXECUTIVE DIRECTOR

Tina Heather Nadeau

Matthew Pollack, Clerk
Maine Supreme Judicial Court
205 Newbury Street, Rm. 139
Portland, ME 04112-0368
lawcourt.clerk@courts.maine.gov

VIA EMAIL ONLY

RE: MACDL Comments on Digital Court Records Access Rules

Dear Mr. Pollack,

This letter is the Maine Association of Criminal Defense Lawyers' response to the Court's request for comments on its draft "Digital Court Records Access Rules." We recognize the delicate balance between privacy and transparency regarding such records and appreciate the opportunity to comment.

There are a few issues that MACDL members have brought up concerning these proposed rules, which I share here for later development, we hope, through public hearing. We are pleased to see that this Court has decided to establish its procedures and rules regarding access to digital court records outside of the legislative process. Memorializing these proposals as rules rather than legislation will give the Court the flexibility and responsiveness it needs to address concerns and problems as they emerge—and they certainly will emerge.

To start, we would recommend that these rules reflect a difference between "public" records—those that are generally accessible to the public in person—and "online" records, those which are allowed to be accessible online immediately. The ability to disseminate online information is effortless and once that information hits online, there is no retrieving it or limiting access to it ever again.

We are extremely concerned with public, digital access to *any* juvenile record whatsoever and would strongly urge this Court to prohibit the dissemination of any juvenile information online to anyone apart from the litigants, the juvenile's parents or guardians, law enforcement, and alleged victims. **Proposed Rule 5, subsection (a)**, therefore, should be amended to strike the allowance of public access to the names and dates of birth of minors in juvenile actions "to the extent that public access is permitted by statute." Similarly, **proposed Rule 6, subsection (d)**, should strike "to the extent that the records are not open to public inspection." We point to **proposed Rule 6, subsection (k)**, which has a blanket prohibition against posting Protection from Abuse records online "although otherwise publicly available at a courthouse." If PFA records are deserving of additional protections from online access, surely juvenile records are entitled to the same protections.

By rule, this Court should declare that juvenile records are not public records. As

recommended by the TAP Report and by the ABA, “Juvenile records should not be public records. Access to and the use of juvenile records should be strictly controlled to limit the risk that disclosure will result in the misuse or misinterpretation of information [and] the unnecessary denial of opportunities and benefits to juveniles . . .” IJA-ABA JUVENILE JUSTICE STANDARDS, *Standards Related to Juvenile Records and Information Services: Part XV: Access to Juvenile Records* 192 (1996). The ubiquity and permanence of information available on the internet makes this recommendation even more needed in 2019. Public digital access to any juvenile record surely undermines the main purpose of our juvenile code: rehabilitation. The missteps of youth should not permanently stain juveniles through their lives. Allowing any juvenile record to be accessible digitally is highly problematic and this Court should protect all such records from public, digital access.

Any rule or policy regarding digital records and electronic filing should make allowances for *pro se* litigants, particularly those who are incarcerated and without meaningful access to a computer or the internet. This is an access to the courts, an access to justice issue for many litigants, including those who do not have access to computers, cannot travel easily to libraries and other places where the public can access computers, have limited English skills, lack literacy or technical skills, or lack the resources to pay fees electronically. Exempting certain litigants from electronic filing requirements is important. Exempting indigent and other under-resourced people from paying certain fees is also imperative, if not Constitutionally mandated.

No new rule or policy should prohibit the parties to a case from accessing sealed records electronically. Any rule or policy should make clear that any sealed record is sealed from the public at large, not from the litigants themselves. Also, the Court should be made aware of pending legislation that could affect **proposed Rule 8**. The pending legislation, which is being introduced by sponsor Representative Rachel Talbot Ross. The heart of that legislation is that juvenile court records should be immediately, automatically, and irrevocably sealed upon completion of the juvenile’s disposition. Additionally, the legislation will establish procedures for adults convicted of crimes to petition courts to seal their court records after certain amounts of time have passed and other conditions are met.

Sealing is terribly important for people who are trying to move past their criminal histories and move on with their lives—Maine currently only has a process for juveniles to petition to seal their records; there is really no process for adults to petition to seal their records at all (apart from those who were 18 to 20 years old at the time of their Class E convictions, a statutory scheme that is sunseting in October 2019). The proposed legislation makes it clear that, once sealed, the court/criminal records are available to law enforcement, the judiciary, and certain specially limited entities. The process this Court has proposed for moving to allow access to previously sealed or impounded material would undermine the purposes behind sealing court records. What we would hate to see is this process being used as a work-around to the sealing of court records.

We are also concerned that there is still no remedy available for people aggrieved by a party’s filing or the court’s uploading of non-redacted documents containing confidential or other sensitive information. Looking at **proposed Rule 7, subsection (b)**, and **proposed Rule 9**, the burden is placed solely on the filing party for compliance with the rules regarding “impounded or sealed cases, documents, or [non-public] information.” Respectfully, this requirement does not adequately protect from the uploading and dissemination of non-public, sealed, or

impounded information. Particularly in the criminal context, there are valid concerns that sensitive, confidential information about our clients and other participants in the case—given the sheer volume of documents—will regularly be uploaded for digital access without appropriate redaction or labeling. This currently happens all the time in public court files: information that should be confidential is just there for the taking should it fall into the wrong hands without appropriate screening.

We repeat previous comments we have made: *The Judicial Branch needs to hire and train clerks who will be tasked with ensuring that the redaction and confidentiality mandated by this proposal, as well as ensuring that certain types of records remain non-public, are actually followed to the letter.* This is too important a consideration for the Judicial Branch not to request appropriations for additional, specialized staff in each courthouse. We cannot do this on the cheap. We cannot skimp on having the necessary personnel if we are to ensure that privacy is protected and the law is followed.

Thank you for giving us the opportunity to submit our initial comments on these draft rule proposals. We look forward to continuing dialogue with the Court on these issues.

With appreciation,

A handwritten signature in blue ink, reading "Tina Heather Nadeau". The signature is fluid and cursive, with a large loop at the end.

Tina Heather Nadeau, Esq.
Executive Director

**Comments from practitioner work group at the Maine Center for Juvenile Policy and Law
on the Judicial Branch’s proposed: (1) Amendments to 4 M.R.S.A §§ 7, 8-C, 8-D; and (2)
DRAFT Digital Court Records Access Rules
Submitted 3/27/2019**

Who we are

Over the last year, the Maine Center for Juvenile Policy and Law has facilitated numerous discussions among a practitioner work group¹ (herein referred to as the “work group”), made up of both defense attorneys and prosecutors, to conduct a comprehensive analysis of the records provisions of the Maine Juvenile Code.

Several members of the work group testified before the Supreme Judicial Court on June 7, 2018 on the importance of protecting juvenile records in serving the purposes of the Maine Juvenile Code, and endorsed the Judicial Branch Task Force on Transparency and Privacy in Court Records (TAP) report’s strong recommendation around juvenile record confidentiality. Members of the work group testified to the importance of protecting juvenile records from public electronic access and supported the TAP report’s strong recommendations that no juvenile court records should be accessible through electronic/internet access.

Since then, the work group has focused its efforts on proposing ways the Juvenile Code might be simplified and re-organized to clarify current law with respect to the treatment of juvenile court records in a way that aligns with the TAP report and essentially retains present policy.

This document

The work group has carefully reviewed the Judicial Branch's proposed: (1) Amendments to 4 M.R.S.A §§ 7, 8-C, 8-D; and (2) DRAFT Digital Court Records Access Rules (“DCRAR”), and appreciates the opportunity to provide comment and feedback.

We have a number of concerns about how the transition to the new digital case management system (DCMS), as authorized under the DCRAR, would impact the mandates of the law and the purposes of the Code that require juvenile cases be treated with greater concern for the privacy of alleged juvenile offenders.² We also have some suggestions regarding clarity, and questions that we feel must be addressed (either within the language of the DCRAR or the Title 4 amendments) before any version reaches the Legislature for a vote or is prepared to be promulgated.

¹ Work group members include: Ned Chester, Esq.; Kristina Dougherty, Esq.; Christopher Northrop, Esq.; Tanya Pierson, ADA; Christine Thibeault, ADA; Jill Ward, Project Manager, Maine Center for Juvenile Policy and Law.

² 15 M.R.S. § 3002(1)

Table of contents

This document is organized as follows:

- I. Concerns that apply to both the Title 4 amendments and the DCRAR
- II. Comments on the Title 4 amendments
- III. Comments on the DCRAR
- IV. Comments on the coordination of the Title 4 amendments and the DCRAR
- V. Questions to be answered
- VI. Conclusion

I. Concerns that apply to both the Title 4 amendments and the DCRAR

A. Juvenile case records should not be made available to the public online

Members of this work group and others testified before the Judiciary last summer about the importance of juvenile record confidentiality in achieving and protecting the purposes of Maine’s Juvenile Code, and some of the unintended consequences that have resulted from confusion about the law and practice. Further, the PREAMBLE of the DCRAR proclaims to “implement the recommendations of the privacy workgroup regarding access to court records.” The TAP report states clearly that “[a]fter much discussion, the Task Force agreed to recommend that juvenile case records not be made available to the public online.”³ There was only one dissenting vote to this recommendation, even though the Task Force included representation from law enforcement, prosecutors, victims’ rights advocates, the business community, the judiciary, the attorney general’s office, the Maine State Bar Association, and the public.

It appears, however, pursuant to proposed Rule 5(a), that the presumption of confidentiality of juvenile records as recommended in the TAP report is not reflected in this draft of the DCRAR, where information is not accessible by the public (through the DCMS), “except in juvenile actions to the extent that public access is permitted by statute.” More directly, in proposed Rule 6(d), the records of juvenile proceedings are excluded from public access (through the DCMS), to the “extent that the records are not open to public inspection.” And under 4 M.R.S. § 8-D(2)(a), electronic access by the public is the presumption, unless non-public under statute, rule, or order.

If this is not the intent of the DCRAR, then we strongly suggest that the DCRAR be reworded to say so. Otherwise, it is our position that juvenile case records should not be made available to the public online. Keeping juvenile records off of electronic public access serves the primarily

³ TAP Report, pg. 12.

rehabilitative mission of the juvenile justice system, and the expectation that the system will best achieve its objectives if the juvenile and his or her mistakes are protected from public scrutiny.

Even if it is the intention of the Judicial Branch to eventually have some juvenile records online, we recommend delaying the transition for juvenile records until bugs and holes in the new DCMS are identified and worked out. We know from the research that there is already a deficit in knowledge around stakeholder understanding of current law with respect to the handling of juvenile records.⁴ The possible negative consequences of the improper release of records are enormously magnified if the records can be accessed online. During this initial roll-out of the DCMS, the risks are simply too grave to permit access to particularly sensitive juvenile court records through electronic means. Some jurisdictions that have made this transition already and believed digital juvenile records were adequately protected have found that confidential, protected information is still finding its way online.

B. Other states with DCMSs do not support public, online access of juvenile records

Looking at the other New England states, New Hampshire, Vermont, Massachusetts, Rhode Island and Connecticut all have DCMS, but none allow public online access of juvenile records.⁵ Of particular note, New Hampshire has special exceptions to confidentiality for juveniles charged with class A crimes, similar to in Maine, yet still does not permit online access to the records in those cases.

C. The statutes protecting Maine’s juvenile case records were written before digital access was possible, and therefore, the Title 4 amendments and the DCRAR should be flexible enough to accommodate any future statutory changes that may amend confidentiality provisions of juvenile case records.

The majority of provisions controlling the access of juvenile case records are contained in 15 M.R.S. §§ 3001-3507, with a few provisions scattered throughout other areas in Maine law. They were written before digital access was possible, or even contemplated. In particular, § 3308(2)⁶ grants public inspection of certain named documents from hearing made public under § 3307(2).⁷ These provisions, as they were written, allow the public the right of “inspection” of court documents at the courthouse.

⁴*Unsealed Fate: The Unintentional Consequences of Inadequate Safeguarding of Juvenile Records in Maine* (2015) <https://cpb-us-w2.wpmucdn.com/wpsites.maine.edu/dist/2/115/files/2018/05/UnsealedFate-w9c6fz.pdf>.

⁵ *E.g.*, <https://secure.vermont.gov/vtcdas/user;jsessionid=DA93D87A8E8371D0E2BCC711F5876AA7?SUBMIT=FAQ&CURRESTATE=vt.court.docs.user.Welcome>

⁶ last amended in 1997

⁷ last amended in 2009

We agree that the new DCMS should be used for public inspection, but suggest that basing online access as described in these provisions is not appropriate, and/or requires further careful consideration. If the Title 4 amendments and the DCRAR move forward, than we suggest that online, access to any/all juvenile records through the DCMS is reserved for authorized non-public persons and entities.

D. The reliance of the proposed amendments/rules on the laws controlling the confidentiality of juvenile case records is premature, where the laws regarding juvenile case records are likely to be addressed in future legislative sessions.

Unlike as is the case for child protection records,⁸ there is no general declaration of the confidentiality of juvenile case records. Certain key words regarding access to otherwise confidential records remain undefined. For example, under § 3308(4) certain confidential juvenile records may be “inspected” by other persons (non-parties) under certain circumstances, but it is not clear what the term “inspected” means. For example, does that statute authorize just a visual inspection or would include making a copy of those records either by hand or by some mechanical or digital means?

Our work group has spent the last year drafting a significant proposed revision⁹ to Title 15 that provides clarity to the juvenile code as it relates to maintaining the confidentiality of juvenile case records, and supports consistency around questions of access and dissemination across system stakeholders. These revisions are solely for the purpose of clarity and do not include any policy changes.

We suggest, again, that the Title 4 amendments and the DCRAR should be flexible enough to accommodate any future statutory changes that may amend confidentiality provisions of juvenile case records.

E. Public access online is not the same as inspection at a courthouse, online access puts the protections guaranteed by the Maine Judicial Courts in jeopardy.

Article I, Section 6 of the Maine Constitution grants accused persons the right to a speedy, public, and impartial trial. But, “[i]n the digital age, the risk of identity theft, stalking, or other misuse of information made public because of a court proceeding is far greater than it was” when that language was drafted.¹⁰ “[H]arms are exacerbated by the readily available nature of information in the digital age.”¹¹ “[T]he litigant may never be able to recover from the public

⁸ 22 M.R.S. 4008(1)

⁹ Available upon request.

¹⁰ See, Rory B. O'Sullivan and Catherine Connell, *Reconsidering the History of Open Courts in the Digital Age*, 39 SEATTLE U. L. REV. 1281 (2016). pg 1298

¹¹ *Id.* at pg. 1299.

exposure of the information, particularly if the information turns out to be false.”¹² This concern is particularly relevant in the case of a juvenile proceeding.

The purpose of the juvenile code is, in part, to assist juveniles in becoming responsible and productive members of society. 15 M.R.S. § 3002(1)(D). A youth’s ability to benefit from and move on from their contact with the juvenile system is undermined by the spread of information about this interaction to the public.

II. Comments on the Title 4 amendments

A. Substantive suggestions/comments

1. Application to juvenile cases

§ 8-D: Permits digital access to public juvenile case records. As explained above, we suggest there be no public, online access to juvenile records

2. Application to all case types

B. Clarity

- The language shifts between “digital” (e.g., § 7) and “electronic” (e.g., § 8-D(1)). Are they referring to something different?

- It is unclear as to what is covered (in the jurisdiction of the Supreme Judicial Court), where the rules reference, for example, “records and documents” (§ 7), “information, data, and documents” (§ 8-D(1)), “case records” (§ 8-D(1)), and “court records” (§ 8-D(2)).

- Will email be considered part of the case records? (§ 8-C(1))

- Will email be considered to be in “custody of its clerks”? (§ 7)

III. Comments on the DCRAR

A. Substantive suggestions/comments

1. Application to juvenile cases

¹² *Id.*

Preamble: The preamble purports that the “rules implement the recommendations of the privacy workgroup regarding public access to court records.” However, the working group clearly stated that all juvenile records should not be publicly accessible online. (see above)

Rule 5(a): To keep juvenile records offline, the phrase “except in juvenile actions to the extent that public access is permitted by statute” should be removed. But even if it is the intention of the Judicial Branch to eventually have some juvenile records online, we suggest that this phrase be temporarily removed until it is confirmed that the DCMS is running smoothly.

Rule 6(d): To keep juvenile records offline, the phrase “to the extent that records are not open to public inspection” should be removed. But even if it is the intention of the Judicial Branch to eventually have some juvenile records online, we suggest that this phrase be temporarily removed until it is confirmed that the DCMS is running smoothly.

Rule 5: The list of “specific information” should be expanded to include all documents related to juvenile cases, except to the extent permitted by statute.

Rule 7(b) and Rule 9: These rules place the burden of redaction on “the filing party.” This is unreasonable for unrepresented juveniles.

2. Application to all case types

Preamble: The dangers of online access are not limited just to the “dissemination of personal information,” online access can disrupt the outcome of cases and the lives of persons involved beyond the life of the case.

Rule 2(c): Three days seems insufficient for parties to review material that will potentially be public and available online.

Rule 5: Why is “[f]inancial information or documents filed in support of requests for waiver of payment of court fees or costs, or in support of requests for court-appointed counsel” no longer part of the list of information excluded from public access? (*see* § 1905(2)(F) in the previous draft of the DCRA)

Rule 7: The DCRAR is unclear as to the difference between “impound” vs. “seal,” and should provide an explanation of what happens when something is impounded or sealed.

Rule 7(a): Another factor in the consideration for impounding/sealing is the purpose of the juvenile code.

Rule 7(b): Can juvenile clients be expected to understand filing rules?

Rule 8(a): The DCRAR should include a specific definition of “party in interest” in the impounding/sealing section: what does it mean when a non-party seeking access to a sealed/impounded case is considered a “party in interest”?

Rule 9: Can juvenile clients be expected to understand filing rules?

And, finally: Specific consequences should be added for violation of the DCRAR, as is done in other areas of the Maine Code.^{13,14}

B. Clarity

Regardless of the underlying policy, clear drafting and the consistent use of language is critical for those relying on the DCRAR for guidance as to the procedure and propriety of access to court records. Therefore, we raise the following questions.

Preamble ¶ 4: the title says “digital” and Rule 1 refers to the “digital case management system,” but this section refers to “electronic” access.

Rules 2(a), 3(a), 3(b), 6(d), and throughout the Drafters’ Notes - 2019: The DCRAR should include a specific definition of “inspection” and/or “inspection or copying.” When someone asks a clerk to “inspect” a document that is “open to public inspection,” what is going to happen? Does this include the right/opportunity for the requester to make a hard copy? Will clerks print a hard copy of requested documents? Can persons who are far from a courthouse request copies to be forwarded electronically in a format which would allow them to make a hard copy or take a screenshot? This is likely to be a question that the clerks will face on a frequent basis.

Rule 1: Where access to records depends on who is seeking them, the draft confusingly refers to “litigants and all other persons and entities”, “parties [and their]. . . lawyers”, “named parties or attorneys of record”, etc. (Rule 1, Rule 2(j)(2)(B), Rule 3(b)). We suggest that just one version is used throughout the DCRAR.

¹³ For example, in 16 M.R.S. §809, “Unlawful dissemination of confidential intelligence and investigative information. . . A person is guilty of unlawful dissemination of confidential intelligence and investigative record information if the person intentionally disseminates intelligence and investigative information confidential under section 804 knowing it to be a violation of any of the provisions of this chapter. . .Unlawful dissemination of confidential intelligence and investigative record information is a Class E crime.”

¹⁴ For example, in 22 M.R.S. §4008(4), “Unlawful dissemination; penalty. A person is guilty of unlawful dissemination if he knowingly disseminates records which are determined confidential by this section, in violation of the mandatory or optional disclosure provisions of this section. Unlawful dissemination is a Class E crime, which, notwithstanding Title 17-A, section 1252, subsection 2, paragraph E, is punishable by a fine of not more than \$500 or by imprisonment for not more than 30 days.”

Rule 2(e) vs. Rule 6: What is the difference between “proceedings” vs. “judicial proceedings”?

Rule 2(g) vs. Rule 1 vs. Rule 8(a): What is the difference between “court records” and “court records and data” and “case, document, or information”?

Rule 2(g)(1): What is a “file” in the context of the digital case management system?

Rule 2(g)(2)(A): What are “materials” in the context of the digital case management system?

Rule 2(b) vs. Rule 5(d): What is the difference between “case or party identifying information” vs. “personally identifiable information”?

Rule 1 vs. Rule 2(f) vs. Rule 2(g)(1)(C) vs. Rule 2(j)(2)(A): Use just one of the following: “judicial officers and other court personnel” vs. “court clerk” vs. “court clerks or staff” vs. “Judicial Branch staff.”

