CHAPTER IV

Privacy v. Transparency: How Remote Access to Court Records Forces Us to Re-examine Our Fundamental Values[1]

Nicolas Vermeys

Introduction

In February of 2010, the Victoria *Times Columnist* published a special report on the lack of uniformity regarding public access to court documents in British Columbia.[2] According to the report, British Columbia's courts would, at that time, "routinely and wrongly deny access to information that should be available to the public." In order to resolve this and other issues,[3] British Columbia has since moved toward eAccess to court records with the launch of B.C. Court Services Online, a service that "provides electronic searches of court files, online access to daily court lists and e-filing capacity."[4] Generally speaking, remote access or "eAccess" to court records implies that those interested in studying the contents of a court file, primarily the judge and litigators, no longer need to travel to the courthouse to do so, nor do they need to make multiple photocopies of the relevant documents to serve a copy to the court and/or opposing council. In fact, in British Columbia, as in other jurisdictions,[5] eAccess to court records is seen as an efficient way to guarantee that the procedures put into place are the same no matter who is behind the computer monitor. Such a practice also limits arbitrary access to procedures due to the clerk's personal understanding of policies or lack of experience. Thus, eAccess is seen both as a way to democratize access to court records, and to facilitate it—both strong arguments in favour of implementing such a solution.[6]

Furthermore, and notwithstanding these obvious efficiency arguments, eAccess to court records is also seen as a way to increase access to justice in a broader sense. In fact, as explained in a 2013 report prepared by the Action Committee on Access to Justice in Civil and Family Matters:

> The technology in all courts and tribunals must be modernized to a level that reflects the electronic needs, abilities and expectations of a modern society. Interactive court forms should be widely accessible. Scheduling, e-filing and docket management should all be simplified and made easily accessible and all court and tribunal documents must be accessible electronically (both on site and remotely).[7]

Although few would argue against better access to justice, eAccess to court records also raises the question of how much access is too much. Of course, the answer to that question really depends on what court records actually include. If the information contained therein is, as both federal[8] and provincial[9] legislators seem to suggest, purely public data, one could argue that there is no such thing as "too much access."[10] However, if court records are repositories of confidential information,[11] it could be argued that even limited access is unwarranted. Therefore, before going any further, one must define what the expression "court records" actually encompasses.

As defined by the Canadian Judicial Council's Judges Technology Advisory Committee in its 2005 *Model Policy for Access to Court Records in Canada*, court records can be defined as files that "include any information or document that is collected, received, stored, maintained or archived by a court in connection with its judicial proceedings." [12] Said court records can therefore include the following elements, among others:

- Case files;
- Dockets;
- Minute books;
- Calendars of hearings;
- Case indexes;
- Registers of actions; and
- Records of the proceedings in any form.[13]

As can be gleaned from this enumeration, court records will therefore often contain private, sometimes very sensitive data. Although this is particularly true of trial courts where records will often contain evidence, the same could be said regarding factums or other legal briefs submitted to appellate courts, although the risks are usually less important for higher courts since the documents they receive mainly address points of law and can therefore be edited to limit the use of sensitive private data and other personal information.[14] Notwithstanding this possibility, the fact remains that enhancing access to court records—primarily at a trial-court level—also means further eroding the privacy rights of parties, witnesses, and other stakeholders in the legal process, which could also have a direct impact on these individuals' willingness to take part in said process.

Of course, the competing values that are privacy and the transparency of court proceedings (which requires better access to court records) have always been at odds. Therefore, by increasing access to court proceedings, eAccess is seen by some as a threat to the somewhat fragile equilibrium that has existed between privacy and transparency by favouring the latter at the expense of the former.[15] This paper aims to examine this issue by (i) studying how eAccess can destabilise this careful equilibrium and, more importantly, (ii) what can be done to re-establish a balance while still taking advantage of this technological solution.

Privacy and Transparency of Court Proceedings: When Technology Destabilizes a Historically Complex but Feasible Equilibrium

As explained by the Supreme Court in *Lac d'Amiante du Québec Ltée v 2858-0702 Québec Inc*,[16] the perpetual tug-of-war between one's right to privacy under the *Privacy Act*[17] or other similar pieces of legislation[18] and the constitutional principle of transparency of court proceedings will usually end with transparency winning out.[19] As the court explains:

> Of course, the right to confidentiality will end if the adverse party decides to actually use the evidence or information obtained on discovery, when that party chooses to use all or part of it in his or her own case. The legislative intent that information

> be communicated in a civil trial will then prevail, to ensure that the system is transparent. On the other hand, at the examination on discovery stage, concern for transparency is not an issue because the examination is not a sitting of the courts. It is therefore legitimate in that case to give greater weight to the privacy interest, by imposing the obligation of confidentiality on information that is disclosed.[20]

That being said, and as demonstrated in the previous quote, the fact that transparency will usually take precedence is not an immutable concept, as there are instances where privacy will win out over transparency.[21] Therefore, eAccess to court records cannot simply be adopted because transparency usually prevails if it does not allow for those cases where privacy is seen as the superseding value:

> The justice system has the dual responsibility of being open to the public and protecting personal privacy. Its technology should be designed and used to meet both responsibilities.
>
> Technology use may create or magnify conflict between values of openness and personal privacy. In such circumstances, decision makers must engage in a careful balancing process, considering both values and their underlying purposes, and should maximize beneficial effects while minimizing detrimental effects.[22]

How should decision makers undertake this balancing process? By trying to identify the underlying principles that command the accessibility of court records. Transparency, in itself, has no value. It is merely a means to an end: that courts be open. Furthermore, actual transparency has never truly existed in our system since access to court records requires knowledge of their contents and the time and energy to actually consult a given file. These hurdles often create a practical obscurity that ensures the relative confidentiality of private data. Therefore, with eAccess accentuating transparency while eliminating practical obscurity, technology is not simply allowing for more transparency; it is redefining how transparency is to be understood.

The Open Court Principle as an Argument for eAccess to Court Records

As stated above, the transparency of court proceedings is simply a means to an end. That end, as explained by the Supreme Court in

Edmonton Journal v Alberta (Attorney General),[23] is to allow "public scrutiny of the courts."[24] This, in turn, cannot be done unless court proceedings and, consequently, court records[25] are "open and accessible to the public and to the media."[26]

This notion of free access, commonly referred to as the "open court principle,"[27] is, as the Supreme Court puts it, intrinsically linked to our fundamental "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication," as guaranteed by section 2(b) of the *Canadian Charter of Rights and Freedoms*:[28]

> The principle of open courts is inextricably tied to the rights guaranteed by s. 2(b). Openness permits public access to information about the courts, which in turn permits the public to discuss and put forward opinions and criticisms of court practices and proceedings. While the freedom to express ideas and opinions about the operation of the courts is clearly within the ambit of the freedom guaranteed by s. 2(b), so too is the right of members of the public to obtain information about the courts in the first place.[29]

As explained by Dickson J in *Attorney General of Nova Scotia v MacIntyre*,[30] this very important notion is the underlying reason why transparency supersedes privacy when dealing with court proceedings:

> Many times it has been urged that the 'privacy' of litigants requires that the public be excluded from court proceedings. It is now well established, however, that covertness is the exception and openness the rule. Public confidence in the integrity of the court system and understanding of the administration of justice are thereby fostered. As a general rule the sensibilities of the individuals involved are no basis for exclusion of the public from judicial proceedings. The following comments of Laurence J. in *R. v. Wright*, 8 T.R. 293, are apposite and were cited with approval by Duff J. in *Gazette Printing Co. v. Shallow* (1909), 41 S.C.R. 339 at p. 359:
>
> Though the publication of such proceedings may be to the disadvantage of the particular individual concerned, yet it is of vast importance to the public that the proceedings of courts

