

Testimony Against

LD 1759, An Act Regarding the Electronic Data and Court Records Filed in the Electronic Case Management System of the Supreme Judicial Court

May 28, 2019

Senator Carpenter, Representative Bailey and members of the Judiciary Committee:

My name is Peter Guffin. I am a member of the Maine Bar and a practicing attorney. In 2017 I served as a member of the Maine Judicial Branch Task Force on Transparency and Privacy in Court Records.

Because prior professional commitments will prevent me from attending the public hearing later today, I offer these written remarks in the hope that they will assist you in your work.

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.

I urge the Judiciary Committee to issue a report recommending that LD 1759 ought *not* to pass.

First, the bill oversteps the Legislature's power and authority under the Maine Constitution. **Second**, the bill not only intrudes on the Supreme Judicial Court's exclusive authority to exercise judicial power, it also impinges on the Court's ability to interpret the expansive concepts of privacy and transparency in the context of digital court records access over time and to carry out its core function of making judgments among competing interests and values. **Third**, the bill lacks important measures to protect the privacy rights of Maine citizens, measures which do fall *within* the prerogative of the Legislature.

Separation of Powers

The bill imposes on the Supreme Judicial Court certain rulemaking parameters in connection with its developing and adopting rules addressing the management of

and access to electronic data and court records filed with or generated by the state courts and stored in an electronic case management system. The bill also establishes general policies for the Supreme Judicial Court regarding access to electronic court records.

The management of court records – paper or digital - is at the core of the judicial power. *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978) (“Every court has supervisory power over its own records and files.”) The bill thus oversteps the Legislature’s power and authority under the Maine Constitution.

The bill also directly conflicts with past precedent in which the Supreme Judicial Court has held that under the Maine Constitution it holds the exclusive authority to exercise judicial power.

In a strikingly analogous context, in the direct letter of address dated April 25, 1986 submitted by a unanimous Supreme Judicial Court to the Honorable Joseph E. Brennan, then Governor of Maine, the Honorable Charles P. Pray, then President of the Senate, and the Honorable John L. Martin, then Speaker of the House of Representatives, the Supreme Judicial Court declared that it was “compelled by the Maine Constitution not to follow the expressed mandate of the Legislature,” stating in part as follows:

“With the enactment of P.L. 1985, ch. 515, which becomes effective July 16, 1986, the Legislature has directed this Court to promulgate rules governing photographic and electronic media coverage of proceedings in the trial courts of this State. Upon due consideration, this Court concludes that the governance of media access to courtrooms is within the judicial power committed to this Court by the Maine Constitution. Me. Const. art. VI, §1. Chapter 515 constitutes an exercise of judicial power by the Legislature in violation of the provisions of the Constitution allocating the powers of government among three distinct departments and forbidding any person belonging to one department from exercising any power properly belonging to another department. Me. Const. art. III, §§ 1, 2. Accordingly, we respectfully decline to promulgate rules as contemplated by the legislative act.”

Earlier this year the Supreme Judicial Court solicited public comments regarding its proposed draft Digital Court Records Access Rules. Those rules are still under consideration by the Court.

The bill is ill-conceived and unconstitutional and appears to be an attempt to do an end-run-around the Supreme Judicial Court's deliberative rulemaking process already underway.

Transparency and Privacy

The core function of the Supreme Judicial Court is to properly interpret the concepts of open access and privacy *in context over time* and to make judgments among competing interests and values.

As concepts, open access and privacy are broad and expansive ideas and values that require fresh thinking to be applied in specific circumstances. As Judge Coffin wrote,

“[t]he emphasis on fairness, the entitlement of each person to equal respect, the view of the great clauses in the Bill of Rights as concepts, susceptible of adjustment in each era rather than as fixed, specific conceptions, the recognition that the authoritative construction of these clauses is not the province of the majority, and the caution that the proper approach to individual rights is not simply a ‘balancing’ of the rights of individuals against those of society, but rather a tilt toward the individual – all these spell a different, individual-oriented jurisprudence..”

Frank M. Coffin, *The Ways of a Judge: Reflections from the Federal Appellate Bench* (1980), at 240.

The bill lays out certain, particular rules concerning the electronic case management system, thus establishing “fixed, specific conceptions” or embodiments of the general concepts of privacy and transparency which are incomplete and subject to being applied reflexively without the necessary reevaluation and recalibration from time to time in response to advances in technology and changes in societal norms and citizens’ reasonable expectations of privacy.

In doing so, the bill ignores the bigger picture and does a disservice to the broad and expansive interests and values reflected in those concepts. It also impinges on the Supreme Judicial Court's ability to interpret the concepts of privacy and transparency in the context of digital court records access over time and to carry out its core function of assessing these values and making determinations related to the proper functioning of the court systems and in the interests of justice.

As the Supreme Judicial Court itself has acknowledged, it is no easy task to interpret the concepts of privacy and transparency in the context of digital court records and to make judgments among competing priorities.

The difficulty and complexity of the issues at hand cannot be understated, and the need for resolving these issues correctly is of utmost importance to Maine citizens. The stakes are very high, not only for individuals but for society as a whole and the Maine state court system as an institution.

In 2017 the Supreme Judicial Court convened a task force to study the issues and to offer policy recommendations about digital court records access and management. Since then, on at least four separate occasions, the Supreme Judicial Court has solicited and received public comments about these issues.

The comments submitted by the public and various stakeholders, of which there were many, are very thoughtful and informative. To acquaint the Committee with some of the difficult and complex issues, I have attached to my testimony the comments that I submitted to the Supreme Judicial Court regarding its proposed Digital Court Records Access Rules.

Short of divine revelation, it is presumptuous to think that with a few short strokes of the pen this bill can resolve all of these issues.

Privacy Measures Lacking

The bill lacks important measures to protect the privacy rights of Maine citizens, measures which *do* fall within the prerogative of the Legislature.

It is well known that the personal data in court records can expose citizens to targeting by unscrupulous marketers and worse (e.g., stalkers, harassers, and

perpetrators of fraud). It also is well known that data brokers, an industry that is largely unregulated and often hidden from public view, have sold the following lists:

- Rape survivors
- Addresses of domestic violence shelters (which keep their locations secret under law)
- Police officers' and state troopers' home addresses
- Genetic disease sufferers
- Senior citizens suffering from dementia
- HIV/AIDS sufferers
- People with addictive behaviors and alcohol, gambling and drug addictions
- People with diseases and prescriptions taken (including cancer and mental illness)
- Consumers who might want payday loans, including targeted minority groups
- People with low consumer credit scores

World Privacy Forum, *Testimony of Pam Dixon, Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information Do Data Brokers Have on Consumers, and How Do They Use It?*, Dec.18, 2013.

One of the most common sources of citizen data is public record information, including information in court records.

Despite all of this awareness and knowledge, the bill contains no measures whatsoever designed to protect citizens' privacy rights, mitigate harm, or provide citizens with measures to seek remedies. For example, the bill contains

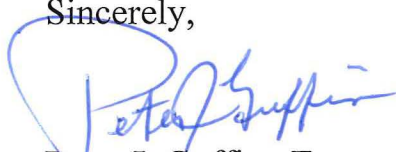
- no prohibition on the misuse of citizens' personal information
- no prohibition on the acquisition of personal information through fraudulent means or with the intent to commit wrongful acts
- no provision for individual remedies in the event of misuse of their personal information.

Conclusion

For all of the foregoing reasons, I urge the Committee to issue a report recommending that LD 1759 ought *not* to pass.

Thank you for your time and consideration.

Sincerely,



Peter J. Guffin., Esq.

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:

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.