IV. Comments on the coordination of the Title 4 amendments and the DCRAR

There is significant duplication between the Title 4 amendments and the DCRAR. Yet, they are not identical. Which is controlling? For example:

- §8-D(2)(a) & Rule 3(a)
- §8-D(2)(b) & Rule 3(b)

Rule 9 vs. §8-D(2)(d): Is “confidential” the same as “nonpublic”?

-

V. Questions to be answered

- If some juvenile records are going to be accessible to the public through the DCMS**, we suggest that the Judicial Branch first address the following concerns:
 - What will happen when a juvenile is charged with a felony level offense (which would be available to the public) and later admits to a misdemeanor level offense (which would not be public)? Does the felony level record get removed? Notably, even if the felony level offense is removed, it is likely to be in the public domain for many months before the case is resolved. The public nature of the original charge may cause irreparable, permanent harm to the juvenile and may significantly affect their rehabilitation process, as the juvenile moves through the system and long after they are discharged.

- This will also be an issue if a case results in a successful deferred disposition which results in the dismissal of the felony level offense and admission to a misdemeanor level offense.
- This will also be an issue in a case of a felony level offense that is “filed” by the prosecutor.
- What happens when a prosecutor changes the charges on a petition/indictment/etc.?
- What happens when a public case becomes non-public?
- What happens when there is a successful deferred disposition?
- What happens, in general, when a case is “filed” by the prosecutor?
- If a juvenile petition is dismissed by the prosecutor, what happens? Are records still accessible online? Is the outcome of the case reported through the digital case management system?
- Rule 1 promises “co-extensive” access whether records are sought at the courthouse or remotely... can someone remotely ask to have copies sent? By email? In the mail?
- Rule 2(a) says that “accessible by the public means” inspected or copied... what does this mean?

Thank you for the opportunity to provide feedback. We would welcome the opportunity to provide more detail.

Respectfully submitted on behalf of the work group,
 Jill Ward
 Maine Center for Juvenile Policy & Law
 University of Maine School of Law
 246 Deering Avenue
 Portland, ME 04102
 jill.ward@maine.edu
 (207) 780-4331
 (207) 317-6310 (cell)



Maine Center for
 Juvenile Policy and Law



Maine Freedom of Information Coalition

PO Box 232, Augusta, Maine 04332

March 27, 2019

VIA EMAIL

Matthew Pollack, Executive Clerk
Maine Supreme Judicial Court
205 Newbury Street Room 139
Portland, Maine 04112-0368

Re. Maine Freedom of Information Coalition's
Comments on Maine Digital Court Records Access Rules

Dear Mr. Pollack:

I am providing comments on the draft Maine Digital Court Records Access Rules on behalf Maine Freedom of Information Coalition ("MFOIC").

The MFOIC strongly endorses the Court's general public-is-public approach toward access to court records, but is concerned that (A) access be timely, as soon as reasonably possible after records are filed with the court; (B) that certain categorical exemptions to access are overbroad and unnecessary in all cases; (C) that the draft rule references an incorrect standard for granting and lifting seals on court records and that the referenced standard, if not revised, will lead to more secrecy in court records than constitutional and common law standards allow; and (D) that any fee schedule the court may adopt not become an unreasonable barrier to public access.

More broadly, the MFOIC favors a policy of maximum reasonable public access to Maine court records and proceedings. Public scrutiny improves judicial functions, enhances the actual fairness and, perhaps as important, the appearance of fairness of judicial proceedings. *See, e.g., Press-Enterprise Co. v. Superior Ct.*, 487 U.S. 1, 8-9 (1986).¹ Public scrutiny of what goes on in court "enhances the quality and safeguards the integrity of the factfinding process . . ." *Globe*

¹ Judicial proceedings "should take place under the public eye, not because the controversies of one citizen with another are of public concern, but because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed." *Cowley v. Pulsifer*, 137 Mass. 392, 394 (1884).

Newspaper Co., 457 U.S. 596 at 606 (1982). The public serves as a “check upon the judicial process – an essential component of our structure of self-government.” *Id.* “If public court business is conducted in private, it becomes impossible to expose corruption, incompetence, inefficiency, prejudice, and favoritism.” *Estate of Hearst*, 67 Cal. App. 3d 777, 784 (1977).

The Maine Freedom of Information Coalition is a tax-exempt Maine non-profit corporation dedicated to educating Mainers about their rights and responsibilities as citizens in our democracy and enhancing knowledge and awareness of the First Amendment and laws aimed at ensuring transparency in government. The members of the Coalition include the Maine Association of Broadcasters, the League of Women Voters of Maine, the Maine Library Association, the Maine Press Association, the Society of Professional Journalists, and a representative of academic/government interests.

The New England First Amendment Coalition is also a member of the MFOIC and joins in these comments. NEFAC is a broad-based organization of lawyers, journalists, historians, librarians and academics, as well as private citizens and organizations who believe in the power of transparency in a democratic society. The coalition aspires to advance and protect the five freedoms of the First Amendment, and the principle of the public’s right to know, in Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island and Vermont. In collaboration with other like-minded advocacy organizations, NEFAC also seeks to advance understanding of the First Amendment across the nation and freedom of speech and press issues around the world.

COMMENTS

Rule 1. Purpose and Applicability

The MFOIC agrees with the principle that “remote access to digital state court records . . . shall be co-extensive with access to such records at courthouses.” It is our understanding that Maine generally does not intend to maintain paper court files; records of court proceedings will be available digitally or not at all, with a few exceptions (e.g., protection from abuse proceedings).

Rule 2. Definitions.

Rule 2(g)(2)(H) makes confidential “[a]ny other court records maintained by the Judicial Branch not expressly defined as court records.” MFOIC suggests that this provision be removed for two reasons. First, it is potentially circular because court records are defined as “including, but not limited to” three categories of records but “other court records” not expressly defined as “court records” are exempt. This creates ambiguity. This could be addressed by removing the word

“court” from Rule 2(g)(2)(H), which would limit the scope of that provision to “other records” of the Judicial Branch.

As defined, “court records” are documents, etc. “received or maintained . . . in digital form . . .” MFOIC assumes that future amendments to the rules will require digital filing in virtually all state court proceedings. We suggest that court records be defined as all records “received, filed, or entered in the Registry of Actions” as this is more comprehensive and consistent with the language in draft Rule 3(c), below. Rule 3(c) uses the phrase “received, filed, or entered in the Registry of Actions” rather than “received or maintained.”

Rule 3. General Access Policy

MFOIC endorses prompt access to public court records and therefore questions the “no later than three business days” timeline for access to records after they are received, filed, or entered in the Registry of Actions by the court clerk, per draft Rule 3(c). We recognize that a brief interval of time may be necessary before a record is made public for newly filed cases to enable the clerk to establish a new case, assign a docket number, or otherwise create a new case file electronically. Once an electronic case file has been created, public access should be available as soon as technology permits and contemporaneous with the parties’ own access to the records. This is the way access works in federal court; access should not be delayed for docketing by the clerk’s office.

For the public and news media, an up to three business day wait is too long. The public has a strong interest in immediate (or as soon as possible) access to court records, including important court orders (e.g., injunctions against state officials), and information about filings of public interest (e.g., complaints of public interest and search warrant affidavits, after they are returned). A multiple business day wait for access to court records could result in a material gap between the effects of an injunction on public activities and public availability of a Superior Court order disclosing the basis for judicial action; this is untenable. The Law Court makes its decisions available very quickly (the same morning) after they are released to the parties. A similar or faster timeline for access to court orders and other case filings is warranted, as permitted by technology.

The importance of timely access to court records has been widely recognized. *See Int’l News Serv. v. Associated Press*, 248 U.S. 215, 235 (1918) (“The peculiar value of news is the spreading of it while it is fresh . . .”); *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 561 (1976) (“As a practical matter . . . the element of time is not unimportant if press coverage is to fulfill its traditional function of bringing news to the public promptly.”). “The newsworthiness of a particular story is often fleeting. To delay or postpone disclosure undermines the benefit of public scrutiny and may have the same result as complete suppression.” *Grove Fresh Distribs. Inc.*

v. Everfresh Juice Co., 24 F.3d 893, 897 (7th Cir. 1994). MFOIC respectfully submits that this precedent and First Amendment principles warrant access to public court records on an as-soon-as-possible basis.

Rule 5. Specific Information Excluded from Public Access

MFOIC recognizes that certain information should be redacted from otherwise public court records, but the proposed list of nearly thirty categories of information is overbroad. We suggest that Maine following the approach taken by the federal courts. Under Fed.R.Civ.P. 5.2 and Fed.R.Crim.P. 49.1, only four categories of information are excluded from public access: (A) all but the last four digits of social security numbers; (B) the year of an individual's birth; (C) minor names except for initials; and (D) the last four digits of financial account numbers. The only category on this list that is more restrictive than the draft Maine rule is dates of birth—under the draft rule only dates of birth of minors are excluded from public access. We suggest that Maine more closely follow the federal approach; inadequate justification is provided in the draft for deviating from that approach.

Our central concern is that these exemptions would apply categorically to every proceeding regardless of case-specific circumstances. Blanket exemptions should only apply to information that can with assurance be identified as confidential in every conceivable situation. Several of the exemptions may be justified in some situations, but not others and should be removed for this reason.

We request that the court remove from the list the following categories:

Rule 5(d)(1). The default rule should be that home addresses are public. Address information is important to positively identify a party to a proceeding. Many people share common names and can only be distinguished from one another by their address. Address information is generally public in Maine and available from municipalities' online tax records databases, among numerous other internet sources. The rule would leave work addresses public, but not everyone works, and some would presumably prefer to be contacted (if at all) at home rather than at work. As mentioned, addresses (work and home) are not confidential in federal court.

Rule 5(d)(4). MFOIC suggests that Maine follow the federal approach and require redaction of all but the last four digits of a social security number.

Rule 5(d)(5). MFOIC suggests that Maine follow the federal approach and require redaction of all but the last four digits of financial account and similar numbers.

Rule 5(f). Health information and medical records are generally public in court records. The comments suggest that HIPAA applies to court records. It does not.² A medical condition may be necessary to understanding the nature of a civil or criminal proceeding, including injuries to a victim or personal injury plaintiff or the mental state of a defendant. It may be appropriate to seal certain information in some medical records in some circumstances but sealing all “personal health information” and all “medical records” (neither of which are defined terms) could make a vast quantity of information confidential and render many important proceedings unintelligible. A headline reporting on a Maine case should not read, “Plaintiff alleges XXXXXX as a result of assault by John Doe, a resident of XXXXXX, who claims to have been suffering from XXXXXX at the time of the incident.”

Rule 5(l). Information made confidential under the Maine Criminal History Record Information Act is public if filed with the court in an otherwise public court record. The Criminal History Record Information Act does not apply to court records. See 16 M.R.S. § 708(3) (“This chapter does not apply to criminal history record information contained in . . . [r]ecords of public judicial proceedings . . . [r]etained at or by the District Court, Superior Court or Supreme Judicial Court.”). The Act is not a basis to make information in court records categorically confidential.

Rule 5(m). MFOIC suggests that financial information filed with the court to support the public benefit of a taxpayer funded counsel or waiver of court fees be made available to the public. This information serves as a check on the system and on representations made by parties to qualify for public benefits. Such information is now generally public.

Rule 5(q). Documents related to subpoenas for potentially privileged or protected documents should generally be public (e.g., the subpoena, any motion to quash, and any court order), with confidentiality extending only when necessary to information submitted for *in camera* review pursuant to applicable rules and to the extent the subpoena describes that information. The existence of such subpoenas and court orders related to them should be public.

Rule 5(s). See comment on Rule 5(q).

² See, e.g., <https://www.hhs.gov/hipaa/for-professionals/faq/judicial-and-administrative-proceedings/index.html>.

Rule 7. Impounding or Sealing Public Cases, Documents, or Information From Public Access

The MFOIC generally agrees with the procedural aspects of draft Rule 7 (e.g., the need to file a motion and affidavit). We also suggest that the Rule be revised to require specific on-the-record findings whenever a motion for a seal is granted.

We respectfully disagree, however, that the standard for sealing or impounding court records should be a balancing test weighing “a reasonable expectation of privacy” against “public interest in transparency.” We suggest that the court remove the second paragraph of Rule 7(a), which refers to this test.³ The privacy/public interest balancing test in the draft rule does not comport with either the First Amendment or common law standard for sealing otherwise public court records. Under both the First Amendment and the common law, a party moving to seal public court records bears the burden of showing that a seal is necessary to serve a compelling interest and that the seal is narrowly tailored to serve that interest.

The Law Court has suggested that “non-disclosure of judicial records could be justified only by the most compelling reasons.” *Bailey v. Sears, Roebuck & Co.*, 651 A.2d 840, 844 (Me. 1994). Earlier in *Maine Auto Dealers Assn. v. Tierney*, 425 A.2d 187, 189 n.3 (Me. 1981), the Court wrote, “Although under appropriate circumstances a court may impound records when publication would impede the administration of justice, the power of impoundment should be exercised with extreme care and only upon the clearest showing of necessity.” *Maine Auto Dealers Assn. v. Tierney*, 425 A.2d 187, 189 n.3 (Me. 1981) (citation omitted). The standards articulated in these cases, the “most compelling reasons” and “extreme care and only upon the clearest showing of necessity,” diverge from the standard referenced in draft Rule 7(a).

Under the First Amendment, which has been repeatedly held to protect the right of the public and the news media to access criminal and civil proceedings (including records),⁴ “The presumption of openness may be overcome only by an

³ The MFOIC’s understanding is that the court intends to adopt one standard for sealing (and unsealing) court records; the same standard would apply whether the records are digital or paper in accordance with Rules 7 and 8.

⁴ Federal appellate courts have widely recognized that this First Amendment right extends to civil proceedings. “Every circuit to consider the issue has concluded that” the “right of public access applies to civil as well as criminal proceedings.” *Dhiab v. Trump*, 852 F.3d 1087, 1099 (D.C.Cir. 2017); *see also Courthouse News Service v. Planet*, 750 F.3d 776, 786 (9th Cir. 2014) (“the federal courts of appeal have widely agreed that [the First Amendment right of access] extends to civil proceedings and associated records and documents”); *In re Boston Herald, Inc.*, 321 F.3d 174, 182 (1st Cir. 2003) (explaining that the First

overriding interest based on findings that closure is essential to serve higher values and is narrowly tailored to serve that interest.” *Press-Enterprise Co. v. Superior Ct.*, 464 U.S. 501, 510 (1984); *see also Globe Newspaper Co. v. Superior Ct.*, 457 U.S. 596, 606-07 (1982) (“to deny the right of access in order to inhibit the disclosure of sensitive information, it must be shown that the denial is necessitated by a compelling governmental interest, and is narrowly tailored to serve that interest”). The Law Court has applied the same standard to criminal trial proceedings. *See Roberts v. State*, 2014 ME 125, ¶ 26, 103 A. 3d 1031 (“It is true that a ‘presumption of openness’ attaches to every stage of a criminal trial, including jury selection, and that the presumption may be overcome only by ‘an overriding interest based on findings that closure is essential to preserve higher values and is narrowly tailored to serve that interest.’”); *State v. Frisbee*, 2016 ME 83, ¶ 22, 140 A.3d 1230 (court may not seal criminal proceedings absent a showing that the party seeking to close the hearing has advanced an overriding interest that is likely to be prejudiced, the closure is no broader than necessary to protect that interest, reasonable alternatives to closing the proceeding have been considered, and adequate findings have been made to support the closure).

The common law also protects the public’s right of access to court records. The Supreme Court has recognized that “historically both civil and criminal trials have been presumptively open.” *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580 n.17 (1980). The same is true of records. *See Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597 (1978) (“the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents”). The New Hampshire Supreme Court observed that “[t]he public right of access to court proceedings and records pre-dates the State and Federal Constitutions and is firmly grounded in the common law.” *Associated Press v. State*, 153 N.H. 120, 125 (2005). “This appears to be the almost universal rule dating from the earliest times.” *Id.* The right to access court records in what is now Maine stretches back as far as the Massachusetts Body of Liberties (1641),⁵ art. 48, which provided, “Every inhabitant of the Country shall have free libertie to search and veewe any Roolles, Reocrds, or Regesters of any Court or office except the Counceil.” This common law right of access is not “not coterminous” with the First Amendment, but “courts have employed much the same type of screen in evaluating their applicability to particular claims.” *In re Providence Journal Co.*, 293 F.3d 1, 10 (1st Cir. 2002). If the draft Rule references a standard for sealing otherwise public court records, then the standard should be the First Amendment/common law standard. The burden is on the party requesting a seal to

Amendment right of access attaches to proceedings “open to the public in the past” and those for which “public access plays a significant positive role”).

⁵ The Law Court has cited the Body of Liberties of 1641 as a widely recognized early compilation of the common law. *Bell v. Town of Wells*, 557 A. 2d 168, 182 (1989).

show that a seal is necessary to serve a compelling interest and that the seal is narrowly tailored. This is not, however, what draft Rule 7(a) says.

In narrow circumstances an individual's interest in personal privacy may be enough to seal otherwise public court records (e.g., juror identities may be redacted from transcripts of voir dire to the extent jurors are questioned about highly personal and private matters), but MFOIC is concerned that "reasonable expectations of privacy," the language used in the draft rule, suggests that generalized privacy interests may be sufficient to seal court records. The opposite is true; except in rare circumstances privacy interests are insufficient to seal court records. *See, e.g., Siedle v. Putnman Investments, Inc.*, 147 F.3d 7, 10 (1st Cir. 1998) ("The mere fact that judicial records may reveal potentially embarrassing information is not in itself sufficient reason to block public access."); *Doe v. Heitler*, 26 P.3d 539, 544 (Colo. App. 2001) ("A claim that a court file contains extremely personal, private, and confidential matters is generally insufficient to constitute a privacy interest warranting the sealing of the file."); *Doe v. New York Univ.*, 786 N.Y.S.2d 892, 902 (N.Y.Sup. 2004) ("embarrassment, damage to reputation and the general desire for privacy do not constitute good cause to seal court records"); *Ex parte Capital U-Drive-It, Inc.*, 369 S.C. 1, 630 S.E.2d 464 (2006) ("Litigants who carry disputes to a publicly funded forum for resolution must necessarily expect to surrender a good measure of their right to privacy."); *see also Associated Press v. State of New Hampshire*, 153 N.H. 120, 133 (2005) ("We are concerned that limitations on access to serve privacy interests comes at too high a cost to accountability and all the benefits associated with transparency.").

The MFOIC suggests that the Court replace the privacy/public interest balancing test with a standard that comports with prevailing law on sealing court records.

Rule 8. Obtaining Access to Impounded or Sealed Cases, Documents, or Information

The MFOIC agrees that nonparties seeking access to an impounded or sealed public case, document or information should be considered a party in interest and that due process should be afforded to all parties to the proceeding when a motion for access has been filed. *See* Rule 8(a)-(b).

The MFOIC agrees that a motion for access should be granted upon a showing of good cause, the standard referenced in draft Rule 8(c). While the exact standard for modifying a protective order is not clearly defined in Maine or the First Circuit, federal courts often apply a "good cause" standard to modify protective orders. *See OfficeMax, Inc. v. Sousa*, 2011 WL 143916, at *2 (D. Me. Jan. 14, 2011); *see also Fairchild Semiconductor Corp. v. Third Dimension Semiconductor, Inc.*, 2009 WL 1210638, at *1 (D. Me. Apr. 30, 2009) ("Fairchild, as the party seeking to

modify the protective order, bears the burden of showing good cause for the modification.”). “To determine ‘good cause,’ a court must balance various factors, including change in circumstances, parties’ reliance on the protective order, and third-party privacy interests.” *United States v. O’Brien*, 2014 WL 204695, at *4 (D. Mass. Jan. 17, 2014); citing *United States v. Bulger*, 283 F.R.D. 46, 53-55 (D.Mass.2012)).

But to determine whether “good cause” has been shown, Rule 8(c) requires that a court consider whether public access and privacy interests have been served *and* whether the moving party or party in interest has demonstrated either: “extraordinary circumstances” or that the “public interest in disclosure outweighs any potential harm in disclosure.” Because “extraordinary circumstances” is not the correct test for lifting an order impounding or sealing court records, MFOIC suggests that it be removed from the draft. The First Circuit has held that something *less than* extraordinary circumstances is sufficient to modify protective orders. *See Pub. Citizen v. Liggett Grp., Inc.*, 858 F.2d 775, 791–92 (1st Cir. 1988) (“While we need not decide the matter definitively, we reject the ‘extraordinary circumstances’ standard. In a case such as this, where the party seeking modification has pointed to some relevant change in the circumstances under which the protective order was entered, we think that a standard less restrictive than ‘extraordinary circumstances’ is appropriate. We need not define how ‘less restrictive’ the standard should be because we find that under these facts the district court had the legal power to modify its prior protective order: the reasons underlying the initial promulgation of the order in respect to the particular document sought no longer exist; and the district court made a reasoned determination that public interest considerations favored allowing counsel to make those particular documents public.”).