> of justice should be universally known. The general advantage to the country in having these proceedings made public more than counterbalances the inconveniences to the private persons whose conduct may be the subject of such proceedings.[31]

As to how this same principle is to be applied to court records, Dickson J adds:

> Undoubtedly every court has a supervisory and protecting power over its own records. Access can be denied when the ends of justice would be subverted by disclosure or the judicial documents might be used for an improper purpose. The presumption, however, is in favour of public access and the burden of contrary proof lies upon the person who would deny the exercise of the right.[32]

As it relates to eAccess to court records, the most important part of the previous statement is that "the ends of justice would be subverted by disclosure or the judicial documents might be used for an improper purpose." As we will now see, the fact that court documents might be used for an improper purpose is the true fear of those who oppose eAccess[33] since it goes far beyond the open court principle to facilitate access for "bail bondsmen, bank employees, title search companies, the real estate community, journalists and apartment managers to work more efficiently and dodge a trip to the courthouse,"[34] therefore basically ignoring the fact that "[w]hen litigants participate in the justice system, they do not waive their right to privacy."[35]

The Rise and Fall of Practical Obscurity as a Means to Ensure Privacy in a Public System

As stated above, there can be no doubt that eAccess is an effective tool in addressing access to justice issues by providing efficient and timely access for judges, parties, and litigators to court records. At the same time, however, eAccess offers these same advantages to others, including members of the general public and even commercial entities that might have a financial interest in the information contained in court files. This raises the question of *who* the open court principle is actually benefitting, since it improves access not only for those involved in a case, as well as members of the public and the press who wish to "comment on the courts as an essential aspect of

our democratic society,"[36] but also for any curious third party who wishes to view the information for reasons unrelated to "public scrutiny of the courts."[37] From a privacy standpoint, this is the aspect of eAccess that is somewhat worrisome. After all, if anyone can view the content of a court record or file, they could mine the personal data found therein and use it in a manner that is contrary to a party's privacy expectations, which, although circumscribed, remain valid.[38]

That being said, eAccess is, in some ways, simply the continuation of prior practice. It has long been agreed, as we have previously demonstrated, that "[t]here is a strong presumption in favour of public access to court records,"[39] and that said presumption "should be displaced only with the greatest reluctance and only because of considerations of very significant importance such as the protection of the innocent."[40]

However, because of practical obscurity (the idea that, although public, data remains difficult to access),[41] the public aspect of court documents and, most importantly, the private information they contain, has remained more theoretical than factual.[42] Access is limited because, with paper records, "[p]eople would have to drive to a courthouse to see them."[43] Therefore, although in theory anyone *could* go to the courthouse to look through boxes of evidence to access this information, in practice, few make the effort.[44] In other words, although court records are public, and therefore courts do not typically need to protect the personal data they contain under privacy legislation such as the *Personal Information Protection and Electronic Documents Act*[45] (PIPEDA) or the *Privacy Act*,[46] the practical challenges associated with accessing these records have, in effect, helped to ensure the confidentiality of the private data provided by litigants.[47] However, as explained by Tom Wright, the former Information and Privacy Commissioner of Ontario, back in 1996,

> [i]n a world of electronic information, "practical obscurity" is no longer sufficient protection for publicly available personal information since in reality, it no longer exists. Indeed, the availability of information electronically creates an urgent need to address the overriding question – just how much is someone else entitled to know about you?[48]

Although this quote might seem outdated, its teachings remain relevant since little has been done to truly address this issue in the

past two decades. In fact, some provinces, such as Quebec, have yet to adopt a policy regarding access to court records[49] even though, as mentioned earlier, the Canadian Judicial Council proposed a model policy back in 2005.[50] In other words, it remains as true today as it was in 1996 that, when court records constitute electronic documents,[51] the barriers to access are rendered almost inconsequential.[52] As a result, "nosy neighbours," "possible predators," and the like[53] can quickly and easily access the personal data contained in court documents, often from the comfort of their own homes. But intrusive individuals, although a cause for concern in some cases, do not necessarily represent as important a risk as one might think.[54] A more valid source of worry, however, is that private organizations such as data brokers, insurance companies, and banks could mine court records[55] as they do websites that publish legal decisions[56] for private data they could not otherwise obtain legally under PIPEDA or provincial privacy legislation. In other words, since eAccess makes court records "publicly available" in a way that was previously unimaginable, and since section 7 of PIPEDA allows for "an organization [to] collect personal information without the knowledge or consent of the individual" when the said information is "publicly available" and specified by the regulations,[57] unrestricted eAccess can become a legal loophole enabling the gathering of private data from a second-hand source without an individual's consent, something that is technically forbidden by clause 4.3 of Schedule 1 of PIPEDA.[58] Obviously, in many cases, it will be difficult for these organizations to establish that the personal data they collected "relate[s] directly to the purpose for which the information appears in the record or document,"[59] which is necessary in order to use, access, or share this data according to PIPEDA and its regulations,[60] as was pointed out by the Privacy Commissioner of Canada in a 2012 finding.[61]

However, it could be argued that such a finding is not sufficient to limit abuse since data mining is difficult to monitor and current punitive measures are considered by many to be ineffective.[62] Once again, this problem already exists in a paper-based court records system, but practical obscurity makes it less intrusive since these organizations do not have the resources to comb through boxes of court records for every individual encounter. They do, however, have the resources to click "find" in a search engine and wait a few nanoseconds to get the data they would otherwise do without.[63]

The risks associated with these practices that, in many ways, stem from the erosion of practical obscurity, have already arisen and been well documented in other areas such as intellectual-property registries,[64] assessment rolls,[65] and case-law database websites.[66] For example, regarding the latter, where court decisions were once published in books that were only available in law libraries and law firms, websites such as CanLII[67] now publish these same decisions online. These freely accessible sites therefore provide the aforementioned organizations with access to information that would otherwise be considered private, sometimes with disastrous results for individuals' privacy rights.

For example, in its *PIPEDA Report of Findings #2015-002*,[68] the Privacy Commissioner of Canada drew attention to the dealings of Globe24h, a Romanian company that mines case-law websites and republishes the decisions they contain under the guise of making "law accessible for free on the internet."[69] However, where CanLII "prohibits external search engines from indexing the text and case name of decisions published on its website"[70] to protect the privacy rights of parties, Globe24h.com is fully referenced in no less than twenty search engines, including Google.[71] Globe24h's business practices have led to at least one claim of violation of privacy against the Canadian court system and its agents, more specifically, against Quebec's *Société québécoise d'information juridique* (SOQUIJ).[72]

As per the *Act Respecting the Société québécoise d'information juridique*,[73] SOQUIJ is a self-funded government agency tasked with "the processing of legal data, in order to improve the quality of such information and to make it more accessible to the general public."[74] As a part of this mission, SOQUIJ makes court decisions available on its website,[75] as well as to third-party legal-research sites such as CanLII, QuickLaw, and Westlaw.[76] In the aforementioned case, a prior decision involving the plaintiff and containing some of his private information[77] was copied off one of these sites and republished on Globe24h.com, making it available through Google. Although SOQUIJ only did what both its constituting act and the Quebec Court of Appeals require it to do (i.e., grant access to the decision) as the official processor of legal data in Quebec, it was sued for not redacting the plaintiff's personal data (something it started doing five years after the fact),[78] therefore making it possible for Globe24h to publish said data online. Although the case was ultimately thrown out for failure to appear, it does emphasize the problems associated with online access to court documents.

