ACLU OF MAINE FOUNDATION
121 MIDDLE STREET
SUITE 301
PORTLAND, ME 04101
(207) 774-5444
WWW.ACLUMAINE.ORG

Comments on Recommendations of the Task Force on Transparency and Privacy in Court Records

Zachary L. Heiden, Esq.
ME Bar No. 9476
Legal Director, American Civil Liberties Union of Maine Foundation
121 Middle Street, Suite 200
Portland, Maine 04101
(207) 774-5444
heiden@aclumaine.org

November 14, 2017

As a member of the Maine Judicial Branch Task Force on Transparency and Privacy in Court Records ("TAP"), I fully endorse the conclusions and recommendations of the taskforce. I submit these comments to explain why the ACLU of Maine believes that these recommendations serve to safeguard the twin interests of open access and privacy.

If accepted, TAP's recommendations would mark a substantial expansion in access to court records in the state of Maine. Under the current paper system, no information is available online. Instead, parties and the public alike must visit the relevant clerks' office to uncover even the most rudimentary case information. Nor may they

access information from the nearest court, but instead must identify the clerks' office where the case resides, and travel there—however far. Or they must pay for the court to process a records request.

The new system, by contrast, will place important court-generated information online, just a click away. *Report of the Maine Judicial Branch Task Force on Transparency and Privacy in Court Records ("TAP Report")*, at 16-17, (September 30, 2017) (also listing exceptions for juvenile cases and certain criminal dismissals). To access other filings, the public may travel to *any* clerks' office. *Id.* at 16-17. Parties and counsel of record, in turn, will have full electronic access to all filings in their cases. *Id.* These changes advance the goal that "government operations . . . be open and transparent." *Id.* at 1.

At the same time, TAP recommends measures to ensure privacy concerns are not trampled during the transition to electronic court records. *See, e.g.*, *TAP Report* at 16-18. As TAP correctly acknowledges, "private individuals have a valid interest in and a right to expect that their own private information will be handled appropriately." *Id.* at 1.

TAP's recommendations strike a reasonable balance between the twin goals of access and privacy. As explained below, digital records are

qualitatively different than paper records. Extending access to electronic platforms thus implicates different privacy concerns and merits caution. Additionally, TAP's recommendations echo the conclusions of prior efforts in the transition to electronic court access. In sum, TAP's recommendations are reasonable, especially as Maine's first attempt at system-wide electronic records.

I. Digital Is Different

Digital information is qualitatively different from paper-based records. For hundreds of years, a court record was a written or printed document, which existed in one place at one time. The age of mechanical reproduction allowed for court records to be copied and disseminated, but they were still objects that existed in physical space. In contrast, an electronic court record is simply information--a collection of ones and zeros--which is stored on a computer server that could be located anywhere in the world.

The implications of digital data are enormous, and they are both positive and negative. Concerning court records, this change means that more people can more easily obtain information about what is happening in our court system, whether it involves their own personal

legal matters or matters of public concern. But, it also means that the sensitive information contained in court records is more easily located and disseminated, imperiling personal privacy.

The United States Supreme Court has recognized this new reality, it its landmark decision in *Riley v. California*, requiring police officers to obtain a search warrant before examining the contents of a cellphone seized incident to an arrest. *See Riley v. California*, 134 S. Ct. 2473 (2014). In *Riley*, the government argued that a search of electronic data contained in a cellphone is "materially indistinguishable" from searches of physical items, such as address books, wallets, and notes, which are permitted without a warrant. *See id.* at 2488. Writing for a unanimous court, Chief Justice Roberts rejected that argument, noting that comparing a search of all data contained in a cellphone to a search of physical documents contained in a person's pocket was "like saying that a ride on horseback is materially indistinguishable from a flight to the moon. . ." *Id.* "Both," Chief Justice Roberts wrote, "are ways of getting from Point A to Point B, but little else justifies lumping them together." *Id.*

Though a search of the physical contents of a person's pockets may not constitute a cognizable privacy intrusion, that reasoning cannot be logically extended to digital data that may have overlapping characteristics. *See id.* at 2489. Digital data is different. Magnitudes more data can be stored digitally in a smaller space, and it can be analyzed to reveal patterns with greater speed and accuracy.

Searching through a physical record or document, whether found in a criminal suspect's pocket or in a physical file takes time and effort. And, there is a physical limit on how much information can be contained in a physical case file or in a person's pocket. These physical concerns provide a measure of protection that members of the public have come to rely upon, and which the courts ought to recognize as reasonable.

The transition to digital data eliminates these practical protections. As the Supreme Court noted in *Riley*, "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read." *Id.* at 2489. But, all that data is easily and frequently contained in a cellphone. Similarly, most people would not sort through

the finances, health records, and family histories of all the people seeking to get divorced in a given county, yet the transition to electronic records makes such a search easy to do from any computer anywhere in the world.