The other standard (balancing public interest against potential harm) is a reasonable factor, but should not be made the exclusive one for determining good cause. If a seal would not serve a compelling government interest (or if the interest is no longer compelling after the passage of time), that should be sufficient to establish good cause to obtain access. If a seal is overbroad (not narrowly tailored to serve a compelling interest), that also should be sufficient to establish good cause to narrow or remove a seal on court records. Because of the range of circumstances and variety of situations that may arise, MFOIC suggests that the court leave the applicable standard at “good cause.”

Rule 11. Fees

The Court reserves the authority to establish a fee schedule. In developing a schedule, the MFOIC suggests that the Court consider the policy arguments related to fees for access to federal court records raised in briefing in connection with

Matthew Pollack, Executive Clerk
March 27, 2019
Page 10

litigation challenging the fees charged for records through the Public Access to Court Electronic Records system ("PACER").

The Reporters Committee for Freedom of the Press and 27 media organizations recently filed an amicus brief addressing the benefits of affordable access to court records. See <https://www.rcfp.org/media-groups-advocate-for-affordable-access-to-court-records/> Seven prominent federal judges also filed an amicus brief arguing that PACER should be free. See <http://www.abajournal.com/news/article/pacer-should-be-free-according-to-amicus-brief-by-posner-and-six-other-retired-judges> The American Bar Association has endorsed free access to PACER. *Id.*

The MFOIC suggests that public access to court records be free or, if a fee-for-service model is deemed necessary, as inexpensive as reasonably possible.

CONCLUSION

Thank you for the opportunity to comment on these important rules. As I am the point person for MFOIC on these rules, please contact me with any questions or follow-up at 207-791-3000 or sschutz@preti.com.

Very truly yours,



Sigmund D. Schutz

SDS:jac

cc: MFOIC Board of Directors (*via email*)
Jonathan Silverman, Executive Director,
New England First Amendment Coalition (*via email*)

MITTEL ASEN, LLC

ATTORNEYS AT LAW
www.mittelasen.com

ROBERT E. MITTEL
MICHAEL P. ASEN
DIANE DUSINI
JONATHAN L. GOLDBERG
SUSAN S. BIXBY
MARIA FOX
HEATHER T. WHITING
WILIAM LEETE

85 EXCHANGE STREET, 4th FLOOR
PORTLAND, MAINE 04101

PHONE 207 775-3101
FAX 207 871-0683

March 27, 2019

Matthew Pollock
Clerk, Supreme Judicial Court
Portland, ME

Via email only

RE: Digital Court Records Proposed Rules

Dear Pollock:

Set out below are my suggested changes to or comments about these proposed rules.

1. I think the Court should state at the outset of Rule 1 that the public has a right of access to judicial records with which these rules and future court orders can narrow or deny only with a showing of a compelling governmental interest that is exercised in a narrowly tailored manner. That is the standard applied in the controlling cases.

2. Therefore, the language of Rule 7 should be changed as follows.

In weighing a reasonable expectation of privacy against the *compelling* public interest in the transparency of court records, the court shall consider whether an individual's personal safety, health, or well-being, or a substantial personal, business, or reputational interest outweighs *that compelling* public interest in the information in the court records. *Any such sealing order shall require the sealing of only the minimum amount of the record as is necessary to meet that standard.* (changes in italics)

Such a Motion shall be resolved in no more than 30 days following its filing. There shall be a presumption against the

granting of such Motions when they seek to seal an entire case file.

3. If I understand correctly, the Registry of Actions defined in Rule 2(k) is part of the record. It should never be sealed in civil or divorce actions and I am not sure that the rules as proposed make that point with sufficient clarity.

4. The changes to the FM Rules require the filing of a summary complaint and answer which would remain public along with a summary of the final judgment. I think that Rule 7 should be amended with language requiring the preparation of such documents, which would always be public along with the Registry of Actions, in the extremely unusual circumstance where an entire case is sealed.

5. It is unclear how cases that are now pending in County X will be handled as County X goes on line.

Thank you.

Very truly yours,

Robert Edmond Mittel

Robert Edmond Mittel
email: rmittel@mittelassen.com
207 699 5730

REM:rem



MCKEE LAW

133 State Street, Augusta, Maine 04330
207-620-8294 FAX 207-620-8297

Walter F. McKee • Melissa Reynolds O'Dea • Matthew D. Morgan
Henry E. M. Beck

March 11, 2019

Matthew Pollack, Executive Clerk
Maine Supreme Judicial Court
205 Newbury Street, Room 139
Portland, ME 04112-0368

Re: Maine Digital Court Records Access Rules

Dear Mr. Pollack,

I am writing to provide comments for the Maine Digital Court Records Access Rules. In particular I am writing in regard to proposed Rule 6. I am writing specifically about the final paragraph of Rule 6 which specifically makes family matter proceedings not accessible to the public except for the limited summary information provided in Rule 10.

The current system here in the state of Maine allows for attorneys as well as the public to request family files at any Clerk's window across the state for purposes of reviewing the files. It is often the case, for example, that attorneys handling criminal or protection from abuse matters may also wish to review family matters that contain relevant information for those cases. It also is the case that sometimes parties who remarry may marry a new partner and if information about that new partner's finances are pertinent to a post-judgment divorce matter, then sometimes the only way those materials can be obtained is through a subpoena or through review of other court records that already discuss that new partners' finances. Finally, the public simply has a right to request this information if it's interested in how courts handle important social issues such as custody and child or spousal support where they live.

Particularly sensitive data, such as Guardian *ad Litem* reports, personal identifying information, and tax records are all kept separate in the court file and Clerks will not allow attorneys or members of the public to review this information. This is the system that currently exists.

For reasons that are at least not articulated in this rule, the new system will be the exact opposite. Attorneys in the public will no longer be permitted to access any of the documents in family law cases other than the very basic summary information allowed under Rule 10. It has been indicated at meetings about the Digital Rules that the reason for this change has to do with the possible ease of disseminating information once it's made electronic. The reality, however, is that the parties most likely to abuse this information are the opposing parties in the case and they have the ability to photocopy or take pictures of these documents at any time and send them by email or text to

Page 2 of 2
March 11, 2019

whomever they may wish. These parties will still have the ability to do so under the draft rules. The only change now is that all public access to this information is lost.

Family courts serve an important public function and litigants are aware that family proceedings are open to the public unless specifically excluded by rule. The public's access to these documents should not change now that the Court system is transitioning to a digital format.

Far less severe solutions to the concern about electronic information being disseminated are available. In particular, specific watermarking could be placed on documents identifying the party who digitally accessed them. In addition, anyone accessing these materials can be required to sign off on user terms of agreement prohibiting their misuse of the records. A complete 180 from full access to no-access, even if done for only a temporary period while developing solutions, is not the answer to this concern.

In the event these rules maintain the framework whereby family matter actions are treated as non-public in nature, then some exception must be made so that attorneys and self-represented litigants have the ability to request documents that are necessary for the kinds of related litigation discussed above. It would be best if the system allowing such access is streamlined and does not require a party to reveal a significant amount of his or her strategy to opposing counsel when requesting access to these documents. My recommendation would be an amendment to Rule 2(j) to add an additional category of persons who are not considered "public" to include persons who can demonstrate the possible existence of relevant information in the non-public FM file in some currently pending or anticipated litigation. If such an exception is made, then it would likely be advisable for a form to be created so that *pro se* litigants were able to make use of this exception as easily as attorneys.

Thank you for considering my written comments.

Sincerely,



Matthew D. Morgan
mmorgan@mckeelawmaine.com
MDM/mer/



March 27, 2019

Matthew Pollack, Executive Clerk
Maine Supreme Judicial Clerk
205 Newbury Street, Room 139
Portland, ME 04112-0368
lawcourt.clerk@courts.maine.gov

Re: *Draft of Maine Digital Court Records Access Rules*

Dear Mr. Pollack:

On behalf of the Maine State Bar Association (MSBA), we appreciate the opportunity to provide comments concerning the draft of the new Maine Digital Court Records Access Rules. Overall, the MSBA supports the draft as written. However, we ask for consideration of the following proposed amendments to make clear possible issues that could arise upon implementation.

1. Rule 2(g)(2)(C) should include briefs submitted for judicial settlement conferences.
2. Rule 2(g)(2) should include a category for information submitted for foreclosure mediations.
3. Rule 5(q) protects from disclosure certain subpoenas. It is not the subpoenas themselves that should be shielded, but rather the information produced in response to the subpoena that requires protection.
4. Rule 7 provides a procedure for having documents impounded or sealed that requires the submission of a motion and an affidavit. That motion and affidavit will themselves often need to be sealed, which creates an infinite recursive loop of motions to seal. We therefore propose that the motion to impound or seal should be automatically impounded/sealed itself until ruled upon.
5. Rule 8 provides a method for a party to the case to access sealed documents. We question when that scenario would arise given that sealing a document prevents the public from viewing it, not another party. We believe this needs further clarification, or is not necessary.
6. Rule 8(b) refers to "affected persons," which is not a defined term. This term should be defined.
7. The test for sealing in Rule 7(a) is different from the test for unsealing in Rule 8(c). We suggest making the tests consistent to avoid ambiguity or confusion, or add an explanation as to why the tests are different.
8. Rule 9 should more clearly explain that nonpublic information in a document may simply be redacted as opposed to sealing an entire document as a whole.
9. Rule 11 should limit the Judicial Branch to charging fees that are directly related to the cost of storing and producing the records.

Thank you again for the opportunity to comment on these important Rules. Please don't hesitate to contact me if you have any questions.

Sincerely,

Eric N. Columer, President
Board of Governors

124 State Street | Augusta, Maine 04330
T 207.622.7523 | F 207.623.0083 | info@mainebar.org | www.mainebar.org

COMMENTS RELATED TO PROPOSED DIGITAL COURT RECORD ACCESS RULES
SUBMITTED BY LAURA M. O'HANLON MARCH 27, 2019

To the Honorable Justices of the Maine Supreme Judicial Court:

Thank you for the opportunity to provide feedback on the proposed Digital Court Record Access (DCRA) Rules. My comments consist of several parts: an outline of key points followed by four Appendices and Attachments (Appendix A poses some of the questions that are not answered by the proposed DCRA Rules; Appendix B details specific recommendations related to individual provisions in the draft Digital Court Record Access Rules; Appendix C contains possible amendments to the Maine Rules of Civil Procedure designed to address concerns or facilitate some of the suggestions contained in these materials (which I plan to share with the Civil Rules Advisory Committee); Appendix D attempts to identify similar Unified Criminal Procedure issues; and Appendix E provides links to selected state resources.)

I submit these resources in my personal capacity as a member of the Maine bar and not on behalf of my employer.

Introduction

In keeping with its mission of providing an impartial and effective dispute resolution system that instills public trust and confidence, the Maine Judicial Branch must make its operations transparent, but it must also provide safe and accessible processes for people. While much work has been done to gather specifications, look at process improvement, and develop legislative proposals and rules, there is no description of an effective mechanism for individuals (and businesses), especially nonparties, to understand the potential risks and learn how to seek protection of their privacy from the courts.

To provide the best possible outcome for litigants, justice partners, the court system, and the public, I recommend the Court post the details of its plan, gather stakeholders, and undertake study this issues even if doing so postpones the roll out. Alternatively, the Court should reconsider the timetable for fully implementing this important initiative. For example, rather than allowing remote online access from inception, the Court might start with “courthouse access only” replicating what is available currently until all (or several) regions are on line. Such an incremental approach would allow parties, lawyers, and members of the public to have prompt access while the court system learns more about benefits and risks of this “new to Maine” technology. As the Judicial Branch learns more through an iterative process, the bar becomes more familiar with the system, and the technological tools are tested in Maine, the Court should re-evaluate the approach and make adjustments to the process.

Justice Requires Access to a Meaningful Opportunity to Seek Protection

Standing alone, the proposed DCRA Rules do not provide sufficient guidance to allow unrepresented litigants to navigate a complicated legal system made more complex by a digital overlay. For some, the use of technology will help; however, it is difficult to imagine how persons unfamiliar with the court system (especially those with lower literacy skills, mental challenges, or limited English proficiency) will understand the potential risks of releasing private information, and the procedures available to seek protection of their own sensitive information and that of others. Prior to implementation of remote online access, however, it is imperative that the Court fashion a solution to this key issue.

If public documents are going to be posted online within three days of filing (or receipt or docketing) as suggested by DCRA Rule 5(c), the process identified in DCRA Rule 7 may be entirely ineffective for parties and nonparties to prevent broad public disclosure.¹ Under the draft rules, there is just not enough time for parties to react. In order to have a meaningful opportunity to ask the court to protect information, the people whose information is going to be posted must be made aware of the fact that it will be posted and given a chance to respond.

One way to mitigate the harmful effects of this issue for parties is to delay posting of court record information until after judicial action or when component parts of a case are ripe for judicial action.² For example, in a civil case, a complaint cannot be acted upon until the defendant's response has been filed or any other time for response has passed.³ Thus, the complaint and answer, or complaint and default would be posted together. Under such a system, the public would have more complete information about the case; and parties would have more time to seek court review of information or resolution of privacy disputes; or at a minimum, the chance to respond to allegations in writing.

¹ As noted in my January 25, 2019 comments related to a similar legislative proposal, a plaintiff in a civil case who waits 90 days after filing to serve the defendant (as authorized by Maine Rule of Civil Procedure 3 (and 14 M.R.S. § 553)) may make the defendant's chance to request to seek protection irrelevant. (Appendix C, Attachments C-1 & C-2, address this specific concern).

² Exceptions to this policy could be granted for "high profile" cases or cases involving public figures, if after weighing facts and circumstances of the individual case, the judge determines that it is appropriate to do so or pursuant to criteria proposed by the Media and the Courts Committee and adopted by the Supreme Judicial Court in an Administrative Order or policy.

³ Similar to the process outlined for Family Matters (Digital Court Record Access (DCRA) Rule 10), the court system could post online limited information describing the type of complaint filed with summary demographics and a timeline for response to provide notice of actions.

COMMENTS RELATED TO PROPOSED DIGITAL COURT RECORD ACCESS RULES
SUBMITTED BY LAURA M. O'HANLON MARCH 27, 2019

Beyond those who are parties or actively involved in a case, it is unclear how nonparties will become aware that their personal information is available via remote online access.⁴ Or, how the Maine Judicial Branch will protect their privacy. These individuals may include witnesses who agreed to cooperate with law enforcement in investigating incidents; neighbors, family members of victims or the accused; good samaritans who acted to provide aid to others; or actors who have a limited but an important role in the lifecycle of a lawsuit. Nonparties may face even greater challenges and are even more vulnerable in the publication of electronic information as parties pursue their own adversarial interests without any awareness or obligation to safeguard the specific privacy concerns of others. *See, e.g., Public Citizen v. Liggett Group, Inc.*, 858 F.2d 775, 784 (1st Cir. 1988) *citing Beef Industry Antitrust Litigation*, 589 F.2d at 789 (5th Cir. 1979), cert. denied, 488 U.S. 1030, 109 S. Ct. 838, 102 L. Ed. 2d 970 (1989); Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 St. Louis U. Pub. L. Rev. 63, 63-67 (2006) (courts have a “special obligation to protect the public's interest in individual privacy” with respect to government records).

Who will protect non-party interests? Who will ensure that these individuals are not put at risk or subjected to embarrassment or harassment? Who will provide notification so that they may request that their sensitive information be kept out of the public view, particularly if such information is not necessary to the resolution of the disputes at issue? Historically, “courts [have been and will continue to need to be] sensitive to protect... the harm that can come to... third parties, who may have no control over the information so disclosed[,]” and who may have “never intended” their information be released in an electronic record. Peter A. Winn, *Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information*, 79 Wash. L. Rev. 307, 312, 321 (2004).

Many suggest that the solution lies in technology—in the promise of redaction tools. The Judicial Branch should take advantage of the redaction tools offered as part of Tyler’s product line, which will help. Given my own experience in reading hundreds of “unrepresented missives,” and the state of such technology, however, I am skeptical that software will provide an effective or comprehensive near-term solution. Until the vendor can assure 100% compliance with Court mandates, the Court must find other solutions.

Of course, the Court may decide to require lawyers and unrepresented litigants to safeguard the information of others through redaction or by providing notice to victims, witnesses, bystanders, and others.⁵ Or, judicial officers could be charged with the responsibility for reviewing court records and ordering (sua sponte) impoundment or sealing of information if the public interest is served by prohibiting access; access to such information will create significant risk of harm to requester, other persons, or general public; or there will be substantial prejudice to ongoing proceedings without such protections. *See* suggested revision to DCRA Rule 7(a) in Appendix B.

⁴ Arguably sections of DCRA Rule 5 (p)(q)(s) protect nonparty interests in specific circumstances, but there are no overarching or broad provisions relating to the protection of nonparty information in court records.

⁵ In addition, the Court should promulgate rules punishing lawyer and party misconduct (some examples of amendments to the Civil Rules appear in Appendix C).

Under the first scenario, prosecutors and other attorneys would appropriately complain about the added workload. It would create a burden. It would take extra time; presumably clients would pay for that time. It would bring with it some potential ethical dilemmas. For most unrepresented parties, this would require a better understanding of court process and tremendous training. For many lawyers, this would require new awareness and tremendous training.

With the second alternative, already overworked judges would be asked to spend their time on important but granular tasks.

As an alternative, the court system could hire staff members⁶ (e.g., redaction specialists, legal process specialists, or specialized clerks) to review information before it is posted. However, review of the court record access cases being litigated in the federal courts⁷ demonstrates that such post-filing staff reviews lead to delays, which may or may not run afoul of First Amendment or common law access rights.

Other states have fashioned solutions that allow for transparency of court operations while protecting privacy without making “remote access to digital state court records as provided by [the DCRA Rules ...] co-extensive with access to such records at the courthouses.” DCRA Rule 1. Some, including Indiana, Massachusetts, Missouri, and Oregon, do not rely on remote online access as the sole source of public access to court records. Instead, those courts provide timely public access to court records at the courthouse (in paper or at terminals or kiosks). (See Appendix E for state court links).

The Court should implement similar appropriate time, place, and manner restrictions on the broad release of court record information and be sure that all people (and businesses) have a notice and a fair chance to seek the court’s protection. Maine must find ways to protect those who did not choose to be in court and those who are most in need the court system’s protection.

Finding the right solutions will take creativity and time.

⁶ While it is likely that the reduction in data entry will lead to the ability to reassign current staff members to new functions, at the beginning of this project, it is unlikely that such a reallocation of resources will be possible or happen evenly. To facilitate this tremendous undertaking, the Judicial Branch should consider seeking authorization for new staff positions.

⁷ See, e.g., David Ardia, *Court Transparency and the First Amendment*, 38 *Cardozo L. Rev.* 835, 875 (2017).

Court Record Issues are Being Presented to the United States Supreme Court

Taking more time may be prudent given expected changes in the legal landscape.

It may take a while for them to get there, but with each new decision, the federal courts are creating an opportunity for the United States Supreme Court to begin addressing court record issues. Soon, the highest court may agree to address a foundational issue about which courts should resolve court record access disputes. Much could change if the Court accepts the invitation and resolves the abstention issue.

For years, access to court record issues have been actively debated in federal courts across the United States. *See, e.g.,* David Ardia, *Court Transparency and the First Amendment*, 38 Cardozo L. Rev. 835, 875 (2017). There is a sufficient split of authority among the circuits and the reasoning within the opinions differs widely. *See id.* Eventually, the United States Supreme Court may be called upon to decide the issues. *See id.*

Additionally, Courts of Appeal are divided over whether federal courts should abstain from hearing First Amendment claims related to state court record access and the United States Supreme Court has been asked to resolve the conflict. In late 2018, the Seventh Circuit Court of Appeals determined that in the interest of comity, a First Amendment suit against Dorothy Brown, Chicago's elected court clerk, should not be considered by the federal court. *Courthouse News Serv. v. Brown*, No. 18-1230 (Nov. 13, 2018). The *Brown* decision runs contrary to *Courthouse News Serv. v. Planet*, 750 F.3d 776, 793 (9th Cir. 2014) within which the Ninth Circuit Court of Appeals determined that the federal court's power to decide constitutional matters extends to state court policy and *Hartford Courant Co. v. Pellegrino*, 380 F.3d 83, 100 (2d Cir. 2004) within which the Second Circuit rejected the argument that a challenge to the Connecticut courts' procedures for sealing court documents affected "a central sovereign function" over which state courts had "an inherent power."

Last week, a petition for certiorari was filed in the United States Supreme Court as a result of the Seventh Circuit's ruling in *Courthouse News Serv. v. Brown*, 908 F.3d 1063 (7th Cir 2018),⁸ asking the United States Supreme Court to determine "whether *Younger* and its progeny permit federal courts to abstain, on the basis of general principles of comity and federalism, from hearing First Amendment challenges that seek access to state court filings."