To limit the damages linked to this newfound access, judges have changed the way they write their decisions so as to leave out any unnecessary information that could impact a litigant's (or third party's) privacy rights, and some editors such as SOQUIJ have chosen to redact sensitive data that do not affect the reader's understanding of a given decision.[79] Certain jurisdictions have gone even further and chosen to anonymize decisions to protect these rights.[80] Regrettably, there does not seem to be an equally satisfactory solution to protect privacy with regard to eAccess to motions, evidence, and other documents that have been filed with the court since editing or redacting these documents would affect their integrity, thereby rendering them unusable (for motions or other pleadings) or inadmissible (for evidence).[81] Furthermore, as previously stated, PIPEDA—as it is currently drafted—seems ill equipped to seriously curb commercial data mining of electronic court documents.

Does this mean that eAccess should not be allowed since it facilitates the improper use of court documents, therefore destabilizing the careful equilibrium between privacy and transparency? This would, in our view, equate with throwing out the proverbial baby with the bath water. If the fear is use of court documents for improper purposes, the answer is not to abandon eAccess but, rather, to limit its use.

eAccess to Court Records: Re-establishing a Proper Balance between Privacy and the Open Court Principle

In the first part of this paper, we established that the courts have stated on numerous occasions that public access to court records takes precedence over a litigant's right to privacy, therefore somewhat legitimizing the increased access afforded by eAccess. However, we also underlined the fact that eAccess not only ensures that the open court principle is respected; it also allows for third parties to exploit judicial data in ways that go far beyond what said principle aimed at allowing, therefore making all forms of private data contained in court records available for corporate means or unscrupulous spying.[82]

So how can the judiciary and/or a given department of justice allow for the legitimate use of eAccess, therefore reinforcing the open court principle, while curtailing abusive behaviour that leads to the use of court documents for improper purposes? We believe the answer lies in re-evaluating how we perceive privacy within a digital environment in order to qualify it as a "social value of superordinate

importance," while finding new ways to deter illegitimate uses of court data through technological means that could have similar effects to those of practical obscurity.

Re-evaluating "Social Value of Superordinate Importance"

In order to discriminate as to which types of individuals can have access to court records, the first question is to establish whether such discrimination is even possible. As we stated earlier, the Supreme Court seems to be unequivocal in its belief that privacy rights should not impede access to court records:

> While the social interest in protecting privacy is long standing, its importance has only recently been recognized by Canadian courts. *Privacy does not appear to have been a significant factor in the earlier cases* which established the strong presumption in favour of open courts. *That approach has generally continued to this day* […][83] (Emphasis added)

The day in question was March 29, 1996, a time when the Internet had about 77 million active users,[84] and when download speeds were of around 28,000 bits per second.[85] That context is quite different from today's, as reflected in current statistics (over 3 billion users[86] and downloading speeds of 26 megabytes per second[87]). In fact, most rulings made by the Supreme Court on this issue[88]—the same rulings that are used by proponents of untethered eAccess—predate the internet and the dematerialization of data: innovations that have made it easy for individuals and corporations to collect massive amounts of private information while mining public documents.[89] In this sense, court records accessible through eAccess could quickly become another repository of big data to be exploited by third parties,[90] something that was unfathomable in 1996.

In light of this technological evolution (some would say "revolution"), should unrestricted eAccess to court records be allowed to ensure that the rule of public accessibility is respected, or should it be limited due to the private nature of the requested contents? According to Dickson J in *AG of Nova Scotia v MacIntyre*: "[t]he rule should be one of public accessibility, to be departed from only if necessary to protect […] *'social values of superordinate importance'*"[91] (emphasis added), such as protection of the innocent. The question therefore becomes that of establishing if, considering the current technological

context, the protection of private data has become a "social value of superordinate importance." To put things differently, we need to identify what the expectation of privacy of Canadian citizens is and should be with regard to their private information once said information is filed with the courts and made available electronically to third parties. Thankfully, although no Canadian studies on this issue have been published,[92] anecdotal evidence does seem to support the position that "the transition to electronic records requires that the whole question of what personal information truly belongs on the public record needs to be rethought."[93] Here is an illustration:

> Earlier this year the City of Victoria made assessment information available on its internet web site. This lasted for one day at which time the mayor shut down the web site. Why? The public complained in large numbers that they didn't like the fact that anyone connected to the internet could have such ready access to assessment information. Yet the exact information has been and remains available on paper at city hall.
>
> I believe this example amply demonstrates that the public feels that it does make a difference when information which has been publicly available in a paper-only world becomes available electronically.
>
> In my opinion, in order for government organizations to determine what personal information should be publicly available electronically, a new test is needed – what I have heard described as putting the information to the "Internet Challenge". This test would involve an assessment of how the public would respond if the information was available on the internet where quite literally anyone in the world would have access to it. If the sense was that the public would respond negatively, the personal information should not be made publicly available in identifiable form in an electronic format.[94]

Although this "Internet Challenge" seems to fly in the face of the open court principle, there is precedent that makes it possible to qualify privacy as a social value of superordinate importance, therefore giving credence to such a litmus test:

> Privacy is recognized in Canadian constitutional jurisprudence as implicating liberty and security interests. In *Dyment*, the court

> stated that privacy is worthy of constitutional protection because it is "grounded in man's physical and moral autonomy," is "essential for the well-being of the individual," and is "at the heart of liberty in a modern state."[95]

These are strong arguments in favour of considering privacy as a social value of superordinate importance which, when considered against the backdrop of technological innovations and data mining, make it difficult to claim that eAccess should be completely untethered, therefore justifying the implementation of ways to limit eAccess through technological means. A parallel could also be drawn with the recently recognized "right to be forgotten" under European law. In *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*,[96] the Court of Justice of the European Union established that information should not be made available online if it "appears […] to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue."[97] Since the purpose in the case of eAccess to court records is the aforementioned need for there to be "public scrutiny of the courts,"[98] it could be said that eAccess to certain court documents containing private data is excessive,[99] therefore justifying the application of technical measures such as those imposed on Google and other browsers (i.e., dereferencing certain types of documents).

Finding New Means to Ensure "Practical Obscurity"

The default reaction to the manner in which we should go about restricting eAccess to court records seems to be that we should allow only judges and officers of the court[100] to access information at a distance, while having all other individuals travel to a courthouse or other controlled location to consult a dedicated terminal, therefore ensuring that practical obscurity remains with regards to those who would consult court records for improper purposes. This solution, however, seems unsatisfactory for three reasons.

First, it creates an unfair advantage for litigants who are represented by an attorney, therefore going against the "equality of arms" principle that is considered by some to be a pillar regarding access to justice.[101] Even if the application of said principle within the Canadian legal system is cause for debate,[102] the fact remains that it seems unjust for the courts themselves to allow one party unencumbered access to court records, while limiting access to the opposing party.[103]

Second, practical obscurity also promotes uneven access for third parties. As Marc-Aurèle Racicot puts it, "Only those individuals or organizations with unlimited time or resources, could easily and rightfully access any locations to gather the data to build information banks for their own purposes. If practical obscurity was an integral privacy safeguard, it was a very poor one, and also very discriminatory."[104]

Third, limiting eAccess to onsite consultations doesn't really take advantage of all that the technology has to offer and, therefore, requires an important financial investment[105] with very little return where access to justice is concerned since, as described earlier, even those who have a legitimate reason to consult court records will be deterred by consultation schedules and travel costs.

Consequently, instead of limiting offsite access, limiting functionalities seems like a more appropriate manner of addressing the situation. This can be done through (1) technological means, or even (2) through the use of intellectual-property legislation.