II. Placing Digital Data Online Can Pose A Unique Threat To Privacy

Making digital data publicly accessible online can pose unique threats to privacy. Other courts have recognized this principle. For example, in *EW v. New York Blood Ctr.*, the court allowed the plaintiff to proceed under a pseudonym, comparing "access to court files by those surfing the internet" to the "modern enterprise and invention" identified by Samuel Warren and Louis Brandeis as capable of inflicting greater mental harm through the invasion of privacy "than could be inflicted by mere bodily injury." *EW v. New York Blood Ctr.*, 213 F.R.D. 108, 112-13 (E.D.N.Y. 2003) (*quoting* Warren & Brandeis, *The Right to Privacy*, 4 Harv.L.Rev. 193, 196 (1890)).

And, in *Doe v. Cabrera*, the court permitted a plaintiff to use a pseudonym in her civil action concerning sexual assault, over the defendant's objection that the plaintiff chose to bring the suit knowing that her identity would be revealed in the process. *Doe v. Cabrera*, 307

F.R.D. 1, 6 (D.D.C. 2014). The court rejected that objection, noting that, in the age of electronic filing, simply being identified in connection with a lawsuit could subject the plaintiff to "unnecessary interrogation, criticism, or psychological trauma." *Id.* at 7. While the court noted its appreciation for "the public benefits of the Internet," it expressed concern over the internet's "unfortunate drawback of providing an avenue for harassing people." *Id.*

III. TAP's Recommendations Accord With Past Efforts To Transition To Electronic Court Records

The balance struck by TAP's recommendations echoes past efforts to transition to electronic court records. In 2005, the Maine Supreme Judicial Court Court created the Maine Taskforce on Electronic Court Records Access (TECRA), to consider the legal and policy ramifications of transitioning from paper to electronic court files.[1] TECRA recommended the adoption of a two-tier approach to private information: (1) confidential information would not be available in any form, and (2) information that is sensitive or that could expose a person to needless harm would be available in person by request at a courthouse but not on a court website. *See Maine Supreme Judicial*

[1] I also served as a member of that taskforce.

Court, Report of the Maine Taskforce on Electronic Court Record Access ("TECRA Report"), 7-8 (September 26, 2005).

In recognizing this second tier of matter—private but not confidential—TECRA breathed life into the concept of "practical obscurity," which applies to records held in paper form in a particular physical location. Such records are protected, though not as absolutely protected as sealed records. That does not make the protection any less meaningful because, as TECRA observed, "[a]lthough the data is theoretically available, it is very unlikely that it would ever be viewed by anyone or widely disseminated due to the fact that it is too inconvenient to uncover." *Id.* "By contrast, electronic data or documents are accessible to an anonymous inquisitor at the click of a button." *Id.* at 9.

TAP has endorsed this important principle as well, noting that "[w]hen individuals go to the courthouse to access files, they must do so in an open manner," while "individuals who access information online can anonymously probe" legal material whether their purpose is benign or malignant. TAP Report, 10. And, TAP member Peter J. Guffin, Esq. further elaborated that personal records were "once protected by the

practical difficulties of gaining access to the records," but the transition to electronic records removes that layer of protection. *TAP Report*, Attachment 5a, Concurring Report of Peter J. Guffin, Esq., 1.

TAP observed that this "practical obscurity" is a way of providing meaningful protection for private material that is not legally confidential, as courts manage the transition from primarily paper to primarily electronic records. This, it is hoped, will minimized the dangers of unforeseen complications, such as the likelihood that domestic violence victims will be less likely to avail themselves of the court's protection if their names and case files are available to casual online browsers, or that financial crimes or identity theft will become even more common.

Some have characterized TAP's proposals as "limiting" court access, but this position ignores the fact that much more information is going to be publicly available if TAP's recommendations are adopted than is available now, to the benefit of litigants and interested members of the public alike. Courts are under no obligation to publish court records on the internet, and doing so creates a very real risk, as discussed in the TAP Report Concurrence of Pine Tree Legal

Assistance, Legal Services for the Elderly, Maine Coalition Against Sexual Assault, Maine Coalition to End Domestic Violence, and Maine Network of Children's Advocacy Centers. *See TAP Report*, Attachment 5b. Courts of all kinds have an obligation to protect the rights of people who come into court, and for that reason, the TAP recommendations have received the ACLU of Maine's support.

IV. TAP's Recommendations Are A Reasonable Transition Measure

Finally, it is important to remember that this is the first step for Maine court records, not the last. As such, it is proper that the Judicial Branch proceed with caution. In time we anticipate that new approaches and processes will be developed to provide even greater public access to information, while also providing even greater privacy protections for those who seek justice in Maine's courts.