The legal landscape is evolving. This Court should consider building a longer bridge from paper to electronic records access that will allow for more public awareness and planning, and that will minimize the need for substantial retreat or renovation following any new legal pronouncements.

⁸ This debate continues in the district courts. For example, just last week, the Honorable Henry Coke Morgan Jr., judge of the Eastern District of Virginia, resolved preliminary motions in an action brought by Courthouse News Service against two court clerks in Norfolk and Prince William counties in Virginia. In his opinion, Judge Morgan rejected the *Brown* rationale regarding abstention stating, "Federal courts have a virtually unflagging obligation to exercise the jurisdiction given to them." *Courthouse News Serv. v. Schaeffer*, 2:18-cv-00391-HCM-LRL at 16 (E.D. Va. March 18, 2019).

Closing Thoughts

Given the numerous questions that remain unanswered, the need for lawyer engagement, and the developing jurisprudence, the Court should follow a less aggressive timeline for the digital transformation, especially providing remote online access.

It is time for the Court to be transparent about its plan for future operations. To be successful, the Court will need to provide clear public information and garner the cooperation of Maine lawyers. A year will be gone before we know it.

The Court should announce the details and seek more feedback. Now is the time to gather the most useful information and informed suggestions, and to be sure that the bar is ready to assist their clients and the Judicial Branch in this major undertaking. And, there needs to be a plan to assist unrepresented litigants in the digital age.

Implicit in my comments and these recommendations is a desire to reduce the possibility that the Maine Judicial Branch and members of the bar will spend great time and effort heading in one direction only to find that a slightly slower more incremental approach would have yielded greater advancement in the future.

As always, if I can be of assistance, please let me know.

Respectfully,

Laura

Laura M. O'Hanlon, Esq.
Bar # 7589
l.ohanlon@aol.com

APPENDIX A—SOME GENERAL QUESTIONS ABOUT DIGITAL COURT RECORD ACCESS

Related to DCRA Rules 2 (g), 5, & 6

Will audio/video recordings or transcripts (the official record) be public documents even in non-public case types? When transcripts or audio recordings are available to the public, how will any individual information that has been designed as non-public be identified and protected? (e.g., if witness testimony includes elements that would be protected pursuant to DCRA Rule 5) If not, will the existence of those records allow for re-identification of parties or redacted information in the online records?

Related to DCRA Rule 1 indicating the county probate courts are not included in these rules

How will the State Court system treat Probate Court or Federal Court pleadings that were subject to different rules when they are transferred to the State Courts? How will the state court system treat Federal Court pleadings filed in the trial courts? Who will undertake the review to assure that non-public information is not posted online or otherwise inappropriately made public?

Related to DCRA Rules 5, 6, 7

May parties “agree” to exclude information from public access through protective orders or other agreements? Or, may parties waive the protections of Rules 5 & 6 by agreement? Does this require an amendment to the DCRA or other procedural rules.

General:

Are the Digital Court Record Act (DCRA) Rules applicable to Appellate Proceedings? If so, are there any new requirements related to briefs filed in nonpublic cases? Are there any changes to the requirements related to what may be included in the Appendix? Or, related to the preparation of the record (by the parties or trial court clerks) on appeal? If the DCRA Rules apply to appeals how will the Court protect information that is submitted through Probate Court matters that are appealed to the Law Court?

How will search functions be structured? (e.g., will searchers need to know docket numbers or party names to search or will there be more general search capabilities?) How will the information be displayed? (e.g., full documents capable of being captured and retransmitted or pieces of documents that can be viewed in their entirety but not easily reposted?)

How long will information remain available? Is there any archival policy for digital information?

Do the DCRA rules apply to exhibits, such as government records or business records, that contain information essential to the case but may not comply with DCRA Rule requirements in their original form?

How will the Court effectuate the purpose of expungement orders, where newly expunged records were previously posted on the internet? Similarly, how will pardons be treated?

What is the effect of these rules on cases filed prior to the effective date of DCRA Rules? Are records that were public and in existence prior to DCRA Rules be subject to the DCRA requirements? How will those records be treated?

**APPENDIX B- SELECTED COMMENTS REGARDING
SPECIFIC DIGITAL COURT RECORD ACCESS RULES**

I. DCRA Rule 2(j)(2)(C)(D)(E)

See suggested new DCRA Rule 13 in Attachment B-1 (described below)

For entities authorized by law or rule, the court should require some form of nondisclosure agreement or certification of confidentiality.

II. Clarification of DCRA Rule 3

As written subpart (c): “Unless otherwise ordered by the court, a digital court record accessible to the public shall be available no later than three business days after it is received, filed, or entered in the Registry of Actions by the court clerk” does not clearly identify when the information will be made public. (*e.g.*, Is this intended to vary depending on case type? Or is three business days after the last one of these events? Does the clerk have discretion to delay entering pleadings into the Registry of Actions?)

III. Suggested Revision to DCRA Rule 5

Rule 5(b)(c)

This suggestion relates to the discussion of images of minors in the rules as referenced on pages 7, 14, & 17. Rule 5(b)(c) describes images also referenced in 17-A M.R.S. §511-A, but later on pages 14 & 17 names and images of a minor are described more generally. For the avoidance of doubt, I suggest that Rule 5(b) contain the broadest description rather than the narrower description

Rule 5(d)

Amend subpart (2) to include

“residential addresses unless necessary to resolution of the litigation”

Broaden subpart (8) to protect: “DNA-identifying data or other biometric information”

Reconsider broad availability of full birth dates. While there may be some industries that require full birthdates and there may be some instances where it would be of benefit to the party in question to have the full date of birth published, there are significant risk of identity theft related to this identifier.

Additions to Rule 5

(v) Oral statement(s) (contained in the transcripts) that relate to information shielded from public access pursuant to Rule 5 and transcripts in matters excluded from public access pursuant to Rules 6 & 7 of these Rules or otherwise impounded or sealed by the court.

(w) A document, pleading, or exhibit tendered or admitted into evidence during an *in camera* review that is not subsequently entered into the record.

(x) Information related to requests for disability accommodations filed with an individual court or otherwise submitted to the Judicial Branch that becomes a part of the Court Record.

(y) documentary evidence or orders from another court or tribunal containing information that would be excluded from public access pursuant to these Rules.

**APPENDIX B- SELECTED COMMENTS REGARDING
SPECIFIC DIGITAL COURT RECORD ACCESS RULES**

IV. DCRA Rule 6
Rule 6(d)

It is unclear to me whether 6(d) juvenile proceedings refers only to those matters arising under the Juvenile Code, 15 M.R.S. §§ 3307-3308, as suggested by the Drafter's Notes to Rule 6 (d) on page 17 or whether this can be read more broadly to include other proceedings involving minors that arise outside of the Juvenile Code (e.g., civil violations involving minors). In accordance with current research regarding brain development and from the justice community, "[j]uvenile records should not be public records. Access to and the use of juvenile records should be strictly controlled to limit the risk that disclosure will result in the misuse or misinterpretation of information [and] the unnecessary denial of opportunities and benefits to juveniles . . ." IJA-ABA JUVENILE JUSTICE STANDARDS, Standards Related to Juvenile Records and Information Services: Part XV: Access to Juvenile Records 192 (1996).

Suggested additions

(L) Minor Settlements

(M) Motions for ex parte Order Approving Replevin

(N) Motions seeking Temporary Restraining Orders

IV. Suggested changes to DCRA Rule 7(a)

DCRA Rule 7(a) requires a motion to impound or seal "be accompanied by an affidavit stating the basis upon which a movant has standing...." DCRA Rule 8(a) relating to obtaining access to impounded or sealed information states (in part) that a "nonparty seeking access... shall be considered a party in interest for the limited purposes of the motion...." Although there are slightly different interests at issue, it seems that those seeking to have matters impounded or sealed could be treated as limited purpose parties-in-interest without having to submit an affidavit. Alternatively, the Court should add a provision indicating that those whose personally identifiable information appears in the information, document, or court record be considered parties in interest for the limited purpose of the motion to impound or seal.

Furthermore, I would encourage the Court to consider broadening the considerations for impounding or sealing. Here is language from Indiana: if the "1) public interest served by prohibiting access, 2) access will create significant risk of harm to requester, other persons, or general public, OR 3) substantial prejudice to ongoing proceedings cannot be avoided."

Finally, it may be time to either clearly explain the difference between "impoundment" (i.e., shielded from public view) and "sealing" (i.e., shielded from all)⁹ or do away with the distinction in the procedural and digital court record access rules.

⁹ I very much appreciated the explanation provided at March's Civil Rules Committee meeting.
LOH 3-27-19

**APPENDIX B- SELECTED COMMENTS REGARDING
SPECIFIC DIGITAL COURT RECORD ACCESS RULES**

V. Suggested revision to DCRA Rule 9 (d)
To avoid too many different procedures, consider treating noncompliance with Rule 9 in consistently with noncompliance under the current Civil Rules. *See* M.R. Civ. P. 5 (f). Require that a certificate of compliance be filed with each pleading/motion and treat failures to submit like other deficiencies handled by the clerk under Maine Rule of Civil Procedure 5. *See* notes in Appendix C.

VI. Suggested new rule DCRA Rule 13
Information sharing should be controlled and documented; *See* Attachment B-1

VII. General & nit:

Where the DCRA rules refer to other rules of procedure, it would be most helpful to the reader to have them refer to the specific subpart and to have those subparts be conformed to anticipated rule amendments. For example, on page 16 in the Drafter's Notes for Rule 5, subparts (q)(r)(s)(t)(v) refer to specific criminal procedure rules without subparts or subparts of the current rule rather than the proposed rule amendments (*e.g.*, Rule 5 (r) refers to unified criminal procedure rule 4(b) it will become 4(d)) & 5 (v) refers the reader to unified criminal procedure rule 32 (c) but it would be improved by referring to 32(c)(3))

Drafter's Notes on page 15 is missing a semicolon at the end of subpart (m).

**APPENDIX C- RELATED TO
MAINE RULES OF CIVIL PROCEDURE**

DCRA Rule 13 Transfer of Court Record Information or Access to Court Record Storage

- (a) This Rule applies to information sharing and access to the court record storage systems by Private or Governmental Persons, Vendors, or Entities Assisting the Judicial Branch performing its functions or those granted access by policy set by the State Court Administrator (“Administrative Partners”) in order to protect Court Record information and to protect the case management system from unnecessary burden or risk of damage through inappropriate access, hacking, or viruses.
- (b) If a court or other private or governmental entity provides Court Record information to a Administrative Partner to provide information technology support, to gather, store, process, transfer, or otherwise use assist the Judicial Branch in performing its functions, the State Court Administrator shall enter into a written contract with such Administrative Partner prior to any information sharing.
- (c) At a minimum, contracts with Administrative Partners accessing or receiving Court Record information will require the Administrative Partner to comply with widely recognized general data security principles of governing confidentiality, integrity, and availability of information and the intent and provisions of the Digital Court Record Access Rules. For purposes of this section, the term “Administrative Partner ” also includes a state, county, or other governmental agency that provides information technology services to a court.
- (d) Each contract shall require the Administrative Partner to assist the court in its role of educating litigants and the public about the Court’s Court Record Access Policy and existence of the Digital Court Record Access Rules. The vendor shall also be responsible for training its employees, agents, and subcontractors about the provisions of this Rule.
- (e) Each contract shall prohibit vendors from disseminating Aggregate Data, Bulk Data or Compiled Data, without first obtaining written approval as required by Rule 4.
- (f) Each contract shall require the vendor to acknowledge that Court Records remain the property of the court and are subject to the directions and orders of the court with respect to the handling and access to the Court Records, as well as the provisions of these Rules.
- (g) Each contract shall include provisions that expressly state the administrative, physical and technological security requirements necessary to ensure the protection of Court Record information under the particular business arrangement and prohibit the Administrative Partner from further dissemination of Court Record information without the express written permission of the court.
- (h) The State Court Administrator will develop process for monitoring Administrative Partner compliance with the provisions of this Rule which shall include plans to address noncompliance.
- (i) These requirements do not apply to those information transfers required pursuant to a lawful court order or otherwise compelled by law. When appropriate, the State Court Administrator will seek a protection order or otherwise act to protect the release of Court Record Information.
- (j) These requirements are in addition to those otherwise imposed by law.

(Based on Indiana Administrative Rule 9 (I))

APPENDIX C—ISSUES RELATED TO THE MAINE RULES OF CIVIL PROCEDURE

In line with the recommendations provided in my comments submitted related to the proposed Digital Court Record Access Rules, I provide the following sample amendments to the Maine Rules of Civil Procedure, statutory change, and new forms:

1. Amendment *Maine Rule of Civil Procedure 3*

Related: Statute 14 M.R.S. § 553

2. Amendment *Maine Rule of Civil Procedure 5*

Related: Sample Certification Form

Based on Indiana's Form A-5 - Local Rule Certifying Compliance with Trial Rule 5 (G) found in

<https://www.in.gov/judiciary/iocs/files/PublicAccessHandbook.pdf>

Related: Sample Court Order Template

Based on Indiana's Form A-4 - Order to Comply with Administrative Rule 9 found in

<https://www.in.gov/judiciary/iocs/files/PublicAccessHandbook.pdf>

3. Amendment Maine Rule of Civil Procedure 7

4. Amendment Maine Rule of Civil Procedure 11

The approach in these drafts is to provide maximum notice to members of the bar and public and options for Rules Committee. When the Committee considers these drafts, it may determine that fewer references or rule amendments would be sufficient to implement the DCRA Rules.

In addition to the proposed amendments, some sections are highlighted in yellow to reflect areas of these rules that may require attention when information about the Maine Judicial Branch's e-filing and case management system information becomes available.

**ATTACHMENT C-1A-PROPOSED AMENDMENT
MAINE RULE OF CIVIL PROCEDURE 3**

STATE OF MAINE
SUPREME JUDICIAL COURT
AMENDMENTS TO
THE MAINE RULES OF CIVIL PROCEDURE

3-27-19 Draft 2019 Me. Rules --

Effective: XXXX, 2019

All of the Justices concurring therein, the following amendments to the Maine Rules of Civil Procedure are adopted to be effective on the date indicated above. The specific amendments are stated below. To aid in understanding of the amendments, an Advisory Note appears after the text of each amendment. The Advisory Note states the reason for recommending the amendment, but the Advisory Note is not part of the amendment adopted by the Court.

1. Rule 3 of the Maine Rules of Civil Procedure is amended to read as follows:

RULE 3. COMMENCEMENT OF ACTION

Except as otherwise provided in these rules, a civil action is commenced (1) by the service of a summons, ~~and~~ complaint, ~~and~~ notice regarding Electronic Service, and certificate of compliance with Maine Rule of Digital Court Access 9, or (2) by filing a complaint with the court no sooner than 10 days and no later than ~~When method (1) is used, the complaint must be filed with the court within 20 days after completion of service. (2) For good cause shown and after considering the privacy interests of those involved, a court may allow a party to file the complaint with the court before service of a summons, complaint, and notice regarding Electronic Service.~~ When method (2) is used, the return of service shall be filed with the court within 90 days after the filing of the complaint. If the complaint or the return of service is not timely filed, the action may be dismissed on motion and notice, and in such case the court may, in its discretion, if it shall be of the opinion that the action was vexatiously commenced, tax a reasonable attorney fee as costs in favor of the defendant, to be recovered of the plaintiff or the plaintiff's attorney.

Advisory Note– XXXXXX 2019

**ATTACHMENT C-1A-PROPOSED AMENDMENT
MAINE RULE OF CIVIL PROCEDURE 3**

The amendment to Rule 3, together with newly promulgated Maine Rules of Digital Court Record Access and amendments to the Maine Rules of Civil Procedure, are part of a package of simultaneous amendments related to the implementation of electronic filing within the Maine State court system. The amendment to Rule 3 requires service upon parties prior to filing unless leave of court is granted to file first and serve second. In this way, parties will have notice of the information to be filed with the court and will have a meaningful opportunity to petition the court for protection of confidential or sensitive information. Filing would not occur until the receiving party had a realistic timeframe within which to make protection requests. Judges retain the discretion to authorize an alternative process upon a finding of good cause and after considering the privacy interests of parties and nonparties and the implementation of appropriate safeguards.

2. This amendment shall be effective XXXX 2019.

**ATTACHMENT C-1B-PROPOSED AMENDMENT
14 M.R.S. §553**

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 14 MRSA §553 is amended to read:

§553. Action commenced when complaint is served and filed

An action is commenced when the summons, ~~and~~ complaint, notice of electronic filing, are served and the complaint, certificate of compliance with Maine Rules of Digital Court Record Access, and return of service are ~~or when the complaint is filed with the court unless otherwise authorized by court order,~~ or when the complaint is filed with the court unless otherwise authorized by court order, ~~whichever occurs first~~

SUMMARY

This bill requires parties commencing legal action to provide notice of the allegations to opposing parties prior filing with the court. The purpose of this amendment is to provide parties with information about the contents and allegations within a lawsuit and to allow them to have a meaningful opportunity to petition the court for the protection of any sensitive or confidential information prior to publication of court record information.

ATTACHMENT C-2A PROPOSED AMENDMENTS
MAINE RULE OF CIVIL PROCEDURE 5

STATE OF MAINE
SUPREME JUDICIAL COURT
AMENDMENTS TO
THE MAINE RULES OF CIVIL PROCEDURE

3-27-19 Draft 2019 Me. Rules --

Effective: XXXX, 2019

All of the Justices concurring therein, the following amendments to the Maine Rules of Civil Procedure are adopted to be effective on the date indicated above. The specific amendments are stated below. To aid in understanding of the amendments, an Advisory Note appears after the text of each amendment. The Advisory Note states the reason for recommending the amendment, but the Advisory Note is not part of the amendment adopted by the Court.

2. Rule 5 of the Maine Rules of Civil Procedure is amended to read as follows:

RULE 5. SERVICE AND FILING OF PLEADINGS AND OTHER PAPERS

....

(b) Same: How Made. Whenever under these rules service is required or permitted to be made upon a party represented by an attorney, the service shall be made upon the attorney unless service upon the party personally is ordered by the court. When an attorney has filed a limited appearance under Rule 11(b), service upon the attorney is not required. Service upon an attorney who has ceased to represent a party is a sufficient compliance with this subdivision until written notice of change of attorneys has been served upon the other parties. Except as otherwise provided in these rules, service of the documents described in subdivision (a) upon a party who is represented by an attorney or an unrepresented party **who has opted in to Electronic Service shall be made**

(1) by delivering a copy to the attorney or to the party; or
(2) by Electronic Service to the last known electronic mail address provided to the court or, if no electronic mail address is known, mailing it to the last known regular mail address, or, if neither is known, by leaving it with the clerk of the court.

If Electronic Service to the last known electronic mail address is returned as undeliverable, or the sender otherwise learns that it was not successfully delivered,

**ATTACHMENT C-2A PROPOSED AMENDMENTS
MAINE RULE OF CIVIL PROCEDURE 5**

service must then be made by regular mail. Service shall be complete upon the attempted Electronic Service for purposes of the sender meeting any time period. Service of the documents described in subdivision (a) upon an unrepresented party who has not opted in to Electronic Service or service of documents excluded from Electronic Service below shall be made by mailing them to the last known regular mail address of the party, or, if no mail address is known, by leaving them with the clerk of the court.

“Electronic Service” means the electronic transmission of a pleading or document. Unless otherwise approved by the court, pleadings and other documents being transmitted electronically shall be sent or submitted as an attachment in portable document format (PDF), except that documents produced pursuant to rules 33 and 34, any record in support of summary judgment in excess of 50 pages, and the record of proceedings filed pursuant to Rules 80B or 80C are not required to be produced or transmitted in electronic format, and, in addition to being electronically served, original signed answers to interrogatories are required to be produced to the requesting party. Electronic Service shall be complete when transmitted, shall be presumed to have been received by the intended recipient, and shall have the same legal effect as the service of an original paper document.

....

(e) **Filing With the Court Defined.** The filing of pleadings and other papers with the court as required by these rules shall be made by filing them with the clerk of the court except that a justice or judge may permit the papers to be filed with that justice or judge, in which event the justice or judge shall note thereon the filing date and forthwith transmit them to the office of the clerk. After hours or other office filings are subject to Rule 5(g).

(f) **Filing of Papers Not in Compliance with Rules, Orders or Statute.** Filings that are received but which are not signed, or are not accompanied at the time of filing by a legally required element, including but not limited to, a filing fee, appeal fee, registry recording fee and envelope or summary sheet, or, if filed by an attorney, do not have the attorney’s Maine Bar Registration Number, shall be returned by the clerk as incomplete. The clerk will not docket the attempted filing but will retain a copy of the attempted filing and the notice of return for six months. The offeror may refile the documents when all elements are complete. The filing will be docketed when the complete filing is received.