1. Privacy Through Limited Search Functions and Other Technological Means

The obvious starting point in controlling eAccess is identifying which documents or, rather, which information should be made accessible. As one author puts it:

> The adjudicatory facts upon which a court relies to dispose of a case or controversy according to the rule of law need never include the specific, arbitrarily assigned street address of a person's home, the precise series of numerals composing his or her telephone number, or the exact digits of his or her Social Security number. That a person has a Social Security number may be relevant to the just and rational disposition of a case, but the specific number will not be. That a person resides along a particular street or next to one of the parties may be relevant, but the exact house number will not be. Similarly, the general education that an individual might be expected to acquire from the perusal of court records does not include committing to memory the street addresses of fellow citizens, their Social Security numbers, or their bank accounts. Accordingly, such information should be omitted from publicly accessible court records and documents, irrespective of their form or the public's method of accessing them.[106]

Second, it becomes important to assess what access entails. Does it simply grant a right to view, or does it also grant a right to copy, publish, broadcast, and such. Regarding this latter possibility, it seems that access should not encompass the right to broadcast, at least not during the trial: "No case has come to my attention in which a Canadian appellate court has ruled that a media applicant is to have unfettered access to an exhibit of this nature for copying purposes so that it may broadcast the evidence during an ongoing jury trial."[107]

Furthermore, in criminal matters, access should always be weighed against the accused's right to a fair trial: "In this particular case, dissemination to the public and public access to this material in videotaped format can only serve to sensationalize the evidence with the real possibility of an adverse impact on the accused's fair trial rights."[108]

The previous quote also elicits another interesting question: does access have to be given to the original version of a document (e.g., a video recording), or is access to a transcript sufficient to meet the "strong presumption in favour of public access to court records"?[109] According to one decision, a transcript would be sufficient when the dissemination of footage could be prejudicial to the accused:

> Having acknowledged that discretion, I caution myself that publication of court exhibits in pictorial form must not disrupt the proper and orderly discharge of this trial. Furthermore, the accused's right to a fair trial and the legitimate privacy rights of any witness or even non-witness must be protected from undue sensationalism. After all, written words tend to be more rational and less evocative than pictures or film. Pictures and film often evoke immediate visceral response whereas words generally require reflection and assessment. The public seeing the pictures or film lacks the calm serenity of a courtroom and the limiting instruction the trial judge gives the jury as to the use to be made of the pictorial exhibit.[110]

Of course, the previous examples all pertain to access *during* the proceedings, but what of the accessibility of these same documents *after* the trial is over? Should access be allowed to ensure that the open court principle is respected, or disallowed because of the sensational nature of the requested contents? Actually, if it is agreed that the

documents made available to the public after the proceedings do not need to be originals[111] or, rather, documents resulting from the transfer of an original document,[112] and that certain types of private data are not deemed necessary to allow for "public scrutiny of the courts,"[113] then there is a way to allow eAccess while protecting personal information through the use of what Lawrence Lessig refers to as "Code,"[114] that is, the architecture of the internet or, in the case at hand, eAccess software. As one author puts it, Code "determines which people can access which digital objects…. How such programming regulates human interactions…depends on the choices made."[115]

In the case of eAccess, Code can be used to control access to a document "by means of a restricted view technique"[116] such as blanking.[117] It could also be used to set constraints on consultation periods, to block aggregation tools,[118] or to simply limit research functions within certain types of documents.[119] After all, as pointed out by some authors, access is only truly a problem when files and documents are searchable:

> Online, documents are not only easier to access – they are easier to find. Access to paper records typically requires that one first identify the case number (or name) and the courthouse. Paper records can be cross-indexed according to a (small) number of identifiers (e.g., case number and case name), thus providing alternate means of access. It is not possible, however, to index paper documents "on the fly" according to different criteria, nor is it possible to index paper documents according to specific aspects of content. Electronic documents, however, can be identified virtually instantaneously according to any number of criteria, and documents can be identified on the basis of content as well as "header" or traditional identifying information and specific case files could be identified on the basis of partial information that does not include the traditional identifiers of case name and/or case number.[120]

That being said, not only *can* Code be used to curb such extensive research functions,[121] it should. For example, in Quebec, section 24 of *An Act to Establish a Legal Framework for Information Technology*[122] states that

> The use of extensive search functions in a technology-based document containing personal information which is made public

> for a specific purpose must be restricted to that purpose. The person responsible for access to the document must see to it that appropriate technological means are in place to achieve that end. The person may also set conditions for the use of such search functions, in accordance with the criteria determined under paragraph 2 of section 69.[123]

Therefore, through the use of Code, it is possible to provide public access to court records without having to answer the question "who is the public?"[124] Of course, the public will not have access to all the information contained in a court file, but it will have access to all pertinent information to "comment on the courts as an essential aspect of our democratic society."[125]

This will obviously require judges to enact rules as to which information will be made available through eAccess so that clerks can classify said information properly[126] (something that should be relatively quick if the eAccess software is programmed using a legally driven approach such as the one developed by the Cyberjustice Laboratory[127]), but, as section 49 of the Quebec *Code of Civil Procedure*[128] states, this remains within a judge's purview:

> The courts and judges, both in first instance and in appeal, have all the powers necessary to exercise their jurisdiction.
>
> They may, at any time and in all matters, even on their own initiative, grant injunctions or issue orders *to safeguard the parties' rights for the period and subject to the conditions they determine*. As well, they may make such orders as are appropriate to deal with situations for which no solution is provided by law. (Emphasis added)

2. Privacy Through Intellectual Property Rights

To close out this section, we would like to mention a less-travelled route than the "Code" argument that could become a hurdle to eAccess: intellectual property rights. As is well established, court records will almost certainly contain copyrighted materials.[129] Therefore, parties could theoretically object to their being accessible online through the use of copyright laws,[130] even if the true purpose of such an objection is the protection of their privacy or of that of a third party.

Granted, copyright laws were never designed to uphold privacy rights, and there are exceptions within the *Copyright Act*[131] as

interpreted by the courts[132] that allow for copyrighted material to be made public when incorporated in court records, but these exceptions do not necessarily cover eAccess. As quoted in *Vallance v Gourlay-Vallance*,[133] "government should not be in the business of publishing public documents […] government is simply required to make such documents available."[134] However, by allowing for eAccess to court documents, courts are not simply making copyright material available, they are effectively communicating them to the public by telecommunication, a right that is reserved to the copyright holder under section 3(1)(f) or the *Copyright Act*. As one author puts it, courts "have effectively moved from repositories of documents to active publishers."[135]

Obviously, a party suing the courts for copyright violation seems like a far-fetched idea, but it does raise a further argument to deter third parties from gathering data through court records. For example, Rule 2.504 of the 2015 California Rules of Court[136] states that

> The court must give notice of the following information to members of the public accessing its records electronically, in any manner it deems appropriate: […]
> (2) That copyright and other proprietary rights may apply to information in a case file, absent an express grant of additional rights by the holder of the copyright or other proprietary right. This notice must advise the public that:
> (A) Use of such information in a case file is permissible only to the extent permitted by law or court order; and
> (B) Any use inconsistent with proprietary rights is prohibited.

Such a warning might be sufficient to deter certain members of the public and, when joined with the proper technological barriers, may yet make eAccess both efficient and protective of copyright and, indirectly, privacy rights.

Furthermore, since section 29 of the *Copyright Act* allows for "[f]air dealing for the purpose of research, private study, [and] education", and since "Lawyers carrying on the business of law for profit are conducting research within the meaning of s. 29 of the Copyright *Act*,"[137] individuals who seek to consult such documents to prepare their own cases could do so without fear of litigation.[138] The same principle would logically apply to members of the public and the press who wish to "comment on the courts as an essential

aspect of our democratic society,"[139] as section 29.2 of the *Copyright Act* extends the fair dealing exception to news reporting. It should finally be applicable to those who would require access for the purpose of insuring "public scrutiny of the courts,"[140] which would logically fall under the exception of "[f]air dealing for the purpose of criticism or review" as per section 29.1 of the Act. However, mining these documents to gather marketable data would most likely fall outside the fair dealing exception, as one could gather from *Waldman v Thomson Reuters Corporation*,[141] where a class action suit was filed against the publisher for copying "court documents that have been authored by lawyers and reproduces them on an electronic data base and search and retrieval service known as 'Litigator.'"[142] Although the reach of a settlement in the case has ultimately prevented us from obtaining a clear decision as to whether or not lawyers have a copyright in court documents,[143] the class action authorization did, at the very least, hint at such a possibility.

