Canada's Courts Online: Privacy, Public Access and Electronic Court Records

Elizabeth F. JUDGE*

* Assistant Professor, Faculty of Law, Common Law Section, University of Ottawa, Ottawa, Ontario.

Finding the delicate balance between access to public records and personal privacy has been characterized as "one of the most challenging public policy issues of our time."[1] Court records are a subset of the larger category of "public registries". Public registries can be defined as lists of personal information that are under the control of a public body, maintained by rule, statute or practice, and open in whole or part to public inspection, copying, or distribution. Court records have several special characteristics that set them apart within this larger category of public registries and make finding the appropriate balance between access and privacy especially difficult.

Chief Justice Beverley McLachlin in a speech last year to the Canadian Bar Association addressed in part the Supreme Court's role as a national leader in electronic court records and the ideal of having a single system that would apply across Canada's courts. The Chief Justice gave an update on the Supreme Court's own website and observed that, while the Supreme Court was trying to put as much information as possible on the site to allow the profession, media, courts and public to follow developments, they were deferring plans to add factums. She observed that the experience of some courts in the United States who "went 'e' very quickly" and had problems with "voyeuristic access" was an object lesson that the Supreme Court should go slowly to carefully consider privacy and access.[2]

---

1 B. Givens, "Public Records on the Internet: The Privacy Dilemma", online: http://www.cfp2002.org/proceedings/proceedings/givens.pdf at 1.

2 Remarks of the Right Honourable Beverley McLachlin, P.C. to the Canadian Bar Association, Saskatoon, Saskatchewan, August 12, 2001; J. Tibbetts, "Top court retreats from full Web access: Chief Justice has privacy concerns about posting court records" *National Post* (August 23, 2001) A3.

How can courts protect private information, preserve public access to the courts, and avoid being cast in either the role of "censors or editors"?[3]

I. CANADA'S COURTS TODAY

Currently, reasons for judgment for federal and provincial courts are available over the Internet, on the courts' own sites, through law societies, or through third-party providers who make the information accessible to the public free of charge. Typically, opinions on public access sites are available for court decisions from the 1990s to the present, although the Supreme Court's site offers reasons from the 1980s. Appellate reasons for judgment are widely available, and often trial judgments can be accessed as well. Proprietary databases with fee-based searching have been available before this by providers such as Quicklaw, whose databases offer more extensive coverage.

II. LEGAL FRAMEWORK

The *Privacy Act* governs the public sector's use and collection of personal information and the public's access rights to personal information held by the government. That Act's use and disclosure rules for the public sector do not apply to personal information that is "publicly available".[4] In provincial privacy legislation, courts are frequently explicitly exempted or not included in the list of public bodies covered by the statutes. Provincial legislation, like the federal counterpart, also includes exceptions for personal information that is a matter of public record.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies fair information principles to the private sector.[5] *PIPEDA* does not apply to the press in the ordinary course of making information available for journalistic purposes and does not apply to the public sector. Under *PIPEDA*, personal information can qualify for privacy protection even though it is "publicly available", but regulations can remove certain public information from this protection. A regulation has been adopted which names five public sources, including records of judicial or quasi-judicial bodies, to which the Act's privacy protection

---

3 *Shulman* v. *Group W. Prod. Inc.*, 955 P.2d 469 at 474 (Cal 1998).

4 R.S.C. 1985, c. P-21, as amended, s. 69(2).

5 S.C. 2000, c. 5.

does not apply.[6] However, this exemption applies only if the use of the personal information relates directly to the purpose for the information being in the public record.

The regulation has been criticized because it is very difficult to apply the "public purpose" idea to court records, given that court records historically have been a rich resource for a broad range of purposes. Presumably, mining court records for at least some commercial marketing would not be permissible, but the scope of the regulation is unclear until there is more discussion about the appropriate public purposes for court records and the personal information within them.

As I will describe, the combined effect of these statutes suggests how important it is to consider what information is "publicly available" in court records and the public purpose for court records. Different ways of defining "public" information have different impacts on judicial resources in terms of the costs of technology and personnel, and on the public with respect to access and privacy.

III. RECENT DEVELOPMENTS

Many examples in the press recently on Internet access to court records have been inspired by what one US case called "prurient interests without proper public purpose."[7] To illustrate with one recent case, the clerk of courts in Hamilton County, Ohio was profiled in May 2002 in the press because he added a "comprehensive name search" feature to the website, www.courtclerk.org, and traffic to the once sleepy website increased exponentially by voyeurs seeking titillating information on local celebrities.[8] In that newspaper profile, the clerk was reported as explaining that Ohio's public records law left him no choice but to make sensitive documents available since he must provide the information in any manner that the court maintains it. The site now includes a pop-up window supporting that position with links to the article, "Privacy and Court Records on the Internet: Mutually Exclusive Concepts" whose conclusions are self-explanatory from the title. He contends that the law requires an all

---

6 SOR/2001-7.

7 *In re Application of KSTP Television*, 504 F. Supp. 360, 362 (D. Minn 1982).