**ATTACHMENT C-2A PROPOSED AMENDMENTS
MAINE RULE OF CIVIL PROCEDURE 5**

Filings that do not contain a certificate of compliance with Maine Rule of Digital Court Record Access 9 as specified in subpart (1) below will be impounded. The Court may impose sanctions for noncompliance, including striking the pleading from the record with the same effect as if the pleading had not been filed, or authorize the filer to submit an amended pleading pursuant to the terms of an order. The Clerk shall serve a copy of the any such order and the impounded pleading upon non-complying party or the attorney of record by certified mail and shall serve a copy of the order only upon all other parties of record. Pending the filing of any authorized amended pleading, the time for the filing of responsive pleadings shall be extended for an equal period of time.

....

(k) Electronic Filing. Filings by electronic transmission of data or by means of a compact disk (CD) or floppy disk or any other method for electronic or internet filing in place of the filing of paper documents required by these rules, is not permitted.

(l) Certificate of Compliance with Maine Rules of Digital Court Access 9.
(1) Any pleading which sets forth a claim for relief, including motions, except those specified in subdivision (2) below, shall be accompanied by a properly completed and executed Certificate of Compliance in a format approved by the Administrative Office of the Courts. (2) Certificates are not required in case types and proceedings excluded from public access as identified in Maine Rule of Digital Court Record Access 6.

Advisory Note– XXXXXX 2019

The amendment to Rule 5, together with newly promulgated Maine Rules of Digital Court Record Access and amendments to the Maine Rules of Civil Procedure **XXX**, are part of a package of simultaneous amendments related to the implementation of electronic filing within the Maine State court system.

These amendments to Rule 5 require filers to include a certificate of compliance with Maine Rule of Digital Court Record Access 9 and direct the clerk to impound filings that do not contain a certification that the filings comply with Maine Rules of Digital Court Access. The amendments outline consequences of noncompliance, and describe the filer’s responsibility for filing amended filings.

**ATTACHMENT C-2B
SAMPLE PARTY CERTIFICATION**

All pleadings filed by a party shall contain a verification certifying that the pleading complies with the filing and signature requirements of Maine Rules of Civil Procedure 7, 5 & 11 applicable to information excluded from the public record under Maine Rule of Digital Court Record Access 9.

A certification in substantially the following language shall be sufficient:

Certification of Compliance with Maine Rule 5

_____ I/We hereby certify that the foregoing document complies with the requirements of Maine Rules of Civil Procedure 5, 7, & 11 with regard to information excluded from the public record under Maine Rule of Digital Court Record Access 9.

OR

_____ I/We hereby certify that pursuant to Maine Rule of Civil Procedure 5(1)(2), the foregoing document is not subject to the certificate of compliance requirements of Maine Rules of Civil Procedure 5, 7, & 11.

_____ (Signed by party or counsel of record)

_____ (Printed Name)

_____ Bar Number (attorneys only)
_____ (Date)

**ATTACHMENT C-2C
SAMPLE FORM ORDER**

The court has received a pleading filed by (Insert Name of Party) denominated as (Insert Title of Pleading) that was impounded (protected from public view) because it does not comply with the requirements of Maine Rule of Digital Court Record Access 9 and Maine Rules of Civil Procedure 5, 7, & 11.

Alternative 1:

It is Ordered that (Insert Name of Party) shall file an amended pleading that fully complies with Maine Rule of Digital Court Record Access 9 [within (Insert Number) days] [on or before (Insert Date)]. Failure to comply will result in the striking of the pleading from the record. Pending the filing of the amended pleading, the time for the filing of responsive pleadings shall be extended for an equal period of time.

Alternative 2:

Due to repeated noncompliance or otherwise in the interest of justice, it is Ordered that the noncompliant pleading referenced above is stricken from the record.

Applies For Both Alternatives:

The Clerk shall serve a copy of the within order and the impounded pleading upon (Insert Name of Party) or their attorney of record by certified mail and shall serve a copy of this order only upon all other parties of record.

Justice/Judge

Date: _____

**ATTACHMENT C-3 Proposed Amendment to
Maine Rule of Civil Procedure 7**

STATE OF MAINE
SUPREME JUDICIAL COURT
AMENDMENTS TO
THE MAINE RULES OF CIVIL PROCEDURE

3-27-19 Draft 2019 Me. Rules --

Effective: XXXX, 2019

All of the Justices concurring therein, the following amendments to the Maine Rules of Civil Procedure are adopted to be effective on the date indicated above. The specific amendments are stated below. To aid in understanding of the amendments, an Advisory Note appears after the text of each amendment. The Advisory Note states the reason for recommending the amendment, but the Advisory Note is not part of the amendment adopted by the Court.

3. Rule 7 of the Maine Rules of Civil Procedure is amended to read as follows:

RULE 7. PLEADINGS ALLOWED: FORM OF MOTIONS

....

(b) Motions and Other Papers.

(1) An application to the court for an order shall be by motion which, unless made during a hearing or trial or under Rule 26(g), shall be made in writing, shall state with particularity the grounds therefor and the rule or statute invoked if the motion is brought pursuant to a rule or statute, and shall set forth the relief or order sought. (A) Any motion, opposition, or reply shall include a certificate of compliance with Maine Rule of Digital Court Record Access 9 unless exempted pursuant to Maine Rule of Civil Procedure 5 (1) (2). Any motion except a motion that may be heard ex parte shall include a notice that matter in opposition to the motion pursuant to subdivision (c) of this rule must be filed not later than 21 days after the filing of the motion unless another time is provided by these Rules or set by the court. The notice shall also state that failure to file timely opposition will be deemed a waiver of all objections to the motion, which may be granted without further notice or hearing. If the notice is not included in the motion, the opposing party may be heard even though matter in opposition has not been timely filed.

....

**ATTACHMENT C-3 Proposed Amendment to
Maine Rule of Civil Procedure 7**

....

Advisory Note– XXXXXX 2019

The amendment to Rule 7, together with newly promulgated Maine Rules of Digital Court Record Access and amendments to the Maine Rules of Civil Procedure **XXX**, are part of a package of simultaneous amendments related to the implementation of electronic filing within the Maine State court system. The amendment to Rule 7 requires those signing pleadings to certify that the pleadings comply with the Maine Rules of Digital Court Access.

2. This amendment shall be effective XXXX 2019.

**ATTACHMENT C-4 Proposed Amendment to
Maine Rule of Civil Procedure 11**

STATE OF MAINE
SUPREME JUDICIAL COURT
AMENDMENTS TO
THE MAINE RULES OF CIVIL PROCEDURE

3-27-19 Draft 2019 Me. Rules --

Effective: XXXX, 2019

All of the Justices concurring therein, the following amendments to the Maine Rules of Civil Procedure are adopted to be effective on the date indicated above. The specific amendments are stated below. To aid in understanding of the amendments, an Advisory Note appears after the text of each amendment. The Advisory Note states the reason for recommending the amendment, but the Advisory Note is not part of the amendment adopted by the Court.

4. Rule 11 of the Maine Rules of Civil Procedure is amended to read as follows:

RULE 11. SIGNING OF PLEADINGS AND MOTIONS; SANCTIONS

(a) Attorney Signature Required; Sanctions. Subject to subdivision (b), every pleading and motion of a party represented by an attorney shall be signed by at least one attorney of record in the attorney's individual name, whose address, including email address, shall be stated. A party who is not represented by an attorney shall sign the party's pleading or motion and state the party's address, including email address. Except when otherwise specifically provided by rule or statute, pleadings need not be verified or accompanied by affidavit or certificate. The signature of an attorney or party constitutes a representation by the signer that the signer has read the pleading or motion; that to the best of the signer's knowledge, information, and belief there is good ground to support it; ~~and~~ that it is not interposed for delay; and that it complies with the Maine Rules of Digital Court Record Access. If a pleading or motion is not signed, it shall not be accepted for filing. If a pleading or motion is signed with intent to defeat the purpose of this rule, the court, upon motion or upon its own initiative, may impose upon the person who signed it, upon a represented party, or upon both, an appropriate sanction, which may include an order to pay to the other party or parties the amount of the reasonable expenses incurred because of the filing of the pleading or motion, including a reasonable attorney's fee.

**ATTACHMENT C-4 Proposed Amendment to
Maine Rule of Civil Procedure 11**

....

Advisory Note– XXXXXX 2019

The amendment to Rule 11, together with newly promulgated Maine Rules of Digital Court Record Access and amendments to the Maine Rules of Civil Procedure **XXX**, are part of a package of simultaneous amendments related to the implementation of electronic filing within the Maine State court system. The amendment to Rule 11 requires those signing pleadings to certify that the pleadings comply with the Maine Rules of Digital Court Access.

2. This amendment shall be effective XXXX 2019.

APPENDIX D RELATED TO MAINE RULES OF UNIFIED CRIMINAL PROCEDURE

Unified Rule of Criminal Procedure 49 (d) states, “papers shall be filed in the same manners as civil actions.” To ensure compliance with the new DCRA rules, I suggest that a certification of compliance with DCRA Rule 9 be added to Rule 49 expressly-either adding language identical to the civil rules or adapting the concept for the criminal law context.

Similarly some motions are not filed in the first instance, but eventually have the potential to be filed with the court. For example, Unified Rule of Criminal Procedure 2(b)(3) requires counsel to exchange motions and responses and to file those with the court only when they are not resolved prior to trial. To be sure that the information ultimately filed with the court complies with the requirements of DCRA Rule 9, it would be prudent include references in this rule as well.

APPENDIX E—LINKS TO OTHER STATE COURT INFORMATION

Indiana

Remote access is not guaranteed in all courts. When provided, it is restricted to summary information.

On line court record access (Odyssey)

<https://www.in.gov/judiciary/>

Administrative Rules

<https://www.in.gov/judiciary/rules/admin/index.html>

Bench card

<https://www.in.gov/judiciary/iocs/files/pubs-trial-court-ar9-benchcard.pdf>

Public Access to Court Records Handbook

<https://www.in.gov/judiciary/iocs/files/PublicAccessHandbook.pdf>

Massachusetts:

Provides public access to electronic court records only at kiosks in the courthouse. Lawyers have full online access to all case files.

Court Dockets, Calendars, and Case Information

<https://www.mass.gov/search-court-dockets-calendars-and-case-information>

Uniform rules on public access

<https://www.mass.gov/trial-court-rules/trial-court-rule-xiv-uniform-rules-on-public-access-to-court-records>

Missouri

Public access online is limited to docket information only, not the whole case file. Free public access to full case files is at courthouse terminals only. Lawyers have full online access to all case files.

Court Records (Case.net)

<https://www.courts.mo.gov/casenet/base/welcome.do>

Court Operating Rule 2

<https://www.courts.mo.gov/courts/ClerkHandbooksP2RulesOnly.nsf/e2aa3309ef5c449186256be20060c329/dc2e80286afa4ad286256ca60051dee2?OpenDocument>

Oregon

Public access to electronic files is available in court kiosks for any record that is not juvenile, adoption, civil commitment, or sealed. Online access for attorneys is broader, and extends to every public case and public document.

Oregon Judicial Department Online Records Search

<https://webportal.courts.oregon.gov/portal/>

Court Record Access FAQ

<https://www.courts.oregon.gov/services/online/Documents/Calendars-Records/recordSearchFAQs.pdf>

Case or Court Record Search Overview

<https://www.courts.oregon.gov/how/Pages/find.aspx>

Remote Public Access to Electronic Court Records: A Cross-Jurisdictional Review for the D.C. Courts

http://www.courtexcellence.org/uploads/publications/RACER_final_report.pdf

Memorandum Regarding the Maine Digital Court Records Access Rules

PINE TREE LEGAL ASSISTANCE, INC.

P.O. Box 547
Portland, ME 04112-0547
(207) 774-4753

March 27, 2019

Pine Tree Legal Assistance is a statewide nonprofit providing free legal assistance to low-income individuals in the civil justice system in Maine. It has been in operation since 1967 and currently maintains offices in six locations (Portland, Lewiston, Augusta, Bangor, Machias and Presque Isle.) It currently employs 39 lawyers, most of whom regularly appear in Maine District Courts throughout the state, and, less frequently, before the Superior Court, Supreme Judicial Court and Maine Probate Courts.

The Maine Supreme Judicial Court has invited comments on the proposed creation of the Maine Digital Court Records Access Rules and related amendments to the Maine Rules of Civil Procedure. Pine Tree Legal Assistance writes to provide feedback on how the proposed rules would affect access to justice, low-income litigants, and the ability of legal aid attorneys to effectively assist their clients throughout the state of Maine.

These comments are intended to supplement our comments regarding the previously proposed Digital Court Records Act. We support several important differences between the Digital Court Records Act and the proposed rules. Including Protection from Abuse cases on the list of confidential matters will provide significant protections for survivors of domestic violence, sexual assault and stalking. Not including recordings of hearings in the electronics records will ensure that testimony that includes sensitive and private information will not be made public.

Like the Digital Court Records Act, the proposed rules create a basic framework for the new electronic court records system to be implemented throughout the Maine court system. Due to the central role the technological structure of the system will play in allowing access and privacy, critical questions that will affect low-income litigants' access to justice remain unanswered.

A. Confidentiality

A transparent and public court system is essential to providing access to justice. We appreciate the extent to which the Digital Court Records Access Rules balance the need for transparency with individual privacy rights. However, we have several concerns regarding how the rules will affect the privacy of the low-income Mainers we serve.

The Digital Court Records Access Rules provide that documents will appear in the electronic system within three days of when they are filed. However, in many ways, the Internet is intractable. Once something is posted online, it is difficult to 'unring the bell.' The only meaningful way to protect a litigant's confidential information from being made public is to provide enough time for them to file a motion to redact documents after they are served but

before the document is posted for public reviewing. Allowing a certain number of days before a document is posted online after filing (we suggest fourteen days) would give litigants this opportunity.

Maine Rules of Civil Procedure Rule 4 allows plaintiffs to commence an action by either filing and then serving the defendants, or serving the defendants and then filing. If filings appear in the electronic records within three days of when documents are filed, this will mean that information about defendants is accessible to the public prior to the defendants having notice of the action in cases if filing happens before service. Instead, documents initiating an action should appear in the system only after proof of service has been filed.

The processes for sealing records in Rule 7 and correcting mistakes in Rule 12 will be essential in giving litigants the ability protect their own privacy. However, it is important that the system is accessible – especially for pro se litigants. Rule 7 should have an associated form that is easy-to-read and fill out. Anecdotally, our legal aid colleagues in other states have reported socioeconomic inequities in litigants’ access to the sealing process. Maine should avoid this pitfall by creating a system that ensures access for all.

We support Rule 9 which addresses the procedure when information is filed in documents that is confidential under the rules. We agree that it necessary for the courts to have the option to sanction parties who violate the rules. However, we are concerned that the specificity and technical nature of the rules means many pro se parties will fail to follow them. Sanctions should not be imposed against parties when information is inadvertently or mistakenly disclosed without malicious intent.

B. Searchability and Use of Information

Many of the ways in which the electronic records system will affect the privacy of individuals will be dictated by the technological structure of the system. The proposed rules do not address what information will be required to search the database. As we discussed in our comments submitted on January 25, 2019, the setup of this basic function will dictate whether the public will be able to trawl for information in the court records or whether searches will require specific information known by people with interest in a specific case. The latter approach will better protect the privacy of individuals while still allowing the public and the press access to case information.

To the extent the Digital Court Records Act allowed the purchase of bulk data from the court records, we support the proposed rules not affirmatively allowing this and instead delaying the specifics of Rule 4 regarding bulk data until after the system is in place and functional. When the rules about bulk data are created, it is important to remember that allowing outside people or organizations to purchase bulk data will have a significant impact on low-income Mainers. It will allow individuals or organizations outside the court system to control the distribution and accuracy of court information by using court information to create their own databases. In turn, this will provide for greater instances in which low-income Mainers are denied housing and employment based on information that may not be complete or accurate when landlords and employers use the outside database instead of the official record. To preserve the integrity of

case information, the rules should prohibit the purchase of bulk data and also prohibit the further dissemination of information from the records for commercial purposes. This would allow an employer or landlord to do their own background check but would also ensure they are accessing accurate information under the control of the court system.

C. Fees

The rules contemplate that fees will be charged for accessing files. While this could help to limit the access of people who are looking for bulk data or looking for ways to take advantage of the availability information, fees give greater access to the court system to people and law firms that can afford to pay them. Giving litigants and attorneys free access to their own cases is essential to ensure that all parties to a case have equal access to the case file; no party should be given an advantage in the case because they can better afford access to the file.

Allowing legal aid organizations, as defined in Maine Rules of Civil Procedure Rule 89(c), to have free access to records would also expand access to justice. Attorneys often need to access files in which they have not entered their appearance. This is true for legal aid attorneys in several situations: when they are not going to enter their appearance but are considering whether to do so, when they need documents from a case related to a case they are working on, or when they are giving pro se litigants advice. Pine Tree attorneys and other legal aid attorneys now go to courthouses to review files. If we are required to pay for this access to information, it will add new costs to our budgets and will result in less representation for low-income Mainers.

Fee waivers will be essential for litigants. However, the current fee waiver system is too onerous for use for simple tasks, like reviewing documents, given that applications must be reviewed by both a financial screener and a judge. Streamlining this process will be required to ensure necessary access to information by low-income litigants.

D. Family Law Rules

Limitations on Interim Hearings

The addition of the last sentence of Rule 107(b)(2) and the last sentence of Rule 110A(b)(4)(C) attempts to limit interim hearings to one interim hearing “during any stage of the case.” Because the “stage of the case” is not defined, this language is confusing and subject to inconsistent interpretation. Additionally, the limitation on interim hearings might lead to Magistrates declining to hold interim hearings on issues such as child support as soon as possible in the case, which would disproportionately impact low-income litigants and victims of domestic violence. The court already has discretion to decline to schedule an interim hearing. If additional language is added to these sections of the statute, the language should be more clearly drafted. For example, rephrasing the sentence to read: “The court has the discretion to limit the number of interim hearings scheduled.”

Cellular and Electronic Devices in PFA court

Rule 127 prohibits recording protection from abuse proceedings and posting the official recording to the Internet. This broad prohibition is consistent with VAWA and the court's decision to keep PFA proceedings confidential. However, proposed subsection 127(d) prohibits possession or use of cell phones, smartphones, and a number of other recording devices in a courtroom during PFA proceedings. This prohibition would impact litigants' ability to present evidence in PFA cases, which often is contained on such devices, and would also restrict attorneys' use of these devices during court proceedings. Although prohibition of possession and use of these devices would support the court's prohibition on recording PFA proceedings, a less restrictive rule related to possession and use would support both litigants and attorneys who may need to access these devices for legitimate purposes during the PFA process.

Respectfully submitted,



Nan Heald, Executive Director

Pine Tree Legal Assistance

PO Box 547

Portland, ME 04112

Telephone: 207-774-4753

Digital Court Records Access Rules
Sun Journal, Kennebec Journal and Morning Sentinel comments, submitted by
Executive Editor Judith Meyer
March 27, 2019

Thank you for this opportunity to comment on the draft Maine Digital Court Records Access Rules. This has been a very transparent process, and our journalists have welcomed the opportunity for input.

Our newspapers join in the comments of the Maine Freedom of Information Coalition, but wanted to place special emphasis on several elements of proposed Rule 5, specific information which, as drafted, would be excluded from public access.

(d)(1)Home addresses:

Certain personal identifying information is critical to identifying the correct person involved in any criminal or civil action, not just someone who may have the same first and last names.

There are at least four women named Judith Meyer who live in Maine. If, under the draft rules, the Judith Meyer who lives in Auburn (that's me) were to commit a heinous crime and the digital file listed Judith Meyer by name only — with no numbered street address — the harm to the Judith Meyer who lives in Randolph, or the one who lives in Camden, or the one who lives on Mount Desert would be extreme and ridiculously unfair.

There are simply too many common names, even within small communities and often on the same street, carrying too much potential for mistaken identity to ignore.

Mainers recognized and embraced the importance of full identification by the court when the names and home addresses were released in connection with the prosecution of Alexis Wright in 2012, the so-called Zumba case.

The alleged Johns in that highly-publicized case argued that their names not be released because of the public embarrassment and potential for damage to their reputations and livelihoods if their identities became known.

The Law Court disagreed, and decidedly so, ordering full names, ages and home addresses be released.

Justice Thomas Warren captured the fundamental need for complete identification when writing: "The principle that court proceedings are public is essential to public confidence. If persons charged with crimes could withhold their identities, the public would not be able to monitor proceedings to observe whether justice has been done and to observe whether certain defendants may have received favored treatment."

This is true whether records are paper or digital, and goes to the very core of public trust.