Conclusion

To conclude, even if one agrees that better access to justice should remain the light that guides all decisions as to how our legal system is to evolve, there is no certainty that such a goal can be reached through facilitated eAccess to court records. As is often restated, technology is not neutral[144] and, therefore, eAccess software will generate both positive and negative externalities. On the one hand, it will make the legal system more transparent, but on the other, it might very well discourage potential litigants from addressing the courts for fear of exposing their lives to the public.[145] Therefore, eAccess could, if not properly curtailed, have the pernicious effect of discouraging individuals from seeking justice or, rather, to forgo the judicial system in favour of more private dispute resolution mechanisms such as arbitration.[146]

Keeping this in mind, before allowing eAccess to court records, the question, as with any other cyberjustice innovation, should not be "what do we have to gain or lose from the process?"—the answer to both questions seems obvious—but rather how to best use the technology in a way that corresponds to our fundamental legal principles.[147] Limiting the use of extensive search functions might be a way to reach this end, as could restraining access to certain types of data through advanced algorithms. However, one thing is certain: trying

to recreate practical obscurity in an online environment is both counterproductive and hopeless. As the Information and Privacy Commissioner for British Columbia put it, "[t]he ease of paper-to-electronic transformation suggests that the practical obscurity that is often considered to be a feature of paper records is less meaningful than many observers have contended."[148] In other words, practical obscurity is dead. Consequently, rather than trying to revive it, we must find new ways of reaching the same ends: protecting privacy while allowing for transparency. In some ways, technology is actually better suited to doing this than paper documents since "controlling access to a document by means of a restricted view technique," while impossible with paper documents, is not only feasible in an online environment, it is also the law in many jurisdictions when dealing with private or otherwise confidential information.[149]

Notes

1 This paper was made possible by a grant from the Social Sciences and Humanities Research Council of Canada.

2 The report, which used to be available at: http://www.timescolonist.com/news/Special+Report+Access+denied+open+court+system/2520905/story.html, is no longer accessible online.

3 Although not directly linked to this particular issue, "[t]he ministry's motivation to move online stems partially from a problem familiar to many employers: the impending mass retirement of baby boomers is expected to leave a big hole in its workforce." See Robert Todd, "The New Frontier" (7 September 2010), online: *Canadian Lawyer* <www.canadianlawyermag.com/2092/The-new-frontier.html>.

4 Action Committee on Access to Justice in Civil and Family Matters, "Access to Civil & Family Justice – A Roadmap for Change" (2013) at 35, online: *Canadian Forum on Civil Justice* <www.cfcj-fcjc.org/sites/default/files/docs/2013/AC_Report_English_Final.pdf>.

5 This is the case, for example, in many U.S. state and federal courts. See Rebecca Hulse, "E-Filing and Privacy," *SUM Crim Just*, 24 (2009) at 14.

6 For more on the benefits of eAccess, see Gregory M Silverman, "Rise of the Machines: Justice Information Systems and the Question of Public Access to Court Records Over the Internet," *Wash L Rev* 79 (2004):175 at 179.

7 Action Committee on Access to Justice in Civil and Family Matters, *supra* note 4 at 16–17.

8 This seems to be the case as neither the *Personal Information Protection and Electronic Documents Act* (SC 2000, c 5) [PIPEDA], nor the *Privacy Act* (RSC 1985, c P-21) apply to court records. See David Loukidelis, "Privacy and Openness in Administrative Tribunal Decisions," *Can J Admin L & Prac* 22 (2009) at 75.

9 See e.g., *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, CQLR c A-2.1, section 3; and *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, section 4(1) a. See also *Alberta (Attorney General of) v Krushell*, 2003 ABQB 252 at para 26, [2003] 7 WWR 174: "There has long been a process whereby people can go to the courthouse and obtain access to court records, subject to orders of the court saying: these records will be sealed, and you can't get at them. That's primarily what we were after there. There's already a process in place for access to court records, and because of the importance of openness of the courts the provisions of privacy have been set aside for a higher social policy of allowing people to see what's going on in the court system. So that's the reason they're excluded, primarily."

10 For such a proposition, see Marc-Aurèle Racicot, "The Open Court Principle and the Internet: Transparency of the Judicial Process Promoted by the Use of Technology and a Solution for a Reasoned Access to Court Records," *R du B* 66 (2006) at 333.

11 Although the concept of "confidential information" is not defined by the Canadian legislator, we use the expression to regroup all data that the parties or the law considers private, secret or otherwise protected. See Nicolas Vermeys, Julie M Gauthier and Sarit Mizrahi, "Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec", a study prepared for the Conseil du trésor du Québec, 2014.

12 Judges Technology Advisory Committee - Canadian Judicial Council, "Model Policy for Access to Court Records in Canada" (2005), online: <http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf>. As the model policy goes on to state: "This definition does not include other records that might be maintained by court staff, but that are not connected with court proceedings, such as license and public land records. It does not include any information that merely pertains to management and administration of the court, such as judicial training programs, scheduling of judges and trials and statistics of judicial activity. Neither does it include any personal note, memorandum, draft and similar document or information that is prepared and used by judges, court officials and other court personnel."

13 Ibid.

14 This could explain why the Supreme Court's decision to make factums available online hasn't caused an uproar in the privacy community. See Supreme Court of Canada, "Policy for Access to Supreme Court of Canada Court Records" (2015), online: <http://www.scc-csc.ca/case-dossier/rec-doc/pol-eng.aspx>.

15 See e.g., Karen Eltis, "The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context," *McGill LJ* 56:2 (2011) at 289. See also Beverley McLachlin, "Courts, Transparency and Public Confidence – To the Better Administration of Justice," *Deakin Law Review* 8:1 (2003) at 1; and Catherine Piché, "Justice Wide Open: Transparency of the Judicial Process in Modern Technological Courtrooms," in *Transparency, A Governance Principle*, ed. Dominique Custos, (Brussels: Bruylant, 2014) at 225. For the opposing view, see Racicot, *supra* note 10.

16 *Lac d'Amiante du Québec Ltée v 2858-0702 Québec Inc*, 2001 SCC 51, [2001] 2 SCR 743 [*Lac d'Amiante*].

17 *Privacy Act*, *supra* note 8.

18 See e.g., *An Act respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, *supra* note 9.

19 "Discussion Paper Prepared on Behalf of the Judges Technology Advisory Committee for the Canadian Judicial Council on Open Courts, Electronic Access to Court Records, and Privacy," online: <http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_OpenCourts_20030904_en.pdf> [discussion paper] ("[…] the right of the public to open courts is an important constitutional rule, that the right of an individual to privacy is a fundamental value, and that the right to open courts generally outweighs the right to privacy").

20 *Lac d'Amiante*, *supra* note 16 at para 70.

21 *Attorney General of Nova Scotia v MacIntyre* [1982] 1 SCR 175 at para 14, 132 DLR (3d) 385 [*MacIntyre*].

22 Washington Courts, "Washington State Access to Justice Technology Principles" (2004), online: <https://www.courts.wa.gov/court_rules/?fa=court_rules.display&group=am&set=ATJ&ruleid=amatj02principles>.

23 *Edmonton Journal v Alberta (Attorney General)*, [1989] 2 SCR 1326 at paras 10-11, 64 DLR (4th) 577 [*Edmonton Journal*].