8 D. Monk, "How Public are your records: County clerk grapples with privacy issues" *Business Courier* (May 17, 2002), online: http://cincinnati.bizjournals.com/cincinnati/stories/2002/05/20/store1.html.

or nothing view: Information must either be available with unrestricted public access or fall within a specific exception to the open records law and filed under seal.

That example profitably emphasizes the hazy position that court staff occupy as they try to appease media and privacy advocates who argue, respectively, for unlimited or no access online for court records.

There are two strong but competing inclinations with respect to privacy and public access, and it is fair to surmise that most of us are of two minds on the issue. On the one hand, as *users* of public information, we are already accustomed to retrieving free information electronically and being able to do sophisticated searches to find precisely the information we want. In some cases, liability heightens that urge to retrieve information since more information and more access has been coupled with an increase in liability when people do *not* avail themselves of available resources. Those making decisions in the employment context, for example, routinely conduct background searches, and personal information in public records is a valuable resource for that purpose. On the other hand, as *subjects* of information, there is an increasing anxiety about privacy invasions from electronic information and the ease with which information can be retrieved about us. So we tend to appreciate public resources that reveal information about other people, but to criticize those resources when they reveal information about ourselves.

Given that court records have been open historically and computer access has been available at courthouses for some time, it may seem curious that the issue has drawn our attention now. Yet we are now setting the parameters for putting information online and we have a chance to review our policies with respect to public records and establish boundaries. While the idea of making court records available on the Internet is the reason that the question of how to balance privacy and public access is being asked now, it is a question that is overdue.

A story reported this fall in the press is a pointed reminder that, while technology may provide a new urgency to resolving the issue of access and privacy and a new context for the debate, the issue is neither novel nor unique. In Winnipeg, a publication ban covered the salacious details of a criminal case involving husband and wife owners of an escort service. But after the couple pled guilty, the Crown tendered two binders worth of paper documents as exhibits for sentencing, which became public records that the public was permitted to view. Sample documents included

customer credit card information, sexual preferences and hourly rates for individual customers, and résumés of escort applicants with nude photos, body measurements, and specialties. Public appointments to view the documents were fully booked after that. Although the publication ban still protects the information from wide dissemination in the press, the informal exchange of information may be just as stinging. It is a cold comfort to the individuals caught up in this case that their information is "only" available at the courthouse and "only" available in paper medium.[9]

IV. TERMINOLOGY

I should say a word about the terminology at the outset. Although I use the term "public" throughout, I reiterate a caution expressed before me that "public records" may be misleading as a descriptive term in the debate, since it implies a certain answer to the question.[10] Although "public" is still used in this paper, the word should be interpreted as referring only to the governmental organization that maintains the records and not as suggesting any particular resolution as to the extent of public access.

Also, so that the term "public records" does not cloud this point, I want to stress the premise. Some people question what all the fuss is about: If personal information is available in public records, how does privacy apply at all? But there is a growing consensus that privacy and personal information are interests that should be recognized, even where the source of the information is a "public" document or can be viewed in public, so that transparency and private life can be balanced.

There are several related issues that are outside the scope of this paper, including private information held in other kinds of public documents, such as property assessment records or public documents that in some jurisdictions are kept in courthouses, but which are not court records, such as marriage licenses. The topic is also related to but does not directly address other kinds of media access to court proceedings, as opposed to court records, such as the issue of cameras in the courtroom. It is also related to online government and initiatives such as the federal courts'

---

[9] R. MacGregor, "Escort agency's books rivet a curious public" *The Globe and Mail* (October 8, 2002).

[10] R. Gellman, "Public Records: Access, Privacy and Public Policy" *Center for Democracy and Technology* (May 16, 1995) 4.

e-filing project. Electronic filing would of course make electronic remote access to court records easier since documents would be filed in a format that could be readily available on the Internet with much less strain on court resources.

V. LEGAL THEORIES AND POLICES

There are strong policies supporting both public access and privacy, and the balance between them is a delicate one.

VI. PUBLIC ACCESS

Historically, there has been a presumption that the public had access to trials. Indeed, public trials were sometimes a spectacle more than a solemn affirmation of citizenry.

The public has a common law right of access to attend judicial *proceedings*, which is now recognized under section 2 of the *Canadian Charter of Rights and Freedoms*.[10a] The public needs to be informed about courts in order to monitor the judiciary process and have public confidence in court operations. Public access helps to ensure fair trials and the integrity of the deliberative process. It helps to guarantee that an accused is given a fair trial, that people are treated similarly, and that courts are not used for persecution (secrecy breeds abuse). The press of course plays an important role. The press does not have special rights to information above what the public holds, but acts as the people's eyes.

In addition to public access to attend trial proceedings, public access to court documents is integral to the common law system: People must know enough factual information about past cases in order to properly anticipate liability, order their business and personal affairs, and as litigants, to be able to prepare court cases and make persuasive submissions to the courts by using precedents to argue how legal principles should apply to new cases. The right to consult and copy court documents has been exercised long before twentieth century statutory freedom of information laws.

[10a] Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11.