(d)(f) Personal health information and medical records

Personal health information and medical records, including, but not limited to all mental health evaluations and records, forensic evaluations, and substance use evaluations and treatment records are the essential building blocks for many cases, both criminal and civil.

How is the public to know and understand the magnitude of a medical malpractice case if health information and medical records of the victim are held confidential?

How is the public to know and understand any defense raised on the grounds of disease or mental defect if mental health evaluations and records are not accessible?

How will the public know and understand the severity of an elevated aggravated assault charge without having access to the medical records and health information of the victim?

And, how will the public know and understand the workings of Maine's drug courts without having access to substance abuse evaluations and treatment records?

Personal health information and medical records of all kinds are openly discussed during court proceedings as motions are heard and trials are held. These records are presented as essential evidence in cases, offered as proof of wrongdoing by one party and of lasting damage to another.

As noted above, continued access to this information is essential to public confidence and understanding of court proceedings.

(d)(m) Information and documents relating to applications for court-appointed counsel

In previous comments, our newspapers argued the necessity to ensure continued public access to financial information and documents filed in support of requests for court-appointed counsel because it's important that the public know and understand who is eligible for these funds and why, and where public money is spent.

I won't repeat the previous comments in full, but would like to briefly reiterate that since the people fund Maine's Commission on Indigent Legal Services, they have an absolute right to know the foundation for these requests, in which a defendant must prove an overwhelming need for financial assistance. Likewise, defendants who may have applied for funding and were denied have a right to know whether they were treated fairly.

And, since the Commission on Indigent Legal Services is frequently strapped for cash and has struggled to pay its bills in the past, defense attorneys in Maine also have a right to know how applications for assistance are managed and how the money is spent because some portion or much of their livelihoods depend upon it.

These applications are currently accessible in case files and continued access to them is a matter of financial accountability.

Again, thank you for the opportunity to comment and I look forward to implementation of the digital platform.



Judith Meyer, Executive Editor

Sun Journal	104 Park Street	Lewiston, Maine 04243	(207) 689-2902
Kennebec Journal	36 Anthony Avenue	Augusta, Maine 04330	(207) 623-3811
Morning Sentinel	31 Front Street	Waterville, Maine 04901	(207) 873-3341

**COMMENTS REGARDING
DRAFT MAINE DIGITAL COURT RECORDS ACCESS RULES**

Chief Justice Saufley, Senior Associate Justice Alexander, and Associate Justices Mead, Gorman, Jabar, Hjelm, and Humphrey:

The Maine Judicial Branch (the “MJB”) has recognized its role in balancing the public’s right to access information related to the justice system against the expectations of privacy held by those individuals who interact with the judicial system to resolve disputes and seek justice. Section 8-C of Title 4 recognizes the inherent authority of the Maine Supreme Judicial Court (the “SJC”) to issue rules that “determine any other processes or procedures appropriate to ensure *adequate preservation, disposition, integrity, security, appropriate accessibility and confidentiality* of the electronic records.”¹ Pursuant to this authority, the SJC has proposed new rules to govern the public’s access to digital court records (the “Rules”).²

As proposed, the Rules fail to construct the “comprehensive framework for public access to digital state court records” they set out to provide,³ and unnecessarily create risks of privacy harm for persons who come to the court seeking to protect their rights. More specifically, the proposed Rules improperly burden litigants with the responsibility to mitigate disclosure risk and lack well-established data privacy protections. Simply put, the Rules fail to provide a comprehensive framework for public access to digital court records and unnecessarily create risks of privacy harm for persons who come to the court seeking to protect their rights.

As discussed in greater detail below, the MJB should ensure that the Rules (1) appropriately require the MJB to assume the responsibility of mitigating privacy harms resulting from unauthorized disclosure of personal information and (2) adopt, or require the MJB to adopt, well-established data privacy principles and procedures.

We prefer the MJB delay implementation of the Rules to further research and revise the Rules in light of the issues raised in these comments. At a minimum, the MJB should adopt a phased implementation plan that allows this important evolution of court administration to continue while also providing additional time to minimize the significant harm to Maine citizens and others who avail themselves of the Maine Court System that may ensue under the MJB’s current approach. It is in the best interest of justice that any rules adopted by the MJB to govern access to digital records put forth a truly comprehensive framework.

¹ 4 M.R.S. § 8-C (emphasis added).

² See Draft Maine Digital Court Records Access Rules.

³ Id. at Rule 1.

I. THE RULES PLACE THE BURDEN OF PROTECTING PRIVACY INTERESTS ON FILING PARTIES AND CREATE BARRIERS TO ACCESS

In attempting to protect privacy interests, the Rules would rely on a series of broad categorical approaches to define filing and disclosure that may ultimately unnecessarily restrict the public's access to court records. For example, while the MJB and Maine Legislature have recognized value in making court records accessible to the public through digital media, the distinction inherent in the Rules' definition of "Court Record" between files maintained by the judicial branch in digital form versus files maintained in paper form creates barriers to access certain files based solely on how they are maintained by the court rather than their content.⁴

As another example of the strain on balancing privacy with access considerations that arise from the Rules, the Rules would place the burden of protecting privacy interests on private parties, including lay people with no prior knowledge of statutory or legal privacy protections. At the same time, the Rules omit any remedies for individuals who suffer unauthorized use or disclosure of their personal information.

The Rules also fail to include mechanisms to hold the MJB accountable to Maine citizens for failing to take appropriate security measures to protect personal information. Such accountability mechanisms are a key facet of protecting the personal information of Maine citizens without unnecessarily restricting access to information. The Rules currently would place primary accountability for protecting the personal information of Maine citizens on filing parties.

The risk of requiring that filing parties redact confidential information and mark pleadings according to whether they may be further disclosed through the digital court records system will in particular create significant challenges to achieving the balance between privacy and access that the MJB seeks to champion.

Under Rule 9 of the Rules, Filing parties bear the responsibility of designating which documents may be disclosed publicly.⁵ Filing parties would need to "conspicuously mark" any files related to cases designated as sealed, impounded, or nonpublic with "NOT FOR PUBLIC DISCLOSURE."⁶ Placing the burden of identifying what information must be protected from disclosure on filing parties, rather than on the MJB (for example, by relying on technological solutions implemented by the MJB), creates risks that documents not intended for disclosure will be disclosed (or vice-a-versa). It also creates a risk that,

⁴ Id. at Rule 2(g) ("Court record" means any file, document, information, or data received or maintained by a state court in digital form. . . .").

⁵ Id. at Rule 9 ("It is the responsibility of the filing party to ensure that sealed, impounded, or nonpublic cases, documents, and information are redacted and/or submitted to the court in accordance with this rule.").

⁶ Id. at Rule 9(a).

pursuant to rule 9(d), filing parties may have their filings rejected if they are improperly labeled.⁷

Because it places the burden of protecting privacy interests on filing parties, and threatens sanctions for parties who fail to meet that burden, Rule 9 would create a barrier to using the digital records system that disproportionately would impact unrepresented parties.

II. THE RULES DO NOT REFLECT APPROPRIATE USE OF TECHNOLOGY SOLUTIONS TO REDUCE BARRIERS TO ACCESS AND SUPPORT THE PROTECTION OF PERSONAL PRIVACY

Some of the above-noted deficiencies in the Rules may stem from the chronic understaffing of the state court system and related concerns about making effective use of limited court resources. For that reason, it is imperative that the MJB thoroughly explore the potential benefits of automated redaction software, and that it do so before finalizing and implementing the Rules.

In a recent white paper, the National Center for State Courts (NCSC) succinctly summarized the important relationship between court privacy policy formulation and the availability of effective technology:

If a court has no technology capability and few resources, then it must close many of its case types and rely on filer liability (again excepting case types that are closed by statute). If a court has some automated redaction capability, then it can open a number of case types and document types. If it has an advanced automated redaction capability that can reliably protect all specified confidential information in any type of document, then it can open a maximum amount of public case information to public access.⁸

In this context, good technology can facilitate better policy. For many years, cost-effective automated redaction solutions were not available to courts, but NCSC focus groups have determined that the latest generation of redaction software shows great promise.⁹ Assuming the MJB were to reach the same conclusion after adequate time and opportunity to explore current technology, the implications would be significant for address some of the Rules' present limitations.

We note also that Tyler Technologies, Inc., a company already contracted by the MJB to assist with computerization of records, recently incorporated automated redaction tools

⁷ Id. at Rule 9(d) ("If any filed document does not comply with the requirements of these rules, a court shall, upon motion or its own initiative, order the filed document returned, and that document shall be deemed not to have been filed.").

⁸ "Best Practices for Court Privacy Formulation," National Center for State Courts (July 2017), at 5, available at <https://cdm16501.contentdm.oclc.org/digital/collection/tech/id/876>.

⁹ Id. at 4 & Appendix B.

into solutions it offers the State of Texas.¹⁰ Tyler Technologies indicates that its redaction capability is “best-of-breed” and “tightly integrated” with its court-focused software solution, Odyssey,¹¹ to protect data that shouldn’t be exposed to the general public. However, it is unclear in the Rules whether this redaction capability is a part of the Odyssey solution chosen by the MJB and, if it is, to what extent the MJB intends to use this solution in protecting the privacy of parties to a proceeding.

III. THE RULES DO NOT REFLECT ESTABLISHED PRIVACY PRINCIPLES THAT WOULD MITIGATE OR ALLOW THE MJB TO RESPOND TO CYBERSECURITY THREATS

Court systems are high-level targets for cyberattacks precisely because court records contain valuable personal information related to individuals and businesses.¹² Unauthorized access to such personal information could cause significant harm to the same, and the lack of safeguards may undermine the public’s confidence in the ability of the MJB to protect their sensitive information, deterring such constituents from accessing the court to seek justice.

In parallel with efforts to explore automated redaction technology, the MJB should consider how to adopt and abide by vital data processing principles – such as transparency, data minimization, storage limitation, security, and accountability. Such principles, which inform recent or contemplated privacy legislation in Europe, California, and Congress, are rapidly becoming the standard against which privacy practices are judged. And their importance in this context is particularly significant; as the Joint Technology Committee formed by NCSC, the Conference of State Court Administrators (COSCA) and the National Association for Court Management (NACM) has observed, “[i]f EU data privacy standards were applied to US courts, the sensitive nature of court data would warrant the most stringent protections,” and courts should therefore have “a game plan for preparing to comply with similar legislation in the US.”¹³

The need for the Rules to reflect well-established privacy principles is not academic, but instead, grounded in the reality of and disruption caused by cyberattacks.¹⁴

¹⁰ Press Release, “Tyler Technologies Enhances eFileTexas and re:SearchTX Portals to Protect Sensitive Case Information: Redaction tool protects sensitive information for filers and Texas court clerks” (Dec. 20, 2018), available at <https://tylertech.irpass.com/Tyler-Technologies-Enhances-eFileTexas-and-re:Sear>.

¹¹ Odyssey Case Manager Overview Brochure, [https://www.tylertech.com/Portals/0/OpenContent/Files/3294/Odyssey-Case-Manager-Overview-Brochure .pdf](https://www.tylertech.com/Portals/0/OpenContent/Files/3294/Odyssey-Case-Manager-Overview-Brochure.pdf) last visited (March 26, 2019).

¹² Judge Herbert B. Dixon, Jr., “Cyberattacks on Courts and Other Government Institutions,” ABA Groups, Judicial Division (Jan. 17, 2019), ¶ 15, available at https://www.americanbar.org/groups/judicial/publications/judges_journal/2018/summer/cyberattacks-courts-and-other-government-institutions/.

¹³ See, e.g., “GDPR for US Courts,” Joint Technology Committee Resource Bulletin (Sept. 19, 2018), at 4, available at <https://ncsc.contentdm.oclc.org/digital/collection/tech/id/876/>.

¹⁴ See, e.g., “Information Systems and Cybersecurity – Annual Report 2018,” Administrative Office of the U.S. Courts, available at <https://www.uscourts.gov/statistics-reports/information-systems-and-cybersecurity->

Cyberattacks on courts and other public institutions are well documented.¹⁵ These attacks typically fall into one of four categories - denial of service attacks, phishing, ransomware, and spyware – any one of which would compromise the principles and goals enumerated in the Rules.¹⁶ Direct access to the MJB is not the only avenue for cyberattacks; judicial records may also be compromised through other government branches. Courts around the nation have faced many of the privacy and protection issues now before the MJB,¹⁷ and the MJB would do well to learn from them.

The lack of Rules to guard against any of the four common types of attacks compromises the Courts enumerated goals and the ability of the Judicial Branch to credibly safeguard the personal information under its control. As it stands, conspicuously absent from the Rules is any mention of use of “processes or procedures appropriate to ensure **adequate preservation, disposition, integrity, security, appropriate accessibility and confidentiality** of the electronic records” that the Legislature has recognized are within the

[annual-report-2018](https://www.ncsc.org/~media/Files/PDF/About%20Us/Committees/JTC/JTC%20Resource%20Bulletins/Responding%20to%20Cyber%20Attack%202-26-2016%20FINAL.ashx); “JTC Resource Bulletin: Responding to a Cyberattack,” Joint Technology Committee, NCSC (Feb. 17, 2016), available at <https://www.ncsc.org/~media/Files/PDF/About%20Us/Committees/JTC/JTC%20Resource%20Bulletins/Responding%20to%20Cyber%20Attack%202-26-2016%20FINAL.ashx>.

¹⁵ See, e.g., Dixon, *supra* note 11; “2018 Verizon Data Breach Investigations Annual Report” at 41, Verizon (2018), available at https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf ([Globally, the public sector faced over 22,000 security incidents with 304 confirmed data disclosures. Personal information accounted for 41% of the data compromised.](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf)); Laila Kearney, “With Paper and Phones, Atlanta Struggles to Recover From Cyberattack,” Reuters (March 31, 2018), available at <https://www.reuters.com/article/us-usa-cyber-atlanta/with-paper-and-phones-atlanta-struggles-to-recover-from-cyber-attack-idUSKBN1H70R0> (cyberattack in which the City of Atlanta’s computer network was infiltrated and crippled by malicious actors); Kieran Nicolson, “State Juror Pool Data Breach Exposed Social Security Numbers,” Denver Post (Aug. 8, 2017), available at <https://www.denverpost.com/2017/08/08/state-juror-pool-data-breach-exposed-social-security-numbers/> (external exposure of information held by the Washington State Administrative Office of the Courts); “Washington State Courts Office Suffers Data Breach,” Government Technology (May 9, 2013), available at <https://www.govtech.com/security/Washington-State-Courts-Suffers-Data-Breach.html> (external exposure of jury files held by the Colorado Judicial Department containing names and other data of 41,140 individuals).

¹⁶ See Brian McLaughlin, “Cybersecurity: Protecting Court Data,” PA Times (May 26, 2017), available at <https://patimes.org/cybersecurity-protecting-court-data/>. (1) Denial of Service attacks usually overwhelm servers to a specific site, preventing legitimate users from accessing services or records. (2) Phishing is one of the more common attacks and solicits personal information from unsuspecting users through e-mail that appears legitimate and requests users to enter items such as user names or passwords to compromise accounts. (3) Ransomware infects software and locks access to data until a ransom is paid. Cyberattackers access vulnerable systems through phishing e-mails, drive-by downloading, and unpatched system vulnerabilities. (4) Spyware infects a computer by producing pop-up ads, re-directing browsers and monitoring a user’s internet activity. To the extent that the MJB’s system is interconnected with other government systems, the risk of exposure to attacks increase.

¹⁷ See, e.g., “Judicial Branch’s Computer System Attacked With Ransomware,” NBC Connecticut (Mar. 9, 2018), available at <https://www.nbcconnecticut.com/news/local/Judicial-Branchs-Computer-System-Attacked-With-Ransomware-476402943.html>; Brian McLaughlin, “Cybersecurity: Protecting Court Data,” PA Times (May 26, 2017), available at <https://patimes.org/cybersecurity-protecting-court-data/>; Ricardo Lopez, “Minnesota Courts Cyberattack Underscores Growing Threat,” Star Tribune (June 25, 2016), available at <http://www.startribune.com/minnesota-courts-cyberattack-underscores-growing-threat/384398871/>.

ambit of MJB authority and responsibility.¹⁸ For example, the Rules do not require the MJB to publish a privacy notice informing Maine citizens about how it uses and discloses personal information. Nor do the Rules indicate whether the MJB is required (instead of merely permitted, at its discretion) to adopt security measures to protect such information. The Rules also do not establish, or require the MJB to establish, a response protocol in the event of suspected or actual unauthorized access to personal information. The lack of reference to, or use of, these well-established data security protocols in the Rules flies in the face of generally established practices across all industries, as well as practices specific to court administration.¹⁹

The obvious deficiencies in the Rules raise significant questions about the process by which the MJB formulated the Rules. Our measured research unearthed several significant issues, the most pressing of which we outlined above. The Rules do not describe the research or authorities relied upon by the MJB in developing these Rules or the SJC's philosophy, and there is no information on the MJB website that would assure the citizenry that the MJB fully recognizes its responsibility to safeguard the personal information under its control, even as the MJB embraces its role in balancing the public's right to access court information and the expectations of individual privacy. As a cursory matter, some questions that come to mind – and for which neither the Rules nor the MJB website provide answers – are as follows:

- How does the MJB plan to address actual literacy and technology literacy deficiencies in potential users of Odyssey, the MJB's chosen software solution?
- Why has the MJB chosen to shift the risk of unintended disclosure to Odyssey users, particularly given that some users will not have the actual or technology literacy to use the system proficiently?
- Does the MJB intend to engage a cross-section of stakeholders during Odyssey implementation to ensure that indigent, rural, and other disenfranchised or low-use users of legal services continue to have a clear and accessible path to justice?
- How does the Court plan to safeguard against the specific types of cyberattacks most likely to occur?
- What procedures and plans are in place to allow the Court to continue to function if (when) a cyberattack is successful?

¹⁸ 4 M.R.S. § 8-C.

¹⁹ See, e.g., "Information Systems and Cybersecurity – Annual Report 2017," Administrative Office of the U.S. Courts, available at <https://www.uscourts.gov/statistics-reports/profile-administrative-office-us-courts-annual-report-2017>. (In this report, the Administrative Office of U.S. Courts informed Congress that it had "developed and launched a mandatory IT security 'scorecard,' enabling courts to conduct annual IT security self-assessments. This resource helps court units identify IT security vulnerabilities, channel resources to address them, and bolster the Judiciary's overall IT security posture.")

- What incident response mechanisms are in place to allow affected individuals to mitigate any undue harm resulting from unauthorized access to the personal information they entrusted to the MJB?
- What technology mechanisms are in place to track individuals' access to the court system that would aid in identifying potential perpetrators of cyberattacks if (when) they occur?
- What incident reporting protocols are in place to track and learn from any unauthorized access and create a body of knowledge to support effective court practice in this area?

The Rules fall far short of providing a comprehensive approach and unnecessarily creates the risk of harm for persons who come to the court seeking to protect their rights. . This barebones approach to such an important evolution of court administration in Maine does not appear to leverage the existing body of knowledge of effective court practice.

IV. Recommendations and Conclusion

The following recommendations are modest actions that we urge the MJB to consider to mitigate or prepare an effective response to the issues set forth above.

1. The MJB should delay implementation of the Rules to further research and revise the Rules in light of the issues raised in these comments or adopt a phased implementation plan to allow this important evolution of court administration to continue while also providing additional time to minimize the significant harm to Maine citizens and others who avail themselves of the Maine Court System that is inevitable under the MJB's current approach.
2. Rule 9 should be amended to redistribute the burden for ensuring adequate labeling of filings containing sealed, impounded, or nonpublic information on the MJB. The Rules also should implement an accountability mechanism that requires MJB to adequately protect the personal information of Maine citizens.
3. To the extent MJB intends to use the automated redaction technology offered by Tyler Technologies, the MJB should revise the Rules to particularly state how and when it intends to leverage the benefits of automated redaction or issue an order that requires the MJB to adopt and maintain a privacy policy that does the same. The Massachusetts Supreme Judicial Court has issued such an order, attached here as Appendix I for reference.
4. The Rules should set forth, or require the MJB to adopt, a privacy policy and well-established privacy procedures, including an annual audit to identify system and process weakness. The NCSC has published best practices for courts in drafting

privacy policies, including a model privacy policy,²⁰ attached here as Appendix II for reference.

While the Rules are intended to further an interest in public access to court records, they also recognize the importance of protecting personal privacy. The Rules fail to balance those two interests because they improperly burden litigants with the responsibility of mitigating the risks that personal information will be disclosed without authorization and fail to incorporate well-established data privacy mechanisms. We urge the SJC to further consider the key challenges to balancing access and personal privacy highlighted in these comments before adopting its final rules.

In offering the above comments and recommendations, we are acting solely in our personal capacities as attorneys specializing in, among other areas, privacy law. We are not submitting these comments on behalf of any client, any organization, or our respective law firms.

