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

Peter J. Guffin, Esq.
ME Bar No. 3522
Partner, Pierce Atwood LLP
254 Commercial Street
Portland, Maine 04101
(207) 791-1199
pguffin@pierceatwood.com

December 15, 2017

As a member of the Maine Judicial Branch Task Force on Transparency and Privacy in Court Records ("TAP"), I submit these additional comments to explain why I support TAP's recommendations and believe that they strike the appropriate balance between the goals of open access and protection of citizens' privacy rights.

There is a vast difference between digital records which are made available online 24/7 via the Internet and paper-based records which are accessible only at the courthouse during regular business hours. In addition to unfettered accessibility, broad and widespread dissemination, and no user accountability, there is a complete loss of control with digital records, such that they effectively become permanent – the Internet never forgets. Courts and others properly recognize the increased threat to privacy by placing digital records online. Ignoring those realities would be a mistake in my view.

The Maine state court system handles many different types of matters and special dockets which often involve the collection by the courts of very intimate and sensitive personal information of individuals, some of whom are extremely vulnerable. Individuals generally are not in a position to refuse providing this information to the court, so choice is not always an

option for individuals. Illustrative matters include divorce, parental rights, parentage, juvenile, veteran and sexual abuse proceedings. In addition, many of the matters in the Maine state court system are handled by the parties *pro se*.

If appropriate policies and rules are not put in place to protect such personal information by the Maine Judicial Branch ("MJB"), individuals may be at significant risk of potential physical, emotional and other harm, including blackmail, extortion, stalking, bullying, and sexual assault. In addition to privacy rights, other constitutionally protected citizens' rights may be implicated if the court grants online public access to such information without appropriate controls in place.

Citizens' rights should not be left behind at the courthouse doors. The public rightfully expects that the courts will respect and protect citizens' privacy rights in the courthouse. If the MJB fails to do so, it risks losing the trust and confidence of the public.

As the collector and holder of sensitive personal information, the Court has a duty to protect individuals against the widespread dissemination of such information to the fullest extent permitted by law.

As Justice Brennan once cautioned: "[B]road dissemination by state officials of [sensitive personal] information . . . would clearly implicate constitutionally protected privacy rights, and would presumably be justified only by compelling state interests. *Whalen v. Roe*, 429 U.S. 589, 606 (1977) (Brennan J., concurring). As he also presciently observed: "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." *Id.* at 607.

Similarly, in a case quashing a government subpoena for redacted medical records relating to late-term abortions performed at a hospital, Judge Posner observed:

> Some of these women will be afraid that when their redacted records are made a part of the trial record in New York, persons of their acquaintance, or skillful "Googlers," sifting the information contained in the medical records concerning each patient's medical and sex history, will put two and two together, "out" the 45 women, and thereby expose them to threats, humiliation, and obloquy. As the court pointed out in *Parkson v. Central DuPage Hospital,* [citation omitted] "whether the patients' identities would remain confidential by the exclusion of their names and identifying numbers is questionable at best. The patients' admit and discharge summaries arguably contain histories of the patients' prior and present medical conditions, information that in the cumulative can make the possibility of recognition very high."
>
> *Northwestern Memorial Hosp. v. Ashcroft,* 362 F.3d 923, 929 (7th Cir. 2004).

Recent developments in technology have dramatically altered society's conception of citizens' privacy rights and expectations. We see this change reflected in an increasing number of recent federal court decisions involving the Fourth Amendment of the U.S. Constitution. Illustrative of this recognition is Justice Sotomayor's concurring opinion in *United States v. Jones*, in which she wrote:

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.
>
> 565 U.S. 400, 417 (Sotomayor, J., concurring).

The same recognition is expressed by state and federal courts across the county in other contexts, including electronic court records. *See, e.g., In re Boston Herald, Inc.*, 321 F.3d 174, 190 (1st Cir. 2003) (holding "[p]ersonal financial information, such as one's income or bank account balance, is universally presumed to be private, not public [citation omitted] [and that] Connolly's strong interest in the privacy of his and his family's personal financial information outweighs any common law presumption [of public access]. . . ."). In the latter case, Judge Lynch, writing for the majority, reaffirmed that: "There is no general constitutional right of access to information in the government's possession. . . . The right to speak and publish does

not carry with it the unrestrained right to gather information" (citing *Houchins v. KQED, Inc.*, 438 U.S. 1, 15, 98 S.Ct. 2588, 57 L.Ed.2d 553 (1978) (plurality opinion)).

The MJB's rules with respect to public access to digital court records, in my view, should align and keep pace with society's evolving conception of citizens' privacy rights and reasonable expectations. The rules of course should not be written in stone. Rather, they should be reviewed regularly and may need to change to adapt to future changes in technology and citizens' privacy expectations.

In sum, unwarranted invasion of privacy should not be the price citizens have to pay to litigate private matters in court. The press' claim for open access is not the only important interest at stake here. There are other compelling interests, including citizens' privacy rights and other state and societal interests. I believe the TAP recommendations strike the right balance between these competing interests and successfully achieve the twin goals of transparency and privacy.