The philosophy behind the right of public access was expressed centuries ago. James Madison, framer of the US Constitution, wrote:

> "A popular government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; and a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."[11]

The two access issues, access to public hearings and access to public documents, give the public a right to access information about the courts. This enables the public to monitor and assess government functions, and an informed electorate can criticize and contribute to the judicial system. Public access increases public trust in the fairness of the judicial system, increases public participation, protects constitutional rights such as freedom of the press, and fair trial rights, and ensures accountability.

Public access, however, is not absolute.

VII. PRIVACY

Privacy has famously been defined as the "right to be let alone" or, more specifically for information privacy, the right of individuals to control how information about themselves is communicated to others.[12] Privacy has been associated with dignity, autonomy, the ability to form and maintain personal relationships, and due process rights. The Supreme Court has incorporated both the "right to be let alone" and the "control" definitions of privacy in their jurisprudence.

While privacy has a constitutional dimension, there are also statutory provisions to protect information privacy. The most widely held legislative model are the fair information principles, which have been adopted in Canada in the *Personal Information Protection and Electronic Documents Act* and by the European Union in their data protection directive.[13] The

---

[11] Quoted in *EPA* v. *Mink*, 401 U.S. 73 at 110-11 (1973), in Letter from James Madison to W.T. Barry (August 1822) in 9 *The Writings of James Madison* 1034 (Gaillard Hunt ed. 1910).

[12] S. D. Warren and L. D. Brandeis, "The Right to Privacy" (1890) 4 Harv. L. Rev. 193; A. F. Westin. *Privacy and Freedom* (New York: Atheneum, 1970).

[13] *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data,* E.C. Doc. 3954L0046, Council Directive 95/46 of October 24, 1995, O.J.L. 281/31.

United States has incorporated fair information principles in sector-specific legislation. The fair information principles ensure that the collection, use, and disclosure of personal information are limited and that there is integrity of the personal information.

The specific principles, adopted by the Canadian Standards Association as the Model Code for the Protection of Personal Information and incorporated as Schedule 1 of *PIPEDA*, are: accountability, identifying the purposes for collecting personal information, requiring consent for the collection use or disclosure of personal information, limiting collection to only that information which is necessary for the organization's purposes, limiting the use, disclosure and retention of personal information to only those purposes which are necessary, unless there is consent, having accurate and up-to-date information, protecting information with security safeguards, providing openness to individuals of the organization's policies for personal information, giving individuals access to their personal information, and providing means for individuals to challenge organizations on compliance.

As with the right of public access, the right of privacy is not absolute. People and public institutions need other people's information in order to do ordinary daily activities, yet people also seek to protect their personal information. Personal information is critical to the fair and accurate resolution of court cases. But other people may not always require unlimited access to the personal information in court records in order that the "*public purposes*" that access serves can be met.[14]

Some personal information may be compelled by law to be disclosed but may not be adequately protected and what protection there is may be even less in the online environment.

The question of the appropriate access to and protection of personal information in court records must be addressed by balancing access and privacy as (at least) two interests that inform the debate.

---

[14] For discussions of the public benefits to a wide access and circulation of information, see D. L. Zimmerman, "Information as Speech, Information as Goods: Some Thoughts on Marketplaces and the Bill of Rights" (1992) Wm & Mary L. Rev. 665; E. Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking about You" (2000) 52 Stan L. Rev. 1049; R. Posner, "The Right of Privacy" (1978) 12 Ga. L. Rev. 393.

A serious concern is the possibility *of unintended consequences* as new technologies permit new forms of access to public records. Full access to court records could lead to less access to information and justice if there is too big a cost in lower public participation. The goals that access is supposed to serve could inadvertently be frustrated by unlimited access. Although access increases public confidence in the judicial process, it is also true that privacy increases public confidence in the judicial system, as people trust in the courts to keep personal sensitive information safe. Indeed, the US Supreme Court has indicated "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 […] [and] in some circumstances that duty has its roots in the Constitution."[15] Uncalibrated access to court records could lead to the unintended and undesirable consequences of *less* public trust in the judicial system and *less* participation.

To take an example from another kind of public record, when voter registration information becomes publicly available online in an effort to promote voting, which some jurisdictions in the United States have experimented with, there is anecdotal evidence suggesting that, in an ironic twist to digital democracy, people may forfeit their right to vote rather than having such information as party affiliation, birthdate, and residential address accessible.[16]

As a strong indicator of the complexity of the issue, it should be emphasized that "access" has more than one sense and, perhaps counter-intuitively, allowing full public access to court records may reduce access in other ways. Public "access", in its ordinary connotation, refers traditionally and positively to access through the media, including access rights to attend trial and access to information in the public court records. But "too much" access could lead to a chilling effect in which people are afraid to access courts because they fear exposure. The unintended result of unfettered access could be more limited discovery or less use of courts,

---

15 *Whalen* v. *Roe*, 429 US 589 at 605 (1977).

16 A. Harmon, "As Public Records go Online, Some Say They're Too Public" *New York Times* (August 24, 2001) A1. The site owners, e-the People, countered that they thought the potential for abuse was relatively low because the site uses the security method of requiring an individual's birthdate before voter registration information is released and it was a "reasonable assumption" that only the individual, family and closest friends would know that information.

and a decreased willingness by complainants and witnesses to come forward voluntarily.