24 Ibid.

25 Ibid: "It is equally important for the press to be able to report upon and for the citizen to receive information pertaining to court documents. It was put in this way by Anne Elizabeth Cohen in her article "Access to Pretrial Documents Under the First Amendment," *Colum L Rev* 84 (1984):1813 at 1827: Access to pretrial documents furthers the same societal needs served by open trials and pretrial civil and criminal proceedings. Court officials can be better evaluated when their actions are seen by informed, rather than merely curious, spectators."

26 *AB v Bragg Communications Inc*, 2012 SCC 46 at para 11, [2012] 2 SCR 567 [*AB v Bragg*]; see also McLachlin, *supra* note 15 ("Openness signifies that the public and the press have free access to the courts of justice and are entitled to attend and observe any hearing. It signifies that court records and documents are available for public examination)."

27 *Edmonton Journal v Alberta (Attorney General)*, [1989] 2 SCR 1326 at paras 10–11, 64 DLR (4th) 577 [*Edmonton Journal*]. For an analysis of the open court principle and its origins, see Jacquelyn Burkell and Jane Bailey, "Revisiting Presumptive Accessibility: Reconceptualizing the Open Court Principle in an Era of Online Publication" (forthcoming). See also Piché, *supra* note 15.

28 *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982*, being Schedule B to the Canada Act 1982 (UK), 1982, c. 11.

29 *Canadian Broadcasting Corp v New Brunswick (Attorney General); Re R. v Carson*, [1996] 3 SCR 480 at para 23, 182 NBR (2d) 81 [*CBC 1996*] .

30 *MacIntyre, supra* note 21.

31 Ibid. at 185. This passage is also quoted in *Edmonton Journal*, *supra* note 23.

32 *MacIntyre, supra* note 21 at 189. This passage is also quoted in *Edmonton Journal*, *supra* note 23.

33 See e.g., Eltis, *supra* note 15.

34 Daniel Morman and Sharon R Bock, "Electronic Access to Court Records", *NOV Fla B J* 78 (2004):10 at 13. The authors are quoting the *HeraldTribune.com* website.

35 *Canadian Broadcasting Corp v Canada (Attorney General)* 2011 SCC 2, [2011] 1 SCR 19 [*CBC 2001*] .

36 *CBC 1996*, *supra* note 29 at para 26.

37 *Edmonton Journal*, *supra* note 23.

38 *CBC 2001*, *supra* note 35.

39 *R v Canadian Broadcasting Corporation*, 2007 CanLII 21124 at para 50 (ONSC).

40 Ibid.

41 For more on this concept, see Burkell and Bailey, *supra* note 15; Piché, *supra* note 15 at 236–37; and Racicot, *supra* note 10 at 345. See also Arminda Bradford Bepko, "Public Availability or Practical Obscurity: The Debate over Public Access to Court Records on the Internet," *NYL Sch L Rev* 49 (2004) at 967; and Nancy S Marder, "From Practical Obscurity to Web Disclosure: A New Understanding of Public Information," *Syracuse L Rev* 59 (2008) at 441.

42 It should be noted, as one author demonstrated, that this is not necessarily a good thing. Although privacy advocates present practical obscurity as a positive thing, it should be pointed out that it also has the undesirable effect of limiting access to justice. See Racicot, *supra* note 10 at 350.

43 Eric Hartley, "Courts Confront Perils of Openness" (2012), online: *Hometown Annapolis* <*www.HometownAnnapolis.com*>.

44 See *Ontario (Finance) (Re)*, 1996 CanLII 7740 (ON IPC) [*Re Ontario Finance*]: "In Ontario, assessment information is publicly available by law. For years anyone has been able to go to the office of the clerk of a municipality and view the assessment roll. However, the paper medium on which information was stored provided a built-in privacy protection. Although it was possible to go to a municipality and copy out the information contained on the paper rolls, using the appellant's situation as an example, in order to do so he would have to travel to 11 municipal offices and copy thousands of pages. The sheer enormity of this task made it unlikely that assessment information would be used other than for assessment-related purposes. Using words of the U.S. Supreme Court, I have described this as privacy protection based on 'practical obscurity'." See also Piché, *supra* note 15 at 237.

45 PIPEDA, *supra* note 8 at s 7.

46 *Privacy Act*, *supra* note 8.

47 See Amanda Conley et al., "Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry," *Maryland Law Review* 71 (2012) at 772; Woodrow Hartzog and Frederic Stutzman, "The Case for Online Obscurity," *California Law Review* 101:1 (2012):1 at 21; Will Thomas Devries, "Protecting Privacy in the Digital Age," *Berkeley Tech L J* 18 (2003):283 at 301; Lewis A Kaplan, "Litigation, Privacy and the Electronic Age," *Yale Symp on L & Tech* 4 (2001):1 at 6; Caren Myers Morrison, "Privacy, Accountability, and the Cooperating Defendant: Towards a New Role for Internet Access to Court Records," *Vand L Rev* 62 (2009) at 921; Peter A Winn, "Judicial Information Management in an Electronic Age: Old Standards, New Challenges," *Fed Cts L Rev* 3 (2009) at 135; Peter A Winn, "Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information," *Wash. L. Rev* 79 (2004) at 307; Lynn E Sudbeck, "Placing Court Records Online: Balancing the Public and Private Interests," *The Justice System Journal* 27:3(2006) at 268; Bepko, supra note 41; Kristen M Blankley, "Are Public Records Too Public? Why Personally Identifying Information Should Be Removed from Both Online and Print Versions of Court Documents," *Ohio St L J* 65 (2004) at 413; John Losinger, "Electronic Access to Court Records: Shifting the Privacy Burden Away from Witnesses and Victims," *U Balt L Rev* 36 (2007) at 419; and David L Snyder, "Nonparty Remote Electronic Access to Plea Agreements in the Second Circuit," *Fordham Urb L J* 35 (2008) at 1263.

48 *Re Ontario Finance, supra* note 44. See also *Toronto (City) (Re)*, 2000 CanLII 21004 (ON IPC). This same issue was later raised by the Canadian Judicial Council in its 2003 discussion paper on electronic access to court records: "Where court records are open to access by the public

but searching capacity is reduced by the need to identify files in court ledgers and file retrieval fees, 'practical obscurity' prevails. The theoretical openness is limited by logistical barriers. However, where electronic access exists, the definition of 'public' will likely expand" ((Judges Technology Advisory Committee, "Discussion Paper", *supra* note 19 at 36).

49 It should however be noted that such a document is currently being worked on by the Quebec Department of Justice for possible adoption in the coming months.

50 Judges Technology Advisory Committee, "Model Policy," *supra* note 12.

51 Section 31 of *PIPEDA* defines electronic documents as "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."

52 In fact authors are still coming to the same conclusion some twenty years later. See e.g., Burkell and Bailey, *supra* note 15: "In the past, access to court documents required a visit to the specific court where the documents were held. Access was restricted to the opening hours of the court office, and those wishing to access the documents had to make those requests in person – thus fully anonymous access of those documents was not possible. All this changes with online documents, since these can be accessed at any time, using any computer with an Internet connection, typically anonymously and even invisibly. In other words, barriers or 'friction' in online court document access are greatly reduced if not eliminated, and as a result the personal information included in these documents is no longer protected by the 'practical obscurity' inherent in access to paper documents."

53 Judges Technology Advisory Committee, "Discussion Paper," *supra* note 19 at 36–37.

54 See Racicot, *supra* note 10.

55 See Kristin M Makar, "Taming Technology in the Context of the Public Access Doctrine: New Jersey's Amended Rule 1:38," *Seton Hall L Rev* 41 (2011):1071 at 1088.

56 For example, the CanLII website had to modify its terms of use to forbid these types of abusive uses of its databanks. See CanLII, "Terms," online: <http://www.canlii.org/en/info/terms.html>.

