Peter J. Guffin, Esq.

ME Bar No. 3522

Comments Regarding Access to Electronic Court Records

Before the Maine Supreme Judicial Court

Date of Public Hearing: June 7, 2018

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

My name is Peter Guffin. I am here today in my personal capacity as an interested and somewhat informed member of the Bar to speak in support of the recommendations of the TAP Task Force, of which I had the privilege to serve as a member. I am not here today speaking on behalf of any client or other organization.

The views expressed by me today are solely 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.

I wish to use my allotted time this morning to build upon a very specific concept that is central to the privacy versus transparency discussion today. The concept is not new and has been touched upon briefly by the Task Force as well as

others, but I believe it deserves more attention. I do not plan to rehash the views previously expressed by me in my concurring report accompanying the Task Force report or the additional comments submitted by me on December 15, 2017. I continue to stand by them fully.

The concept I am talking about is "public" information. Without question, it is a powerful and entrenched concept, essentially functioning today as a permission slip providing cover for a wide variety of data practices, some of which are unscrupulous and dangerous.

"Public" information is not an established and objective concept, however. Although widely used, the term "public" has no set definition in law or policy as far as I am aware. It is an amorphous concept and can mean different things depending on the context.

Having said that, the point that I wish to make is that labeling something as "public" information is a decision that is both value-laden and consequential. "Public" is not a neutral notion, separate from legal and social construction. Designating a court record as "public" information is an exercise of power, and I urge the Maine Supreme Judicial Court to make sure that, in doing so, such designation embodies the values it wants to serve, the relationships and outcomes it wants to foster, and the problems it wants to avoid.

With the Judicial Branch's move to e-filing and electronic access to court records, now is the time to recalibrate the complex balance between the privacy dangers of disclosure and the societal benefits of transparency and to reconsider what court records (or portions thereof) should be designated as public.

Viewing privacy through the ages, we learn that technology advances, such as the ones at issue today regarding e-filing, electronic access and the internet, are often the catalyst driving the desire and need to re-negotiate society's relationship with privacy.

What does it mean to say a court record is public information?

What is the meaning of "public" information in the context of electronic access to court records?

In many cases, saying information is public means it is free for others to observe, collect, use and share. Saying it is private, on the other hand, signals that there might be some rules people need to follow.

Does designating a court record as public information mean the information must be made freely available and easily accessible to anyone and everyone on the planet, 24/7, immediately upon filing and forever thereafter, without restrictions or limitations of any kind, and with permission for the recipients to use with complete impunity?

In my view, the concepts of obscurity and trust should be incorporated into the calculus for determining whether information in court records is designated as public. These concepts play an important role in shaping people's behaviors and perceptions of risk regarding their interaction with the courts and more specifically their expectations of privacy with respect to the personal information they share with the court system.

Put another way, the reasonable privacy expectations of citizens, while not necessarily determinative, should at least be taken into account in determining whether information is made public.

Do parties and witnesses involved in a litigation understand the privacy implications of their disclosing to the court sensitive personal information, whether their own or that of others? That is, do they understand that such disclosure is going to act as a waiver of their right and the right of others to protect that information?

In my view, not all "public records" must or should be made available to the public via remote electronic access.

In reconsidering the balance between privacy and transparency as it enters the digital age, the Judicial Branch should be mindful of the abundant caselaw, which holds that privacy can and does exist in public records.

Under the privacy exemption in the federal Freedom of Information Act (FOIA) and similar state laws, courts have consistently held that "[a]n individual's interest in controlling the dissemination of information regarding personal matters . . . does not dissolve simply because that information may be available to the public in some form or from other sources. In other words, the fact that otherwise private information at one time or in some way may have been placed in the public domain does not mean that a person irretrievably loses one's privacy interest in that information or has no interest in limiting the disclosure or dissemination of the information. In particular, even if information was at some time or place publicly available, a privacy expectation may exist if the information is now hard to obtain and, for a practical matter, now obscure." 37A Am. Jur. 2d Freedom of Information Acts § 239 (citations omitted).