People's confidence in how carefully personal information is treated within the judicial system relates to their willingness to use courts as a dispute resolution mechanism. Parties, witnesses, jurors, and law enforcement are all concerned about protecting personal information for the purposes of physical security (stalking), ongoing investigative efforts, economic security (identity theft), and security of self (against indignity).

Increasing access to court records could result in less access to *accurate* information. People might react by revealing less information during the discovery process or they might deliberately "spike" records with false information and provocative unproven allegations as a litigation tactic, knowing that information will have a wide dissemination.

Another unintended effect could be that some people in the court system might be able to safeguard their personal information more easily than others. Public figures or people that are forewarned that their cases might get media attention know to request to have court records sealed, but with Internet access, anyone's information could be easily "published". Where personal information is protected by special procedures such as requests to have records sealed, it takes legal resources to know about those procedures and to request them and it is a strain on judicial resources to deal with these requests. Procedures to redact information or not to include personal information in the public record should be accessible to the public.

Finally, efforts to rectify the privacy dangers could lead to the unintended effect of endangering the privacy of *users* of the information. Some American policy proposals have vetted the idea of compiling logs of users accessing public court records through remote electronic means. Such an "audit trail" conceivably could help track those who use public information for clearly improper purposes such as identity theft or stalking. However, an effective right to access public information should encompass a user's right to access public information *anonymously*. In this context, an *improperly conditioned* access right would lead to a chilling effect.

There may then be a duty both to further the public's right to access public documents *and* to protect the personal information in those public documents. In balancing these interests, the goal is to limit "unwarranted

disclosure and use" that is unrelated to the public functions that access is supposed to serve.

The two "purist" positions in the privacy and access debate are "total access" and "zero tolerance". First, the full access position, advocated by some researchers and journalists, argues that the full court records that are available now in a paper format at the courthouse should be available wherever they are accessed and in whatever format, including the Internet. The executive director of the Reporters Committee for Freedom of the Press, as an advocate of this position, characterizes plans to distinguish between paper and electronic records as "technology hysteria".[17] Access proponents emphasize freedom of information and the importance of an informed public debate and point to the fact that these are publicly funded databases.

By contrast, some privacy advocates suggest, although it is probably true that they are more often accused of suggesting, that there should be differential treatment between paper and electronic records. The argument here is essentially to continue to exploit the technological limitations of paper formats that produce a *de facto* "practical obscurity". Another version of this argument is to allow remote access and electronic formats but to add access and/or use restrictions. An additional factor is the cost of providing this resource.

VIII. DO ELECTRONIC FORMATS QUALITATIVELY CHANGE PUBLIC ACCESS?

Is new technology itself, then, a reason to change the open access policy? Under the traditional system of having documents available only at courts, there was a *de facto* "practical obscurity". The US Supreme Court has observed that there is a "vast difference" between public records found after a "diligent search" through different physical sites and "a computerized summary located in a single clearinghouse of information."[18] The time, expense, inconvenience, and distance of traveling to the courthouse, and once there, the limited indexing, and limited media formats all restricted the amount of personal information that could be discovered.

---

[17] J. Markon, "Sensitive court records go online, sparking debate over restrictions" *Wall Street Journal* (February 27, 200l) B1.

[18] *US DOJ* v. *Reporters Committee for Freedom of Press*, 489 US 749 at 764 (1989).

Computers and later the Internet, changed the nature of personal information. In particular, search capabilities are greatly enhanced and information can be easily cross-referenced.

The benefits to electronic records and access are several. There is more sophisticated search capability enabling researchers to know what information is retrievable, where and by whom. Researchers in history, education, and media, have much better access to information. That access is much more uniform and available at all hours. People can monitor government more efficiently, as barriers and transaction costs for the public to access court records come down. Finally, people do not have to depend solely on the media's choice of which court records to highlight, they can pull out the information that interests them.

In fact, some have argued that the switch from traditional media purveyors of court information to an electronic "self-serve" or one-stop shopping ultimately better protects privacy. In the traditional model where the public largely depends on the press to introduce them to trials of note and to inform them of new developments, there is a broad distribution of information on a narrow range of subjects; those individuals whose personal information was the subject of inquiry in turn had notice and opportunity and could seek to have private information sealed. Conversely, where information is available electronically and remotely, people pull information on a limited subject whom they have identified in advance, and they are exposed to less "gratuitous" personal information.

On the other hand, the privacy risks increase substantially with new technologies. These risks have been well rehearsed by now. One of the biggest problems is the creation of "digital biographies" or electronic dossiers.[19] With integrated databases, discrete personal information that was located in separate paper records can be combined. Better search capabilities and integrated databases results in a loss of practical obscurity. Integrated databases pose two problems: not only is precise personal information easily available, but so too is inaccurate information. In the electronic context, incorrect or out of date information is as hard to control and as easily spreads as accurate information, and both pose dangers to privacy. As Jeffrey Rosen observes, "[p]rivacy protects us from being

[19] Westin, *supra* note 12; A. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971); S. Garfinkel, *Database Nation: The Death of Privacy in America* (Sebastopol, Calif: O'Reilly and Associates, 2000); R. Whitaker, *The End of Privacy: how total surveillance is becoming a reality* (New York: New Press, 1999).

misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge."[20]

One danger to the loss of practical obscurity is the loss of "social forgiveness". Information that would be formally expunged or discarded under paper retention policies can remain available in electronic format after the paper copy is gone. The long memory of record retention prevents society from reaping the social rewards of rehabilitation; what incentive is there to reform if records ensure that transgressions are always fresh?