57 Which court records are according to the *Regulations Specifying Publicly Available Information*, SOR/2001-7, s 1(d).

58 PIPEDA, *supra* note 8 at Sched 1, s 4.3 ("The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate").

59 *Regulations Specifying Publicly Available Information*, *supra* note 57 at s 1(d).
60 *Ibid.* See also Canadian Bar Association, "Submission on the Discussion Paper: Open Courts, Electronic Access to Court Records, and Privacy" (2004), online: <www.cba.org/cba/submissions/pdf/04-13-eng.pdf>.
61 *Mortgage administrator/broker should have confirmed consent prior to issuing letter of interest for mortgage financing in couple's name*, 2012 CanLII 96454 (PCC): "PIPEDA's regulations specify that publicly available personal information is that which appears in a record or document of a judicial or quasi-judicial body that is available to the public, *where the collection, use and disclosure of the personal information relate directly to the purpose for which the information appears in the record or document*."
62 France Houle and Lorne Sussin, *Powers and Functions of the Ombudsman in the Personal Information Protection and Electronic Documents Act An Effectiveness Study* (Ottawa, Office of the Privacy Commissioner of Canada, 2010).
63 For example, the PACER system in the United States (http://www.pacer.gov/) allows just that. See Philip Leith and Maeve Mcdonagh, "New Technology and Researchers' Access to Court and Tribunal Information: the need for European analysis," *SCRIPTed* 6:1 (2009) at 33.
64 See Mark S Hayes, "The Impact of Privacy on Intellectual Property in Canada," *I P J* 20 (2006):67 at 83.
65 *Re Ontario Finance*, *supra* note 44.
66 Courtney Retter & Shaheen Shariff, "A Delicate Balance: Defining the Line between Open Civil Proceedings and the Protection of Children in the Online Digital Era," *Can J L & Tech* 10 (2012):231 at 238. See also Jennifer Stoddart, "Setting the "Bar" on Privacy Protection" (2008), online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/media/sp-d/2008/sp-d_080817_e.asp>.
67 CanLII, online: <www.canlii.org>.
68 *PIPEDA Report of Findings #2015-002*, online: *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/cf-dc/2015/2015_002_0605_e.asp>.
69 Globe 24h, online: <www.globe24h.com/>.
70 CanLII, "Privacy Policy", online: <www.canlii.org/en/info/privacy.html>.
71 See Globe24h, "Frequent Questions & Answers," online: <www.globe24h.com/faq.html>.
72 See *Thériault-Thibault v SOQUIJ*, 500-32-146975-158.
73 *Act Respecting the Société Québécoise d'Information Juridique*, CQLR c S-20.
74 As a matter of full disclosure, it should be mentioned that the author of this paper is the current vice-president of SOQUIJ's Board of Directors.
75 SOQUIJ, online: <soquij.qc.ca/>.
76 See *Wilson & Lafleur Inc c Société québécoise d'information juridique*, 2000 CanLII 8006 (QC CA).

77 *Thériault-Thibault c McGill Computer Store*, 2006 QCCQ 703 (CanLII).
78 See SOQUIJ, "Politique sur le caviardage" (2014), online: <soquij.qc.ca/documents/file/corpo_politiques/politique-sur-le-caviardage.pdf>.
79 Ibid.
80 See Luc Plamondon, Guy Lapalme and Frédéric Pelletier, "Anonymisation de décisions de justice," TALN 2004, Fès, 19–21 April 2004.
81 *Canada Evidence Act*, RSC 1985, c C-5, s 31.2.
82 For examples of what this data could be used for, see Eltis, *supra* note 15 at 301.
83 *CBC 1996*, *supra* note 29.
84 See Internet Live Stats, "Number of Internet Users," online: <www.internetlivestats.com/internet-users/>.
85 See Brian Nelson, "New Modem Will Speed up Internet Access" (1996) *CNN Interactive*, online: <www.cnn.com/TECH/9610/04/faster.internet/>.
86 See Internet Live Stats, *supra* note 84.
87 Ibid.
88 *MacIntyre*, *supra* note 21; and *Edmonton Journal*, *supra* note 23.
89 This has been decried by then privacy commissioner Jennifer Stoddart. See Kirk Makin, "Online Tribunal Evidence Leaves Citizens' Data open to Abuse," *The Globe and Mail*, August 20, 2008, A5. See also Eltis, *supra* note 15 at 292.
90 See Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2013).
91 *MacIntyre*, *supra* note 21 at para 14. See also *AB v Bragg*, *supra* note 26 at para 13.
92 It should however be noted that such a study is to be conducted as part of the "Towards Cyberjustice" project led by the Cyberjustice Laboratory. See Cyberjustice Laboratory, "The Project," online: <www.cyberjustice.ca/en/the-project/>.
93 *Re Ontario Finance*, *supra* note 44.
94 Ibid.
95 *Toronto Star Newspaper Ltd v Ontario*, 2012 ONCJ 27 at para 41, as cited in *AB v Bragg*, *supra* note 26 at para 18.
96 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12.
97 Ibid. at para 94.
98 *Edmonton Journal*, *supra* note 23.
99 It should be noted, however, that the parallel drawn between eAccess to court records and the aforementioned right to be forgotten is not a perfect one since, unlike websites, court records have a regulated shelf life. See e.g., the Quebec *Archives Act*, CQLR c A-21.1, section 7.

100 By "officers of the court," we refer to "All persons who may practise as barristers, advocates, counsel, attorneys, solicitors or proctors in the Court," as per the *Supreme Court Act*, RSC 1985, c S-26, s24.

101 See Harry Woolf, *Access to Justice: Interim Report to the Lord Chancellor on the Civil Justice System in England and Wales* (London, Lord Chancellor's Department, 1995) as quoted by Master D E Short in many cases including *Simpson v Attorney General (Canada)*, 2011 ONSC 3642 at para 18 (CanLII); *1588143 Ontario Inc v Lantic Inc*, 2010 ONSC 1613 at para 36 (CanLII); *Bank of Montréal v Baysong Developments Inc*, 2011 ONSC 931 at para 41 (CanLII); *Green v Mirtech International Security Inc*, 2010 ONSC 1240 para 32 (CanLII); *Rohit v Nuri*, 2010 ONSC 17 at para 34 (CanLII); and *HMQ (Ontario) v Rothmans Inc*, 2011 ONSC 1083 (CanLII). This last case was however overturned since it was found that Master Short "erred by misapplying the "equality of arms" principle." See *Ontario v Rothmans Inc*, 2011 ONSC 2504 at para 105 (CanLII). For other applications of the "equality of arms principle," see e.g., *Homebrook v Seprotech Systems*, 2011 ONSC 3100 at para 7 (CanLII); and *IPEX Inc v AT Plastics Inc*, 2011 ONSC 4734 at para 55 (CanLII).

102 *Imperial Tobacco Canada Ltd v Québec (Procureur général)*, 2014 QCCS 842 (CanLII).

103 See D R Jones, "Protecting the Treasure: An Assessment of State Court Rules and Policies for Access to Online Civil Court Records," *Drake L Rev* 61:2 (2013):375 at 394.

104 Racicot, *supra* note 10 at 356.

105 Makar, *supra* note 55 at 1084.

106 Silverman, *supra* note 6 at 209.

107 *R v Canadian Broadcasting Corporation*, 2007 CanLII 21124 at para 82 (ON SC).

108 Ibid. at para 81.

109 Ibid. at para 50.

110 *R v Ranger*, [1998] OJ No 1654 (Ont Ct Justice Gen Div) (QL).

111 *An Act to Establish a Legal Framework for Information Technology*, CQLR c C-1.1, 12.

112 Ibid. at s 17.

113 *Edmonton Journal*, *supra* note 23.