Respectfully,



Krystal D. Williams, Esq.
Pierce Atwood, LLP



Julian B. Flamant, Esq.
Hogan Lovells US LLP



Vivek J. Rao, Esq.
Pierce Atwood, LLP

²⁰ Thomas M. Clarke, et al. "Best Practices in Court Privacy Policy Formulation," NCSC (2017).

THE COMMONWEALTH OF MASSACHUSETTS

Suffolk, ss.

Supreme Judicial Court

ORDER

Order Re: Protection of Personal Information

Introduction. Massachusetts General Laws c. 93H provides that the judicial branch shall adopt rules or regulations to safeguard certain nonpublic personal information relating to residents of the Commonwealth, the improper or inadvertent disclosure of which could create a substantial risk of identity theft or fraud. This Order governs the security and confidentiality of personal information as defined by c. 93H in the Judicial Branch. It is designed to safeguard the personal information of all individuals, including nonresidents. It shall apply to the appellate courts, trial courts, court administrative offices and court affiliates, which shall be in compliance by September 1, 2010.

Definition. Under G. L. c. 93H, personal information consists of a resident's "first name and last name, or first initial and last name, in combination with any one or more of the following data elements that relate to such resident:

- a. Social Security number;
- b. driver's license number or state-issued identification card number;
- c. financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.

Chapter 93H provides that personal information "shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."

Information Security Program. Each appellate court, the Trial Court and any court affiliate that owns, stores or maintains personal information about an individual shall develop, implement, maintain and monitor a comprehensive, written information security program

applicable to any records containing such personal information. The information security program shall govern the collection, use, dissemination, storage, retention and destruction of personal information. The program shall ensure that courts and court affiliates collect the minimum quantity of personal information reasonably needed to accomplish the legitimate purpose for which the information is collected; securely store and protect the information against unauthorized access, destruction, use, modification, disclosure or loss; provide access to and disseminate the information only to those who reasonably require the information to perform their duties; and destroy the information as soon as it is no longer needed or required to be maintained. Such information security program shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records.

Every information security program shall include:

- (1) A requirement for notice to the Chief Justice for Administration and Management in the case of a trial court, and to the appropriate Chief Justice in the case of an appellate court, in the event of any incident involving a breach of security¹ of personal information.
- (2) Regular monitoring to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- (3) A regular review, at least annually, of the scope of the security measures. Such review also must be conducted whenever there is an incident involving a breach of security and when there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (4) Documentation of responsive actions taken in connection with any incident involving a breach of security, and actions taken, if any, to make changes in practices relating to protection of personal information.

Departmental reviews. Each appellate court, court department and court entity shall review the type of personal information it collects and maintains with the goal of identifying any personal information that need not be collected or maintained. Each department will report the results of

¹G. L. c. 93H defines breach of security as "the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure."

this review to the Chief Justice for Administration and Management, or, in the case of the appellate courts and affiliated agencies, to the Chief Justice of the Supreme Judicial Court, within six months.

Computer systems. If personal information is stored electronically, the information security program shall include provisions that relate to the protection of personal information stored or maintained in electronic form. Such provisions shall be developed with the Courts' Chief Information Officers.

Contracts. All contracts entered into by the Judicial Branch shall contain provisions requiring contractors to notify the court of any incident involving a breach of security of personal information, and to certify that they have read this Order, that they have reviewed and will comply with all information security programs and policies that apply to the work they will be performing, that they will communicate these provisions to and enforce them against their subcontractors, and that they will implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect personal information to which they are given access as part of the contract from unauthorized access, destruction, use, modification, disclosure or loss.

<u>MARGARET H. MARSHALL</u>)	
)	
)	
<u>RODERICK L. IRELAND</u>)	
)	
)	
<u>FRANCIS X. SPINA</u>)	
)	Justices
)	
<u>JUDITH A. COWIN</u>)	
)	
)	
<u>ROBERT J. CORDY</u>)	
)	
)	
<u>MARGOT BOTSFORD</u>)	
)	
)	
<u>RALPH D. GANTS</u>)	

Dated: January 7, 2010

Best Practices for Court Privacy Policy Formulation

**Thomas M. Clarke, Ph.D.
Janet Lewis
Di Graski
July 2017**



Funding for this project was provided by the State Justice Institute Award SJI-16-P-131. The points of view expressed are those of the National Center for State Courts and do not necessarily represent the official position or policies of the State Justice Institute.

Acknowledgements

This project was funded by a grant from the State Justice Institute. The National Center for State Courts (NCSC) is grateful to the participants in the two focus groups who provided input on this white paper. Those participants are not responsible for the views expressed in the white paper and in some cases may not agree with them.

Privacy Policy Focus Group Members

John Bell
Washington State Courts

Rebecca Green
William and Mary Law School

TJ BeMent
National Association for Court
Management

Richard Hoffman
Council for Court Excellence

Alan Carlson
Orange County, CA Courts

June Kress
Council for Court Excellence

Tom Clarke
National Center for State Courts

Ben Moser
Council for Court Excellence

Paul Embley
National Center for State Courts

David Slayton
Texas Courts

Di Graski
National Center for State Courts

Automated Redaction Focus Group Members

Jason Bergbower
Colorado Courts

Paul Embley
National Center for State Courts

Alan Carlson
Orange County, CA Courts

Di Graski
National Center for State Courts

Tom Clarke
National Center for State Courts

Kevin Iwersen
Idaho Courts

Chad Cornelius
Colorado Courts

Henry Sal
Computing System Innovations

Nancy Crandall
Justice Connections

Tom Trobridge
Teradact

Table of Contents

Background	1
Summary of Current Policies	2
Approach to the Problem.....	3
Conclusion.....	7
Appendix A Revised Model Policy for Electronic Public Access to Court Case Records.....	8
Appendix B State of the Art for Automated Redaction.....	16
Appendix C Automated Workflows Using Automated Extraction.....	19
Appendix D Definitions.....	21

Privacy and Public Access Policies

April 2017

How This Report Should Be Used

The National Center for State Courts (NCSC) conducted two facilitated focus groups to produce this report. One focus group considered revisions to the original 2002 COSCA guidelines white paper on privacy and access policies. The second focus group reviewed the status of automated redaction capabilities and assessed the impact of redaction strategies on policy decisions. The membership of the two focus groups only partly overlapped.

NCSC judged that the relationship between policy and redaction capability was a key one and consequently structured this report around it. Readers will still find a separate section that explicitly recommends revisions to the original policy white paper, but this report deliberately asserts the view that policies and redaction capabilities should be considered simultaneously.

This position, and several others in the report such as a strong rejection of “practical obscurity” strategies, are not shared by all the focus group participants. The report is not based on a universal consensus of the focus group members on all issues. It is instead the position of NCSC. In the same vein, it is not endorsed by the Consortium of State Court Administrators (COSCA) as one of its official white papers. Readers should be aware that the report takes a point of view that not all may share.

Background

As state and local courts progressively convert their business processes from paper to electronic formats, policies around remote electronic access to court case information by the public become ever more important. COSCA last addressed this issue comprehensively in 2002 with a report authored by Martha Steketee and Alan Carlson that proposed a model policy for public access¹. At that time, few courts had implemented electronic filing, so the model policy addressed both manual and electronic access. In the fifteen years since then, courts have learned a lot about living in an electronic world and providing remote access to their case data and documents. Consequently, there is a need to update what we know about this topic and revise the model policy.

¹ “Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts,” Martha Wade Steketee and Alan Carlson, October 18, 2002, State Justice Institute (<http://cdm16501.contentdm.oclc.org/cdm/ref/collection/accessfair/id/210>).

Summary of Current Policies

NCSC has consistently recommended that courts create electronic public access policies before they embark on electronic filing and e-court projects. Once courts have case information in electronic format, the public inevitably wants access to it. Unfortunately, many states only begin the process of creating such policies after they have implemented e-filing. Thus, a few states have electronic case information but still do not have appropriate access policies.

A recent review of the existing state electronic public access policies confirmed that the situation that existed several years ago persists²: states exhibit almost no consistency in their policies across most of the key policy decisions and one can find a wide range of policy decisions for almost all the policy aspects. So, a model policy is still relevant. There are some areas of growing consensus and an updated model policy can report that. In other areas, the courts have consolidated around two or three different policy solutions and the model policy can report that as well³. For other policy aspects, NCSC is advocating that public access and privacy policies be considered in light of new technology capabilities: autoredaction software that uses machine learning to help courts better balance their twin (and often competing) public policy goals, increased public access to court case records and increased public safety in a “cyber” world.

The Center for Legal and Court Technology at the William and Mary Law School partnered with NCSC for years on a quasi-annual conference on court privacy policies. As the years went by, a gulf slowly opened between what the policies required and what courts could actually, reliably implement, especially using technology. No issue illustrates this problem more than redaction.

Most state policies close a broad range of case types and document types to public access, usually justifying this significant retreat from stated preferences for openness by the difficulty and expense of reliably redacting information that should remain confidential. A few courts redact such information using court staff or county clerk staff, but for most courts that strategy is prohibitively expensive. Likewise, a few courts use automated redaction to at least partly replace human

² The Council for Court Excellence (CCE) and the National Center for State Courts (NCSC) administered a survey on privacy and public access policies to COSCA in the fall of 2016 and reported on the results at the December 2016 COSCA conference. *See also* a compilation of state court access policies at <http://www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/State-Links.aspx> (click “Privacy Policies for Court Records”).

³ See Appendix A for the updated model policy for electronic public access to court case records.

reviews, but early vendor products were both expensive and only partly successful in supporting redaction policy requirements.

That left most courts with no alternative than to put the redaction function and resultant liability onto filers. Although widespread, this approach has serious flaws⁴. Audits have found that compliance is not very good. As the proportion of court cases involving self-represented litigants has grown over the last decade or so, the probability that filers will fully comply has correspondingly dropped. That leaves most courts with a very undesirable tradeoff: open case records to the public with significant occurrences of confidential information being disclosed or close an excessive proportion of case records to the public.

Approach to the Problem

This SJI-funded project held two focus groups to address these problems: one concentrating on an update of the model policy and one to assess the state of the art for automated redaction. The two groups had a small proportion of overlapping participants in recognition of the linkage between the two topics. The deliberations of the two groups very strongly reinforced NCSC's belief that what can and should be specified in electronic access policies is constrained or enabled by what can be done well using automated redaction.

To fully understand why this is the case, consider what courts are trying to do. Case documents and associated data never contain information that is all confidential (except of course when they are entirely closed by statute). Some subset of the data or document contains information that should not be released to the public. Protected information may be formally structured, like a social security number, or unstructured, like the name of a crime victim. Similarly, a case document may itself be formally structured with the confidential content in a reliably predictable place and format, or totally unstructured, in which protected information could appear anywhere.

Early versions of automated redaction worked fairly reliably with structured content in structured documents, but otherwise were not very reliable. Consequently, courts had no recourse except to close case types and document types or specify policies that risked revealing confidential information. Being risk averse by nature, courts consistently opted for the former strategy.

For a while this approach seemed to work, but over the last ten years the environment and public expectations have changed dramatically. First, many

⁴ "A Contrarian View of Two Key Issues in Court Records Privacy and Access," Tom Clarke, 2016 Future Trends in State Courts (<http://www.ncsc.org/~media/Microsites/Files/Trends%202016/Contrarian-View-Trends-2016.ashx>).

government agencies have opened considerable amounts of their data to the public on both the federal and state levels. Executive branch agencies gradually opened up their records in response to FOIA and state public disclosure laws. The federal courts incrementally opened more and more data as well. Second, both for-profit and non-profit organizations have steadily increased pressure on all government agencies to release their data. Third, by putting records on-line, the public has access to them beyond traditional brick-and-mortar hours, and this has provided additional value: it reduces traffic to government facilities while allowing the public more convenience by being able to access files with less disruption to their personal and work schedules.

As experience shows the public benefits of doing so, the public has become more comfortable with this trend. As with many aspects of privacy policy, the public can be remarkably fickle in its desires. As the saying goes, “When they are my data, I want privacy. When they are your data, I want access.” Everyone using the Internet (which is everyone) knows that individuals regularly give up aspects of their personal privacy for business benefits that are valued at a few dollars. We often do so even when we know that a business may use our information in ways we would prefer that they don’t or we simply don’t understand exactly how they will use our data.

This tells us that public attitudes toward privacy and openness are not absolute, but are conditioned by perceptions of value tied to how the data will be used and what we get for allowing them to be used. Some organizations will certainly create products and services with open court data that the public will find valuable and support⁵. The role the media play in public accountability is but one example. So, pressure to open ever more court records continues to build. A separate SJI-sponsored focus group on Courts Disrupted found that such pressure would very likely become overwhelming in the near future⁶.

Given this situation, courts desperately need a cost-effective technology solution in the form of automated redaction that can reliably support their policy requirements. Until quite recently that technology was not available, but the latest generation of redaction software is now showing signs of being capable of doing so⁷. Courts in several counties in Florida, Pennsylvania, and Michigan are successfully using the technology, several state courts have pursued Requests for Information or conducted Proofs of Concept, and additional projects are underway or planned in several state court systems to verify the capabilities.

⁵ See, e.g., <https://thistoo.co>, an on-line tool for divorcing couples in Ontario offering, among other services, “Real case data to help you quickly understand how your case will resolve.”

⁶ “Courts Disrupted,” Joint Technology Committee (JTC) Resource Bulletin (to be published at <http://www.ncsc.org/About-us/Committees/Joint-Technology-Committee/Publications-and-Webinars.aspx>).

⁷ See Appendix B for an overview of current automated redaction capabilities.

One can imagine a relationship between policy and technology that can be characterized by several maturity levels. If a court has no technology capability and few resources, then it must close many of its case types and rely on filer liability (again excepting case types that are closed by statute). If a court has some automated redaction capability, then it can open a number of case types and document types. If it has an advanced automated redaction capability that can reliably protect all specified confidential information in any type of document, then it can open a maximum amount of public case information to public access.

Unfortunately, highly capable automated redaction products are still relatively new, so their cost is not insignificant. Current vendors mostly use a transaction fee model, so higher volumes of cases incur higher costs. It is highly likely that those transaction costs will decrease dramatically as more courts implement the technology and national volumes rise. Until then, cost will be a barrier for many courts.

One possible solution for the cost problem is to recall that value is ultimately what matters. A very serendipitous characteristic of highly effective automated redaction products is that they can extract from filings almost any information a court might specify. This capability opens a new and potentially very useful business strategy to courts. Such data extraction could be used to drive many different kinds of automated workflows in court business processes, making courts significantly more cost effective⁸. That in turn would mitigate the up-front cost of the redaction software.

The potential for automated workflows to reduce court costs is quite large. Other industries have been able to extract as much as 95% of their labor costs from very similar business processes. NCSC informally estimates that up to 85% of what court clerks traditionally do could be automated in this way. Several recent court reform projects have identified new business processes for case triage and case management that could also be fully automated, adding yet more efficiency. Even the best electronic courts today have barely tapped into this potentially huge pool of cost savings. Through e-payment, e-filing, e-bench, and other technologies, leading courts have reduced their labor costs by at most 10% or 15% to date.

If courts could emulate other industries using data extraction software and automated workflows, one can imagine a quantum leap in value for court customers at the same time courts are reaping big savings that can be partly reallocated to providing better service in other ways. It could be nothing short of a revolution in the service provided to the public. This would come none too soon, since courts are ~~already losing case filings at~~ a rapid rate and seeing significant decreases in public support and legitimacy because of their operational failings.

⁸ See Appendix C for a discussion of some of the workflows that could and should be automated in this way.

Assuming that courts begin to move up the maturity scale for automated data extraction and workflows, they will quickly recognize that the policy formulation approach used to date will be completely inadequate to the task. Heretofore, courts have convened ad hoc groups to consider and recommend electronic public access policies. Those groups have typically taken months and sometimes years to produce policy recommendations. Those recommendations then enter a court rules process that usually takes at least a year and sometimes longer. At the end, the adopted policies specify in considerable detail the exact requirements as if the capabilities of the court will never change.

This is clearly not agile enough by a large margin in an environment with rapidly changing technology capabilities and even more volatile public expectations. One solution would be to respect that reality by writing rules at a higher conceptual level and moving much of the technical policy detail to locations that can be more readily updated. A corollary strategy would be to make the rules process itself more agile, although how to do so is unclear and certainly outside the scope of this project.

If courts modified their rules-making processes to be more agile, it would pay off in other ways. Major national projects in civil and domestic relations reform have made multiple recommendations for revising court case processes and will probably continue to do so over the next years, as what we know to work grows and technology matures⁹. In many states these processes are enshrined at least partly in court rules that are subject to the same rigid procedures at a time when courts are trying to become more agile. So the benefits of being able to change rules more easily when appropriate would be broadly felt.

Many state courts also need to approach the area of public access policy formulation more broadly than they have in the past. Judges and court administrators often perceive public access as something completely different from policies regarding access by lawyers, case parties, or other justice agencies. They may create yet other policies aimed at use of court data by researchers or third-party data companies. Yet on the technology side, all these policies are implemented by specifying and enforcing business rules using a common technical infrastructure regulating access according to roles and data types. It would be useful for policy makers to become more aware of how their various policies get implemented and ensure that a

⁹ For a discussion of civil reform recommendations, see the SJI-sponsored Civil Justice Initiative's project website at <http://www.sji.gov/civil-justice-initiative-executive-summary/>. For an easily accessible summary of the business rules that could be automated, go to "Automated Civil Triage and Caseflow Management Requirements," November 30, 2015 (<http://www.ncsc.org/~media/Microsites/Files/Civil-Justice/Automated%20Civil%20Triage%20and%20Caseflow%20Management%20Requirements%202015-11-30.ashx>).

coherent approach is taken that supports successful implementation across the board¹⁰.

Conclusion

The wedding of policy and technology is not unique to public access websites: court leaders pursuing important court innovations in procedure and Government-to-Citizen technology (like Online Dispute Resolution, Fines/Fees/Bail Reform, and Case Triage and Tracking) absolutely depend upon their policymaking bodies to better understand – and reflect on their definitions of court business processes – the art of the possible. This is a challenging era to be running a court system for both good and bad reasons. There are many exciting opportunities to improve court operations and services for the public and also to make being a court employee more interesting and meaningful. There are also high and ever rising expectations by the public that we will make significant improvements as an institution.

Court electronic public access policies both reflect and illustrate these two trends. Courts face big challenges in reliably redacting confidential case information and providing safe, open access to the public, but the ability to do so will pay off in other ways that will greatly help the courts do a good job overall. That obviously creates both opportunities and issues. As courts implement useful new capabilities, other courts will want to take note and leverage what is learned in a timely way to move forward as quickly as possible.

¹⁰ The Florida courts have done a good job of taking a more unified approach to their access rules. See <http://www.flcourts.org/resources-and-services/court-technology/technology-standards.stml> (“Standards for Access to Electronic Court Records” and “Access Security Matrix”).

Appendix A

Revised Model Policy for Electronic Public Access to Court Case Records

The 2002 guidelines¹¹ remain an excellent starting point for a revised model policy. So much of the original document is still valid that it makes the most sense to revise the model language in that report rather than create an entirely new model policy. To ensure that the original report was correctly understood and interpreted, the focus groups included one of the original authors.

Summary of Changes to Model Policy

Although the actual revisions with commentary will be presented below in full, a summary of the changes is provided here to indicate the scope and nature of the changes. The section numbers refer to the original 2002 document. Some sections are renumbered in the revised model policy.

Introduction: Retains the openness principle. Replaces the fundamental distinction between paper and electronic records with a distinction between remote and courthouse access. Asserts a new principle that access should be the same whether remote or in person.

Section 1, Purpose: Reduced the number of objectives to the most important ones and added rationales for each of them.

Section 2, Access by Whom: Revisions were made to focus on public access only. The commentary stresses the need for a common technical infrastructure and coordinated policies for access to court information by various roles.

Section 3, Access to What: The definitions in section 3.10 are still valid and useful. Minor revisions were made to focus the policy on court case records, leaving court administrative records to a separate policy. The remainder of Section 3 was simplified, based upon the assumption that public access is remote, electronic access.

Section 4, Applicability of Rule: The section was extensively revised and combined with Section 3 to (1) identify information where there is a consensus to protect, (2) make explicit the connection between openness and redaction capabilities, (3) move conceptually from document-centric to information-centric approaches, and (4) eliminate “practical obscurity.”

¹¹ <http://cdm16501.contentdm.oclc.org/cdm/ref/collection/accessfair/id/210>

Section 5: Renumbered to section 4.0, “Timing of Public Access.” The public expects remote access 24/7/365. A separate but important issue is how soon after filing courts make information available to the public remotely. This is one of several areas where policy is closely tied to redaction strategies.

Section 6: Renumbered to section 5.0, “Access Fees.” The section was revised to describe the three most common funding strategies and the rationales for using each strategy.