Other dangers are security risks. Criminal case complainants and witnesses and members of law enforcement are all vulnerable to physical security risks, such as stalking. In addition, there are economic security risks, such as identity theft.

Another prospect is that court records could be used to create profiles for commercial marketing: "You won custody? How about some diapers." "Web-Detective" for example, advertises that they make all available searches covering property, court records, social security, inmate, wanted lists, criminal, bankruptcy, marriage, divorce, death, birth, vital records in all states, prison records, most wanted databases, reverse lookups, unlisted phone numbers (cell phones or landline), owner's name and address of a cell phone number ("and much much more!") in order to find "all the information that is available on the Internet about you or anyone else in the world!" for a flat rate one time subscription fee.[21] Interestingly, the ad copy emphasizes the paradoxical nature of access and privacy, by urging that the company can "help you conduct thorough and complete personal investigations of *yourself*, or almost anyone else in the world, and find out exactly who has information about *you*, where it is located and what it says."[22]

Thus, technology does change the *de facto* balance between access and privacy that was tenuously preserved through paper documents at the courthouse. This is not to say, however, that the best solution is to set up differential access and use policies that favor on-site over remote access, or paper over electronic formats. With e-filing and electronic courts, most

---

[20] J. Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Random House, 2000) at 8.

[21] Online: http://www.web-detective.com.

[22] *Ibid.,* emphasis added.

or all documents predictably will be electronic in the near future and there will be no corresponding "paper" original archived at the physical site of the courthouse.[23] The very concept of an original in the electronic context is becoming obsolete or at least of diminishing importance, as courts scan past paper documents and new paper originals in "official filings" are less likely to be created. On-site access will likely be primarily through the court's facilities of electronic terminals at kiosks rather than paper copies requested through a face-to-face interaction with the court clerk. In the near future it is predictable that the courthouse will offer infrastructure to access documents but the actual source of documents will be exactly the same as it is for remote access; that is, even at the courthouse one will be accessing electronic documents at an Internet site. Furthermore, use and access policies that favour on-site access and paper formats disadvantage persons with disabilities who may require technology to have an effective access right to public documents. Adopting a formal policy that prohibits the publishing of court documents online is at best, then, a delaying tactic that allows courts and legislatures time to study privacy issues in more detail.

IX. POLICY *VERSUS* TECHNOLOGY

I suggest that the problem of privacy and access does not reside in the development of the new technology of electronic records, although new technology has precipitated the current debate. Instead, the real conceptual

---

[23] CNN.com recently reported one example of electronic courts in Yakima, Washington, where defendants in minor traffic offense cases who plead guilty and ask for a mitigation hearing can argue their cases through e-mail, over a secure server, rather than having to appear physically in court. The judge presides in the courtroom, reads the email and issues a verdict. J. Legon, "Lady Justice Goes Digital: Yakima traffic offenders get their day in court via the Web" (October 2, 2002), online: http://www.cnn.com/2002/TECH/internet/10/02/email.court/index.html. In Brooklyn, all case proceedings for a multi-jurisdictional community court handling criminal, civil, and family court matters are placed online. The objective is to provide the single judge with access to information from multiple sources and includes new information such as extensive survey questions on the defendant's background. Many argue that the increase in efficiency is not worth the sacrifice in privacy and civil liberties. C. Barliant, "E-Court Grows in Brooklyn", *New York Law Journal* (October 10, 2000), online: http://www.nylj.com/tech/101000t1.html. The US Supreme Court also took the highly unusual step of accepting electronic filings when the 2001 anthrax scare in the United States disrupted mail delivery in the Washington, D.C. area and electronic filings curiously became lower security risks than paper ones; the change in rules expired at the year end 2001. "Anthrax Scare Prompts Supreme Court E-Filing discussions" (December 17, 2001), online: http://www.newsbytes.com.

problem is first an ill-defined concept of what constitutes a "public" court record, and second, of not having linked the idea of a "public record" to the functions that such public access is intended to achieve (monitoring the courts, transparency, fairness). In short, the balance of access and privacy is a policy issue and not a technology issue.

Posing the question as whether the courts should make information available in an electronic format and whether that information should be accessible remotely addresses the issues only obliquely. The practical obscurity of past technology limits does not give us a basis for continuing to distinguish between paper and Internet media. The issue is not "paper versus electronic media" or "on-site versus remote access". Instead, the issue is what personal information should be collected by the courts at all, and of that information which is justifiably collected, what information in court records should be "public" because it serves public functions. This approach borrows from the fair information principles the idea that access and purpose are linked. The fair information principles incorporate the theory that defining the purposes for the use and collection of information will in turn work to limit the collection and use of information.