114 Lawrence Lessig, *Code version 2.0* (New York, Basic Books, 2006).

115 Mark Stefik, *The Internet Edge: Social, Technical, and Legal Challenges for a Networked World* (Cambridge, MIT Press, 1999) at 14, as quoted in Lessig, *supra* note 114 at 6.

116 *An Act to Establish a Legal Framework for Information Technology*, *supra* note 111 at s 25.

117 Blanking is a process that consists of masking certain data when an individual does not have the proper security clearance to access said

data. As one author puts it: "For example, when a party or attorney authors a document for filing with a court, he or she could include markup for recognized categories of personal information that the public should be restricted from viewing. Once filed, this document would be stored on a justice information system capable of processing XML markup. Then, when a member of the public accesses this document at a courthouse computer terminal or over the Internet, generic text such as a series of Xs--possibly hyperlinked to a message that explains that personal information has been omitted--would be substituted for the tagged personal information. Moreover, when the same document was accessed by the judge or an attorney of record, the justice information system would be programmed to display the entire document, including the sensitive personal information. As this example makes clear, the justice information system would be programmed to respond to a hierarchy of user access privileges, providing to each user the information that he or she is authorized to view. Significantly, such a system would discriminate among users and not the methods by which they accessed the system. A particular user would be granted access to the same information, whether that user was accessing the system at the courthouse or over the Internet." See Silverman, *supra* note 6 at 211.

118 Lynn M LoPucki, "Court System Transparency," *Iowa L Rev* 94 (2009):481 at 528.

119 One such mean would be to make documents containing private data non-machine readable. See LoPucki, *supra* note 118 at 522.

120 Burkell and Bailey, *supra* note 15.

121 See Silverman, *supra* note 6 at 211 (we can "use XML tags to mark up sensitive personal information and control access to it programmatically); see also Conley et al., *supra* note 47.

122 *An Act to Establish a Legal Framework for Information Technology*, *supra* note 111.

123 Ibid. at s 24. As for paragraph 2 of section 69 of the Act, it simply states that: "69. […] the Government may make regulations determining […] (2) criteria for the use of extensive search functions in respect of personal information contained in technology-based documents that are made public for a specific purpose." The same principle was put forth in section 4.5 of Judges Technology Advisory Committee "Model Policy," *supra* note 12. This concept is analog to the "Right to be forgotten" recently recognised by the Court of Justice of the European Union in *Google Spain SL, Google Inc.* v *Agencia Española de Protección de Datos (AEPD), Mario Costeja González*: "the data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy

— which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information."

124 Judges Technology Advisory Committee, "Discussion Paper", *supra* note 19 at 35.

125 *CBC 1996*, *supra* note 29 at para 26.

126 This seems to be the approach that was adopted in Florida. See Morman and Bock, *supra* note 34 at 16. For an example of the rules that could be adopted under Canadian law, see Racicot, *supra* note 10. Although the author promotes a case-by-case analysis, something that we believe to be impractical in the current context, the criteria he proposes offer an interesting starting point.

127 See Nicolas Vermeys and Karim Benyekhlef, "Reinventing Rituals – How to Develop Technological Solutions to Courtroom Conundrums" (forthcoming).

128 *Code of Civil Procedure*, CQLR c C-25.01.

129 See *Waldman v Thomson Reuters Corporation*, 2012 ONSC 1138 (CanLII). Leave for appeal denied (*Waldman v Thomson Reuters Corporation*, 2012 ONSC 3436 [CanLII]); although a settlement agreement was reached was reached in this case, rendering the point moot. See *Waldman v Thomson Reuters Canada Limited*, 2014 ONSC 1288 (CanLII); *Waldman v Thomson Reuters Canada Limited*, 2015 ONCA 53 (CanLII); *Waldman v Thomson Reuters Canada Limited*, 2015 ONSC 3843 (CanLII); and *Waldman* v *Thomson Reuters Canada Limited*, 2016 ONSC 2622 (CanLII).

130 See Kathryn Yardley, "Online Tribunal Evidence Leaves Citizens' Data Open to Abuse" (2 November 2008), online: *IP Osgoode* <www.iposgoode.ca/2008/11/yardley-kathryn-online-tribunal-evidence-leaves-citizens-data-open-to-abuse/#sthash.03QqlqUZ.dpuf>.

131 *Copyright Act*, RSC 1985, c C-42.

132 Andy Radhakant, "Robust Interpretation of Court Document Copyright," *The Lawyers Weekly* 34:18 (2014) at 15.

133 *Vallance v Gourlay-Vallance*, 2002 ABQB 822, 325 AR 296.

134 Jennifer Lee, "Dirty Laundry, Online for All to See," *New York Times*, September 5, 2002.

135 Karen Eltis, *Courts, Litigants and the Digital Age – Law, Ethics and Practice* (Toronto, Irwin Law, 2012) at 54 as cited in Piché, *supra* note 15 at 247.

136 2015 California Rules of Court, online: <www.courts.ca.gov/cms/rules/index.cfm?title=two&linkid=rule2_504>.

137 *CCH Canadian Ltd v Law Society of Upper Canada*, 2004 SCC 13 at para 51, [2004] 1 SCR 339 [*CCH Canadian Ltd*, SCC].

138 See *CCH Canadian Ltd v Law Society of Upper Canada*, 2002 FCA 187 at para 128, [2002] 4 FCR 213: "'Research' is not qualified in the Act, therefore, research for a commercial purpose, including legal research carried

out for profit by entities such as law firms, is not automatically excluded from this exemption. Research for the purpose of advising clients, giving opinions, arguing cases, preparing briefs and factums is nonetheless research. Of course, if a copy is made for non-private or commercial research purposes, such a fact may affect the fairness of the dealing." This paragraph was cited with approval in *CCH Canadian Ltd*, SCC at para 51.

139 *CBC 1996*, *supra* note 29 at para 26.

140 *Edmonton Journal*, *supra* note 23.

141 *Waldman* v *Thomson Reuters Corporation*, 2012 ONSC 1138. Leave for appeal dismissed (*Waldman* v *Thomson Reuters Corporation*, 2012 ONSC 3436).

142 *Waldman* v *Thomson Reuters Corporation*, 2012 ONSC 1138, par 2.

143 See *Waldman* v *Thomson Reuters Canada Limited*, 2014 ONSC 1288; *Waldman* v *Thomson Reuters Canada Limited*, 2015 ONCA 53; *Waldman* v *Thomson Reuters Canada Limited*, 2015 ONSC 3843; and *Waldman* v *Thomson Reuters Canada Limited*, 2016 ONSC 2622 (CanLII).

144 See Langdon Winner, *The Whale and the Reactor* (Chicago: University of Chicago Press, 1986).

145 This fear is shared by other legal scholars. See e.g., Eltis, *supra* note 15 at 316: "While the decision to publish details of a tort plaintiff's sexually contracted disease may have—at first glance—appeared to constitute a victory for access and transparency, it stands to reason that so doing may dissuade similarly situated plaintiffs from availing themselves of the justice process (for fear of having intimate details exposed not only in dusty court files but online, easily googled by potential employers, landlords, even suitors, and so forth). Indeed, the ultimate result would be to deter access to the courts, thereby frustrating the goal of access in its broadest and most immediate sense."

146 See Karim Benyekhlef and Fabien Gélinas, "Online Dispute Resolution," *Lex Electronica* 10:2 (2005) at 49, online: <www.lex-electronica.org/articles/v10-2/Benyekhlef_Gelinas.pdf>.

147 See Vermeys and Benyekhlef, *supra* note 127.

148 *Sale of Provincial Government Computer Tapes Containing Personal Information*, Re, 2006 CanLII 13536 at para 58 (BC IPC).

149 See *An Act to Establish a Legal Framework for Information Technology*, *supra* note 111 at s 25; see also PIPEDA, *supra* note 8 at Sched 1, s 4.7.3.

Page left blank intentionally