Section 7: The entire “Obligation of Vendors” section was deleted. Several states have developed good contract language for vendors. The Joint Technology Committee (JTC) and the Court Information Technology Officers Consortium (CITOC) will consider developing a model contract.

Section 8: The entire section “Obligation of the Court to Inform and Educate” was deleted. Courts do not need to adopt formal policy guidance on educating litigants, judicial officials, and court staff. Instead, see the new section 3.6 and its commentary, describing the best practice of providing a “one-stop shop” for all public transactions related to court case records (accessing, sealing, expunging, correcting, etc.).

For section content that remains the same, the original commentary is still valid and should be consulted in the original document. Commentary in the revised model policy focuses only on new or revised content.

Assumptions

The world has changed dramatically since 2002. Many courts now operate with completely electronic case records. The revised model policy is designed explicitly to support that new reality and is based upon these assumptions:

1. Courts require electronic filing of all case related information.
2. Courts manage all case related information in case management, document management, and content management systems.
3. Remote public access is supported via Internet and cell phone networks.
4. Remote public access is available essentially around the clock nonstop.

Revised Model Policy for Electronic Public Access to Court Case Records

Introduction

This policy is based on two fundamental principles:

1. Court records are presumptively open to public access.
2. Public access should not change depending upon whether access is remote or at the courthouse.

Section 1.0 – Purposes of the Policy

- a. Maximize accessibility of court case records¹².
- b. Protect users of the court from harm.
- c. Make effective use of court resources.

Commentary: Accessibility is maximized for several reasons: to enhance public trust and confidence, to be accountable, to be transparent, to improve customer service, and to reveal common law. Protection from harm includes individuals, business organizations, government agencies, and the public at large. When balancing openness against potential harm, courts should make the rationales for their decisions explicit. Remote public access is part of a much larger strategy to provide court services online to improve access and convenience and to reduce cost. Cost and efficiency considerations refer to both user costs and court operational costs.

Section 2.0 – Who Has Public Access

- a. Every member of the public should have the same access to court case records.
- b. The public is defined to include:
 - a. Any person, business, or non-profit entity;
 - b. Any governmental agency for which there is no existing policy defining that agency's access to court case records;
 - c. Any media organization; and
 - d. Entities that gather and disseminate information for whatever reason.
- c. The public does not include:
 - a. Court employees;
 - b. Entities who assist the court in providing court services;
 - c. Governmental agencies whose access to court case records is defined by another statute, rule, order, or policy; and
 - d. Parties to a case or their lawyers regarding access to the court record in their case (except possibly when access to information about opposing parties might pose a safety concern as with some domestic violence cases).
- d. Public access is synonymous with anonymous access.

Commentary: Enhanced access outside the public role may be partly addressed by establishing requirements for identification and authenticated access. Business rules for non-public access may be quite complex and best expressed by defining roles, relationships, and the specific scope of access by case type, document type and data type. When properly implemented, the public is one of many roles whose

¹² See Appendix D for definitions of court records, case records, administrative records, and other terms.

access is enforced by a common technical infrastructure. One version of the official case record is maintained and different levels of access are enforced using virtual redaction and masking. One interesting recent issue is that there may be a significant level of attempted access by non-human requestors.

Section 3.0 – Applicability of the Policy

Section 3.1 – General Access Rule

- a. Information in the court case record is accessible to the public except as prohibited by section 3.5 or 3.6.
- b. In general, there should be a public indication of the existence of case information in a record to which access has been prohibited, but that indication should not disclose the nature of the protected information.
- c. If harm may be done by indicating the existence of case information, then no indication of that existing record should be public.

Commentary: If a court hides the existence of case information or the case itself to prevent harm, it should make explicit the rationale it uses to determine when and why such protected information is hidden from the public.

Section 3.2 – Remote Access

All public court case records are presumptively accessible remotely.

Commentary: This section eliminates the ability to recreate “practical obscurity” by making all public court case records available at the courthouse but only a subset of those records available remotely. The principle underlying this part of the rule is that records are either public or not. The method of access should not affect that determination. In order to prevent harm, some court case records that were previously public may need to be closed. Improvements in automated redaction may mitigate that need.

Section 3.3 – Requests for Bulk Distribution of Court Case Records

- a. Bulk distribution of information in the court case record is permitted for public records.
- b. Requests for bulk distribution of information not publicly accessible can be made to the court for purposes with a public benefit. Courts have discretion to refuse such requests, to charge fees reimbursing the court for the cost of distribution, and to impose conditions on the requestor for access.

Commentary: If data are public, they are accessible even if in bulk form. The court has the right to make the requestor pay the cost of assembling and distributing the data in bulk form if they do not already exist in that format. The court may make

non-public data available for public purposes, but only if court users are protected from harm by imposing appropriate restrictions on access, use, and data retention. Bulk requests are often made by data aggregators and resellers. It is important that they provide to their customers only the most current versions of the court case record. A best practice is to require such users to “ping” the court database in real time to check for any changes.

Section 3.4 – Requests for Compiled Information from Court Case Records

- a. The public may request access to public court case records that are not normally compiled in the requested format. The court has the right to make the requestor pay the cost of compiling and distributing the data.
- b. Requests for compiled distribution of information not publicly accessible can be made to the court for purposes with a public benefit. Courts have discretion to refuse such requests, to charge fees reimbursing the court for the cost of distribution, and to impose conditions on the requestor for access.

Commentary: Requestors of compilations of non-public case information are typically barred by the court from selling the data to third parties or using the information to sell a product or service. Courts may impose additional restrictions to prevent harm. Model contracts are useful for ensuring both consistent policy use and comprehensive protection from potential harm.

Section 3.5 – Court Case Records Excluded from Public Access

- a. Court case information may not be made accessible to the public if barred by federal law, state law, court rule, or relevant case law.
- b. Court case records may also be excluded from public access if the court determines that harm would ensue, per the objective in section 1.0(b).

Commentary: Except for federal law, the details of what court case records are excluded from public access will vary from state to state and even from court to court in decentralized court systems. It is hard to predict how often case law might drive changes in what is public.

Common case types that are typically closed because of concerns about harm may include juvenile, family and probate. Document types typically closed include those that routinely include confidential personal information (such as financial disclosures) or potentially injurious but unsubstantiated assertions about opposing parties (such as divorce pleadings). Data types that are typically closed include identities and contact information of jurors, juveniles, witnesses, victims and other potentially vulnerable populations; financial account numbers; physical and mental health records; social security numbers; and other government identification numbers.

Consult the relevant National Institute of Standards and Technology (NIST) security standards on personally identifiable information (PII) that should be protected¹³. A best practice is to redact information in the most focused way that is technically and reliably possible. Thus, ideally, specific data elements should be masked by automated redaction. When that is not possible, then specific document types should be closed. When that is not possible, then specific case types should be closed.

Section 3.6 describes the desired business process for case-specific requests to access information otherwise barred by this section.

Section 3.6 – Requests for Exceptions to Access Policy

The courts will provide a standard process for requests to (a) prohibit access to certain public court case records, (b) allow public access to certain closed court case records, and (c) correct erroneous information in court case records. Court responses to such requests will balance the policy objectives in section 1.0.

Commentary: Considerations of harm should include (1) the risk of injury to individuals, (2) individual privacy rights and interests, (3) proprietary business information, and (4) public safety. The court should also consider applicable constitutional, statutory and common law. Where possible, explicit standard legal tests should be applied to such decisions.

It is an implementation best practice to provide the public with one centralized, easy-to-use website. The same website should support searches of public court case records, requests to expunge cases¹⁴, and requests for bulk or compiled case records.

¹³ See NIST Special Publication 800-122, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),” Erika McCallister, Tim Grance, and Karen Scarfone, April 2010 (<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>). See also “Guide to Protecting Personally Identifiable Information,” Shirley M. Radack, April 28, 2010 (<https://www.nist.gov/publications/guide-protecting-personally-identifiable-information>).

¹⁴ The Uniform Law Commission formed a Drafting Committee on Criminal Records Accuracy in 2014 and presented its first draft of uniform legislation in July 2016 (<http://www.uniformlaws.org/Committee.aspx?title=Criminal%20Records%20Accuracy>).

Section 4.0 – Timing of Public Access

- a. Remote access to public court case records is essentially available at all times, subject to publicly scheduled downtimes for system maintenance and unforeseen technical issues.
- b. Courts should make public court case records available in a reasonable time after filing. Courts should also respond within a reasonable time to requests for access to bulk or compiled case records and for requests governed by section 3.6, and inform the requestor when the bulk or compiled records will be available for dissemination.

Commentary: Remote access should essentially be 24/7/365. With electronic filing and reliable automated redaction, case records should become available for public access in near real-time after filing. Court responses to requests regarding public access should be “reasonable,” i.e. comparable to response times by other government agencies to similar requests.

Section 5.0 – Access Fees

- a. Any fees charged should be reasonable for the services provided.
- b. If fees are charged, there should be a process for requesting indigency waivers, except for bulk and compiled requests.

Commentary: There is no national consensus on the charging of fees. Courts may or may not charge fees for (1) remote public access to court case records, (2) bulk access, and (3) compiled information. There are currently three fee models used by courts: no fees (there should be no monetary barriers to publicly accessible information), fees that only cover the cost of providing access, and fees that exceed the cost of provision and provide additional revenue to the court. Requests for fee waivers based upon indigency should be made available as part of the same “one-stop shop” website that is recommended in the commentary to section 3.6 above.

Section 6.0 – Operational Requirements

Access policy provisions must be supported and implemented in a cost-effective, reliable and enforceable manner.

- a. Best practices should be used to protect court case records not open to the public.
- b. Search capabilities for public court case records should support reasonable flexibility.
- c. Search capabilities should not impose an undue operational burden on court systems.
- d. Persons or organizations granted access beyond what is available to the public should be managed by role and required to identify and authenticate using best practices.

Commentary: The best policy in the world does not adequately protect confidential information contained in court case records if a court does not also implement good security practices. The National Institute of Standards and Technology (NIST) identifies cybersecurity practices and processes in a series of national standards¹⁵. One of many examples is encryption of confidential data in the court database.

If courts offered complete flexibility in searches for publicly accessible data, it would be tantamount to giving the public the database. That would be expensive and risky. Thus, courts must decide what search parameters to support. That should depend partly what the public most often wants to search on and partly on what searches minimize the operational burden on court systems. Finally, public access is by definition anonymous access, so there is no identification of users. This is true for information available without modification. Requestors for bulk or compiled data may be required to identify themselves and comply with other requirements. Non-public access should be controlled using appropriate best practices for well identifying and authenticating other roles that have legal but limited access to non-public case records.

¹⁵ See especially NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013 (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>). NIST is currently working on Revision 5 (http://csrc.nist.gov/publications/drafts/800-53r5/draft_sp800-53-rev5_update-message.pdf). See also NIST's "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014 (<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>). NIST is currently updating its Cybersecurity Framework: a draft version 1.1 was released on January 10, 2017 (<https://www.nist.gov/cyberframework>).

Appendix B

State of the Art for Automated Redaction

Manual redaction of paper records is a time-consuming process. Many courts still manually redact paper files. As more courts are implementing electronic document management systems, or receive files through e-filing systems, there is a growing need to have technology provide redaction solutions in the digital environment. Many vendors have created platforms that have built-in electronic redaction capabilities, or allow for redaction and other related capabilities to be added on as a component provided by a selected vendor solution. The world has been going digital for some time. This will surely increase the demand for not only redaction capabilities, but other related process improvements as well.

Redaction of electronic files starts with the software going through the process of learning patterns to determine areas that have a probability of containing information that should be redacted. Machine learning uses statistical modeling methods to predict targets, and accomplishes this by analyzing a large volume of information. The initial analysis and learning is a human/machine process. The more volume the software learns, the more accurate it becomes at targeting desired information. Other techniques, such as algorithm based natural language processing, is used to extract information from semi-structured and unstructured text. Natural language processing (NLP) is a component of artificial intelligence (AI) combined with computational linguistics, and uses methods that allow the computer to understand and process human language rather than traditional programming language. Some examples of how NLP is used are autocorrect, speech to text, and language translation.

The perspective of court CIOs is gradually shifting away from case documents to information. That information may be standalone data, metadata, or content within documents. It may even take the form of digital evidence, including videos. Redaction software needs to be capable of handling this range of targets in a sufficiently granular way, and many vendors are working towards that goal.

As courts move toward automated workflows, the supporting software needs to seamlessly support and implement those kinds of business requirements. That means redaction software must integrate with e-filing, case management, and document management software. In the near future, it must also integrate with digital recording software and digital evidence databases. Even that daunting degree of software integration may not be enough, since some courts also utilize vendors for related tasks like file analysis, data loss, records retention, data masking, and e-discovery.

Evaluation Criteria

As courts move forward with pilot tests of automated redaction, it will be very useful to collect consistent evaluation data. Some evaluation criteria are suggested here:

- Accuracy and reliability
 - Structured expressions (like case numbers) in structured documents (like forms)
 - Structured expressions in unstructured documents (like scanned pleadings)
 - Unstructured expressions (like a victim's name) in structured documents
 - Unstructured expressions in unstructured documents
- Affordability and pricing structures
- Core functionality
 - Easy specification of redaction targets
 - Easy configuration of redaction requirements (such as reliability thresholds)
 - In-line redaction
 - Ability to train on test documents or data sets
- Integration capabilities
 - Public APIs
 - Integration with third party electronic filing service providers
 - Integration with court electronic filing software
 - Integration with court case management software
 - Integration with court document and content management software

Cost and Benefits

There are various costing models for redaction and other related enhanced features, and vendors have tried to offer some flexibility that takes into account the platform, volume, and level of functionality that the court will need. A common model is the transaction-based fee model, so volume matters. Other costing options might be site based licensing that considers estimated volumes. Several vendors expect court case management companies to offer comparable capabilities as part of their off-the-shelf products in a few years.

To justify the cost of using automated redaction, courts must make an argument for the value of the capability. In the absence of costly liability lawsuits, it is difficult to make a direct argument for the value of automated redaction targeted solely at removing confidential information. If such redaction enables a court to safely open case types and document types that would otherwise have to remain closed, and if that increased openness were perceived as valuable to outside organizations, then there may be political reasons to implement automated redaction.

As the software becomes highly accurate in its identification and understanding of specific target information, it opens opportunities to use this capability in other ways. For example, the software may allow for the information extraction that can support automated workflows and thereby save the court significant time and money that may create a direct business case for adequate value. Deriving that kind of value requires

much more than just implementing the redaction software itself. A court must carefully think through its workflows, identify appropriate automation targets, and often reorganize their administrative organization (staff and skill sets) to support a new way of doing business.

As courts explore new technologies, they should consider the variety of capabilities and their related benefits now available on the market:

- In addition to Optical Character Recognition (OCR), some vendors offer Intelligent Character Recognition (ICR) that can be used for handwritten court case records. A similar capability for audio and video files is developing rapidly.
- In addition to automated data identification, some vendors offer an index that can be used to compare newly filed information to existing court case data (for example, does the party's name on the incoming case submission match the party's name in the court's case management system?).
- Some electronic content management systems offer configurable workflow engines: once the processes of OCR/ICR, automated data identification, and indexing are complete, the ECMS will apply the court's business rules and automatically route the filing to the appropriate next step in the court's workflow such as automated case entry and docketing.
- Enhanced functionality may allow for extracting data from electronic documents and automated entry in case managements systems and/or other databases.

Corrections:

The previous version of this appendix listed Mentis as being part of an Arkansas study. This reference has been removed, but this correction is to clarify that Mentis was not part of the Arkansas study.

A specific vendor listing for redaction software has been removed. The various approaches, integration methods, technology capabilities, and pricing models used by vendors cannot be suitably characterized in a simple list of redaction vendors. It is better for courts to research each solution to determine which approach, capabilities, and pricing structure best fits their platform and needs.

Appendix C

Automated Workflows Using Automated Extraction

Vendors of automated redaction software rightly point out that the ability to arbitrarily locate specified content in court case records potentially enables courts to use that information to automate court business processes in ways that can make courts markedly more efficient. Thus, redaction software might be better thought of as *data extraction software*. Such software enables courts to gather data at the time of filing for use later in a case. This is part of a larger paradigm shift from business processes built around case files and documents to processes based on data¹⁷.

Business Values of Data Extraction Software

Once a court starts down the path of using data extraction to power its business processes, several business goals become achievable:

- Shorten the processing times for court filings and case dispositions.
- Reduce the number of court staff needed to process court filings, manage cases, implement records retention and archiving policies, and respond to records requests.
- Provide more granular public access to court case information.
- Provide appropriately redacted court case records in near real-time, reducing the lag time in publishing new case filings to the media.
- Reduce the risk of exposing confidential court case information to the public.
- Expand the scope of legacy court case records that are available for remote public access, while automating enforcement of retention and archiving policies.
- Improve the quality of court data, from the moment of filing.
- Support more sophisticated analytics of court case information.

Case Management Improvements with Extracted Information

Right now, electronic filers must input data about the filing into a so-called “envelope” so that a court can process it. Some of this “metadata” (data about data) could be extracted directly from the documents being filed, eliminating a data entry step. An important example of such metadata is the document type. Filers must currently either know or select from lists a correct document type, which is usually then checked again manually by a clerk. With high frequencies of self-represented litigants, errors in selecting document types are often made and court resources must be used to correct them. Data extraction technology can be used to reliably and automatically assign document types.

¹⁷ This appendix is based on work done by Alan Carlson for the project focus group.

Obviously, the same approach can be used to assign case types and characterize case parties and their relationships. Thus, data about the case can also be extracted to drive subsequent workflows, especially those needed to perform initial triage and place a case into a case processing track. With powerful data extraction capabilities, such automated triage and case management can support business rules of arbitrary complexity, enabling courts to control cases in a much more fine-grained manner than was historically possible using manual resources. This enables courts to much better follow the dictum of allocating the right resources and attention to each case.

In a similar manner, a court can extract data from filings to help judicial officials make case decisions and issue court orders. Examples include “feeding” parents’ financial data into child support calculators and populating draft court orders with extracted case data.

Data extraction software can do all these tasks more consistently and reliably than humans can, once it is possible at all. Data extraction technology could ultimately eliminate the need for both e-filing envelopes and case cover sheets.

Appendix D

Definitions

Administrative Record – Court records that pertain to management, supervision, or administration of the court and are not part of a case record.

Automated Case Triage – A method of differentiating cases by assigning them to a track early based on issues and corresponding processing requirements, rather than case type. This method also provides litigants with alternate choices from traditional litigation that might offer a more rapid resolution at lower costs.

Automated Workflows – A well-defined set of business processes where information is exchanged and automated actions take place based on a set of procedural rules.

Bulk Distribution - The distribution of all, or a significant subset, of the information in court case records without modification or compilation.

Case Record - Any document, action or information that is collected, received, or maintained by a court or clerk of court connected to a judicial proceeding. It may include an index, calendar, docket, register of actions, official record of the proceedings, order, decree, judgment, minute order. These may have been collected in a case management system that is used to track information. Case records may contain both public and confidential information.

Court Records – The sum of all administrative and case records in the judicial branch.

Compiled Information - Information that is derived from the selection, aggregation or reformulation of some specified subset of data from more than one individual case record.

Data Extraction – An automated means of taking data out of structured forms or using machine learning and other mechanisms to take data out of unstructured text for use.

Machine Learning – A type of artificial intelligence (AI) that uses patterns and predictive analysis to draw inferences and act without the need for precise programming. Inferences become more precise with greater use.

Metadata – Data that provide additional information about another data source to put the information into context, such as title, author, subject, creation date.

Practical Obscurity – A concept based in a paper record environment where an individual's information in government files enjoys some level of privacy because access is limited to an on-site review of a paper file.

Predictive Analytics – An advanced analytics technique using statistical analysis that utilizes new and historical data to forecast the probability of future activity, behavior and trends.

Redaction – The process of obscuring confidential information contained within a public record from view. Redacted portions of the record are blacked out or masked. Redaction may be accomplished manually or through use of technology such as data identification software.

Remote Account Access – Electronic access to records based on role that is defined by rule or statute, and authentication of that role. This access may include greater view of the redacted or un-redacted information in a case file that one may be a party to or that is required as part of an agency service or function.

Remote Public Access – The ability to electronically search, inspect, or copy information in a court case record without the need to physically visit the court facility where the case record is maintained. This generally does not require any type of login or the need to provide identifying information about the member of the public accessing the case record.

Structured Data – Information contained in a database or structure where the information may be readily identified and used. In the context of data extraction software, structured data are identified based upon their unique patterns. Examples include United States Postal Service zip codes, Social Security numbers, and phone numbers.

Unstructured Data – Information not contained in a data structure or database, such as text in documents or multimedia files such as digital recordings of audio or video without XML markup.