Applied here, the government should adopt explicit criteria for what is a "public record", and those policies should be developed from the proper "public purposes" for court records. The definition of a "court record" should be related to the functions of transparency and judicial monitoring. If certain information is not required to achieve the spectrum of objectives that public access is intended to achieve, then such private information or private document should be presumed not to constitute public information. We need public debate to define the policy objectives with some precision and the correlative information that is related to meeting those objectives.

For each kind of information that is collected, we should consider whether the information itself is legitimately needed for the adjudicative process; and second, whether access to required personal information serves the purposes of public monitoring and transparency. Trial participants' privacy concerns should be balanced with the public access right to the information in court records that enables the public to judge the court system.

We already make these distinctions between court records that have a public purpose and those that do not. Some documents generated within the courts for the process of adjudicating and preparing reasons for judgment are not released to the public, such as drafts of reasons, clerk

memoranda, or memoranda by legal staff. And examples can be multiplied from other kinds of public records. For example, many jurisdictions are switching to a system in which real estate and tax information on real property is searchable only by address and not by the property owner's name.[24] The logic, which I believe is instructive, reasons that the proper use of such public information is to ensure that similar properties are taxed at similar rates. Finding out the residential addresses of the famous people in one's town is not a function that is integral to public monitoring of government. However, the extent to which there is consensus for this approach should not be overestimated. The committees deciding these issues are frequently deeply divided. Some public officials worry that restricting search capabilities is tantamount to censorship and may contravene the public mandate to make such documents available to the public. Given that the paper indexes at the courthouse include name searches, some argue that the Internet capability must be at least as open.

The access and privacy advocates both claim support in history. What was the original vision for access, and if we can identify it, what role should tradition and history play in the debate? The key is to look past specific technologies and toward the purpose of the record.

Under the traditional "practical obscurity" model, the scope of public information was broadly defined in theory but the actual access and disclosure was low in practice.

What then can we infer was the intended ideal? In other words, were the limitations of contemporary technology *facilitating* or *hampering* the intended goals? Was the vision one of full access that was *frustrated* by the physical constraints of paper-based records systems, or conversely was the ideal one of limited access coupled with privacy protections where the inherent technology limitations actually *ensured* that the ideal was met? As a 1995 report prepared for the Center for Democracy and Technology on the issue of public records observed, "[o]ne may argue fairly that the intent of the open records law was to permit all such uses without distinction. One may just as easily argue that the expanded use of records resulting from computers and industry practices was not foreseen or intended."[25]

---

[24] See, for example, S. Williams, "County may limit online property record information" (October 9, 2002), online: http://www.jsonline.com/news/wauk/oct02/86348.asp.

[25] Gellman, *supra* note 10 at 27.

In retrospect, practical obscurity may have been a principled policy and not just a logistical fact. The physical limitations that were intrinsic to the traditional model, including time, energy, cost, and geography, were not just inconvenient obstacles toward full unfettered access. Instead they were integral privacy safeguards that helped the system function as it was intended. As new technologies remove those safeguards, other new technologies that protect privacy should be instilled in their stead in order to maintain the balance of disclosure and privacy. That conclusion, however, does not mean we have to continue to distinguish court records based on paper from electronic sources or remote from onsite access.

If this policy of something less than full access to public court records—a public access that incorporates privacy protection—were to be designed today with our awareness of new technologies, how might it be implemented and what factors should we consider? Critical questions to address include: Who should set the policy: courts or legislature? Should standards be statutory, regulatory, or discretionary? Should the policy be applied on a case-by-case basis or through presumptions? What access or use restrictions might be used? Should policies be developed to control access based on the category of user or the kind or amount of information that is requested?

While one effect of the privacy and access debate may be that less information is collected initially, it will certainly continue to be the case that particular highly personal information will be required to be collected in order for judges to make their decisions. But that same scope of information may not be required for the public to fulfill the functions of public monitoring of the courts. These differences between collected and accessible information potentially impose a large cost on staff resources if the court must distinguish which documents in a file can be released, and which information within a document is public or protected.

Various suggestions for protecting personal information while preserving public access have been proffered that seek to add predictability and uniformity to the process. Proponents argue this would decrease costs to the judicial system by enabling court personnel and participants in the trial process to be able to identify in advance what personal information, although required to be disclosed to the courts, would still be protected from public access. Policy advocates frequently suggest a compromise approach that would add restrictions to access, collection, dissemination, and/or derivative uses. Such restrictions could be imposed in several ways, such as by type of case, type of information,

category of user, type of use, type of media format, or source of access. Each of these alternatives in turn raises further questions.

Access restrictions could be implemented by having separate public and private files. Private files would either be full files available only to counsel, parties, and the court or the information could be available in a separate sealed document. Another suggestion has been to have an electronic "holding pen" in which information would be submitted according to the courts' regular rules, but Internet accessibility would be delayed, to allow for requests to seal the information or for the case to be completed. Separate court files and "public records" add complicated resource and liability issues. For example, with respect to procedure, if full information is provided to the court but certain information is redacted for the "public record", who would redact or identify the information? Who would pay the cost for identifying and redacting personal information? Who would be liable if personal protected information was inadvertently released? If the parties are responsible, who would guard the interests of witnesses and jurors and other participants in the trial process (or individuals who are named in court records) who also have privacy interests in personal information? Perhaps the thorniest question in terms of resources is what to do with older records and documents that have been filed before the introduction of the policy. If the documents are scanned for web access, should they also be checked to redact personal information that would raise a privacy interest? This would of course add enormous costs to the project of expanding Internet public access for court records.