Under the federal Privacy Act, courts likewise have held that even publicly accessible information is protected from disclosure. *Quinn v. Stone*, 978 F.2d 126 (3d Cir. 1992); but see *Barry v. U.S. Department of Justice*, 63 F. Supp. 2d 25 (D.D.C. 1999) (distinguishing *Quinn* and holding that a record widely accessible to the public was not protected by the Privacy Act.) In *Quinn*, the court noted that it could find no court to conclude that information already in the public domain could not be protected, stating: "[a]ppellees have cited to this court no case that stands for the proposition that there is no violation of the Act if the information is merely

readily accessible to the members of the public (such as in the local telephone book) and our research has discovered none. We doubt if any court would so hold. To do so would eviscerate the Act's central prohibition, the prohibition against disclosure. For instance, such an argument would short-circuit the delicate balancing courts now engage in between the FOIA and the Privacy Act under 5 U.S.C. § 552a(b)(2). See *FLRA v. U.S. Department of the Navy*, 966 F.2d 747 (3d Cir. 1992) (en banc). To define disclosure so narrowly as to exclude information that is readily accessible to the public would render superfluous the detailed statutory scheme of twelve exceptions to the prohibition on disclosure." *Quinn*, at 134.

This same idea – that privacy can exist in public information – also finds expression in jurisdictions outside the United States. The United Kingdom's Information Commissioner's Office's (ICO) approach to determining what falls into the public domain is instructive. The ICO has a relatively nuanced approach to what constitutes falling within the public domain. Critically, it has determined that "[e]ven if the information itself is already in the public domain, this is not decisive and is not an automatic argument either for or against disclosure."[1] Rather, several different considerations must be weighed before the decision to make information freely available.

[1] Information in the public domain, Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/1204/information-in-the-public-domain-foi-eir-guidance.pdf. At 11.

It is well recognized that the obscurity of people and data and the existence of relationships of trust are two of the most important factors that shape peoples' behavior and perceptions of risk in any given environment. People feel relatively safe when their acts and data exist in zones of obscurity and are disclosed within relationships of trust.

The importance of obscurity with respect to public information was recognized by the U.S. Supreme Court in *United States D.O.J. v. Reporters Comm. for Freedom of Press*, 489 U.S. 749 (1989). There, the Court wrote that "the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private." *Id.* at 763. The passage of time makes information harder to recall because people forget things, records get lost, databases get deleted, and links rot. Information has a natural way of becoming obscure.

Another example of attempts to integrate obscurity into public information doctrine comes from the United Kingdom's ICO's guidance on public records regarding what information is in the "public domain." The ICO has determined that "[i]nformation is only in the public domain if it is *realistically* accessible to a member of the general public at the time of the request. It must be available *in practice*, not just in theory." The ICO goes on to provide nuance, stating that "information will not be in the public domain if it would require unrealistic

persistence or specialized knowledge to find it, even if it is theoretically available somewhere in a library or on the internet. In practice a normal member of the public would still not be able to find that information." The ICO defined a member of the general public as "a hypothetical average member of the general public who is interested enough to conduct some searches for the information, but does not possess any specialized knowledge or research skills."

The calculus for what makes things obscure is complex and includes many different factors like searchability, permanence, comprehensibility, identifiability, and the resources, motivation, and pre-existing knowledge of those who seek to surveil or make use of data. In my view, these factors should be considered when formulating the concept of public information.

Relationships of trust also should be considered as part of such formulation in my view. Trust is a relevant factor for evaluating whether the actual recipients of information render certain disclosures public. These recipients need not be full-fledged "confidants" in the formal sense of the word. People trust others to be discrete, loyal, honest, and protective all the time without demanding a formal obligation of confidentiality. They adjust their risk calculus based on this trust and the likelihood that the information will not travel too far or be used against them.

In my view, maintaining this kind of trust in the court system is critically important.

Limited disclosures generally carry with them expectations of discretion and loyalty, hallmarks of trust, which are recognized in the law of public records. Promises of confidentiality are "generally given weight with regard to an individual's expectation of privacy" and the privacy exception of the Freedom of Information Act. The United Kingdom ICO likewise holds that "[i]nformation disclosed only to a limited audience will not generally be in the public domain, as it is unlikely to be available to a member of the general public."

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).

In closing, unwarranted invasion of privacy should not be the price citizens have to pay to litigate private matters in court. The Maine Judicial Branch's rules with respect to public access to digital court records should align and keep pace with society's evolving conception of citizens' privacy rights and reasonable expectations. The rules should be written to support the Maine Judicial Branch's mission to administer justice by providing a safe, accessible, efficient and impartial system of dispute resolution that serves the public interest, [and] protects individual rights…." 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.

I believe the TAP recommendations at this time strike the right balance between the competing interests of transparency and privacy and should be adopted.

Thank you. I am happy to answer any questions.