With respect to categorizing use restrictions, distinctions could also be based on the purpose of the use (commercial, news, private curiosity, legal). Individual requests might be allowed while bulk copying of databases or batch requests, or transfers of the information would be prohibited. The users themselves could also be regulated through logins and passwords or through subscription services. That approach sacrifices users' anonymity and raises digital division issues if fees are charged for searches.

Instead of user-based categories, restrictions could be based on the information. Restrictions according to the cause of action would be predictable, but over-inclusive in terms of protection. Some suggest that family (custody, domestic and child abuse, property division, adoption, divorce and separation, third-parties in divorce), bankruptcy, employment or disability, and criminal cases should all be subject to tighter restrictions.

The US Federal Courts adopted, only briefly, a policy that gave less public access to information in criminal cases. Another option is to restrict certain categories of information regardless of the cause of action; such information could include party names, financial information (account information might be identified instead by the last five digits) or autopsy photos. Alternatively, certain documents, such as discovery information, could be restricted from public access. Finally, returning to the ideas that have typically defined the debate, the restrictions could be based on media format (electronic versus paper) or by the location where information is accessed (onsite access at the courthouse versus remote).

X. OTHER JURISDICTIONS AND THE BALANCE OF PRIVACY AND ACCESS

New Zealand is distinguished for having a well-developed regulatory framework that is designed specifically for public registries, rather than merely applying general fair information principles to public registries. New Zealand supplements the general data protection rules with four separate privacy principles that apply to public registers. First, search references must be consistent with how the register is indexed. Second, personal information cannot be re-sorted or combined with personal information from another public register in order to sell that information commercially in a new form. Third, public register information must not be made available by electronic transmission except to members of the New Zealand public who want to search the register. Fourth, personal information must be made available free or at a nominal fee. However, court records are not included on the schedule of public registries.[26]

In the European Union, the 1995 data protection directive regulates automatic processing and transfer of personal information. An opinion from the working group on data protection issued in 1999 clarified that personal information must be protected even after it is made publicly available, while still keeping access rights.[27] Some member states have considered or adopted additional protections for court records, such as prohibiting party name searching in court decisions databases (Belgium) or opt-outs.

---

[26] *Privacy Act*, 1993, s. 59.

[27] Opinion No. 3/99 on Public sector information and the protection of personal data, adopted May 3, 1999.

The United States has recently adopted two sets of guidelines covering federal and state court records. The federal policy, adopted a year ago, recommends that files in civil cases, including bankruptcy cases, which are open to the public at the courthouse, should be available through electronic access, except that litigants should remove Social Security numbers, birth dates, financial numbers and names of minor children. Access should be through a uniform system that allows users to be traced if required. For criminal cases, the original recommendation was not to allow electronic access, but within a year of release, that policy is being reviewed and a pilot project allows some courts to have remote public access for criminal cases.[28]

The state courts meanwhile have independently developed their own set of guidelines governing access to state court records.[29] The state court guidelines are more detailed. They rely on a general access rule permitting electronic access. However, individual courts can then specify that certain information, for good cause, can be restricted to a court facility. That policy could change if technology allows information to be redacted from electronic versions. Further, certain information will not be available to the public at all as part of the public court file, such as cases on sterilization, termination of parental rights and adoption, or particular information such as DNA analysis, psychological evaluations, witness or juror contact details, or judicial work product including bench memos and drafts of reasons. Restricted information could be made available to researchers with suitable undertakings to protect it and not resell it.

XI. RECOMMENDATIONS FOR CANADA'S COURTS

Legislatures and courts should consider and answer the following: 1) what information should be collected *because* that information is necessary for a judicial purpose; 2) what information is part of the public court record; 3) what procedures will be implemented to notify people that records contain personal information; 4) what procedures will be available

---

[28] Online: http://www.privacy.uscourts.gov/Policy.htm.

[29] Online: http://www.courtaccess.org/modelpolicy.The Joint Court Management Committee of the Conference of Chief Justices and the Conference of State Court Administrators submitted, "Public Access to Court Records: Guidelines for Policy Development By State Courts" in July 2002 for consideration by the Conference of Chief Justices and the Conference of State Court Administrators at their annual conference.

for people to request that personal information be removed from the public record, including older records; 5) what liability and penalties will be imposed for including gratuitous or false personal information in court records; 6) what liability and penalty will be imposed for inadvertently releasing personal information; 7) how long the retention schedules for court records will be and what the policies will be for purging certain kinds of records; and 8) whether older case files will be converted into electronic formats and made available remotely and with what protection? I offer the following specific recommendations.

First, the same access policy should apply to electronic and paper media, and to remote and on-site sources. Except for parts of the court file that physically cannot be transferred to electronic formats without a significant loss of information, such as real evidence or archival documents where seals, or stains, or handwriting contains critical information, the best option would be to have *only* electronic information available at the courthouse for general public access. This would ensure uniformity and control information flow.

Second, sensitive personal information subject to mandatory disclosure and discovery information should be evaluated as to whether the courts require the information to be collected at all.

Third, the definition of "public" court record and "public purposes" should be carefully articulated. Once information and records are defined as public, access should not be restricted by type of recipient or use. The regulations to the *Personal Information Protection and Electronic Documents Act* supplement this last provision. That Act requires that private third parties get consent from the individual before personal information from public court records are used for non-artistic or non-journalistic commercial purposes that are inconsistent with the *judicial* reason that such information was originally collected.

Fourth, on access, some information should presumptively be public and, in fact, to go further, some information must be public in order that the public purposes of monitoring the courts and ensuring transparency can be met. Basic court calendar and docket information should ordinarily be available, including attorneys of record, awards, costs, and issues. The fact that the court file or document exists should generally be available to the public. The reasons for judgment, perhaps most essentially for the common law system, should be freely available to the public and through

the technology that best facilitates this access. However, personal identifying characteristics can be removed in special circumstances.

Fifth, typically, the designation of presumptively personal information should be applied at the level of specific kinds of information, not types of documents or types of cases, which will tend to be too restrictive of public access. Personal information that does not fit within a presumptive protected category could be protected by sealing or confidentiality orders.

Sixth, information that is presumptively private should be protected regardless of the resources of the requesting party. There should be a procedure to notify parties of the kinds of personal information that does not need to be disclosed in court records and that other personal information which is required to be disclosed is protected, and to notify interested persons when their personal information has been disclosed in documents filed by other persons. There should be simplified procedures, suitable for unrepresented persons, to request that personal information be protected.

Seventh, privacy-enhancing technologies should be incorporated where appropriate. Strategies might be used such as limiting public search inquiries to certain search fields within the database (one could even consider not having party names as a search field). More sophisticated technology such as XTML could be used to help achieve the maximum public access with the protection of personal information by precisely defining fields. This could give flexible privacy options with the least over- or under-inclusiveness, rather than relying on a crude binary model which classifies individual files, or documents, as entirely private or public.

Eighth, the fair information principles are a useful model but cannot be applied too literally to court records, which are different from other public records. Especially given the uncertainty about what a proper "public purpose" is for using court records, it would be problematic to apply those principles without refining them. For example, the fair information principle of specifying "uses" for the information collection should not be applied too narrowly since court records have historically been open and used traditionally for a broad range of purposes. Fair information principles, to take another example, often use an opt-in or opt-out procedure for consent for personal information, but this would not be feasible for court records, such as reasons.

Ninth, the privacy of users of public records should be respected. In an effort to protect personal information, other people's anonymity should not be sacrificed. The approach under fair information principles of implementing audit trails to enforce permissible uses would violate users' privacy and anonymity. This is also a concern for security protocols that create user logs. In addition to privacy-enhancing technologies, additional protective measures could be implemented in emergency situations. For example, suppression devices could block personal information, such as the address of a self-represented complainant, where such protection is urgent to protect physical security.

Tenth, although generally use restrictions are not a good idea, one exception is bulk copying and combining of public records for commercial purposes or reselling. This practice most likely contravenes the regulation under *PIPEDA* and the prohibition could practically be enforced.

CONCLUSION

There is a fragile balance between the public interest in public access and the equally *public* interest in privacy. Privacy is not simply a personal interest limited to the individual subjects whose information is vulnerable to exposure more widely and more easily than was contemplated before the introduction of the Internet. If public access, use and dissemination of court records does not consider both *privacy* and access, the effect may be to lessen access to justice overall. We should forth-rightly acknowledge that it is not paradoxical that public records can contain private information and that full access to justice is attained *not* by full access to information but by a balanced treatment which links access to proper public functions; moreover, we should recognize a concomitant duty in public institutions that collect personal information to safeguard the privacy of individuals to the extent that is consistent with the goals of transparency and monitoring. Privacy and public access to court records are not mutually exclusive objectives. Rather, there should be access with respect for personal information.

More sophisticated technology will facilitate this balance, allowing parties and courts to mark protected information as fields that will not be exposed in the public record.

Redefining what is "public information" would also reduce incentives to discover such information. Logically, the intensity with which public record resources are mined for personal information would be reduced if the burden for knowing such information were removed. Employer liability in hiring decisions would be proportional to the amount of *public* information that is available about individuals.

Because the legislative framework relies on "public purposes" and "publicly available" to define protections for personal information in public records, this paper argues that the conundrum of how to balance privacy and access is best approached by first linking "public records" and the information within those records to the public purposes for the records. By so doing, the analysis focuses on the underlying policy objectives instead of the questions of "paper versus electronic" sources or "on-site versus remote" access.

Of course the tension between access and privacy interests cannot be resolved by simply redefining all court records as private records. The procedure that I have outlined may not in the end result in the scope of the category of "public court records" being significantly narrowed. But it can limit the amount of personal information that is included in court records while allowing public access to personal information that is required for the public purpose of monitoring the courts.