McGill Law Journal
Revue de droit de McGill

The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context

Karen Eltis

Volume 56, numéro 2, february 2011

URI : https://id.erudit.org/iderudit/1002368ar
DOI : https://doi.org/10.7202/1002368ar

Aller au sommaire du numéro

Éditeur(s)

McGill Law Journal / Revue de droit de McGill

ISSN

0024-9041 (imprimé)
1920-6356 (numérique)

Découvrir la revue

Citer cet article

Eltis, K. (2011). The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context. *McGill Law Journal / Revue de droit de McGill*, *56*(2), 289–316. https://doi.org/10.7202/1002368ar

Résumé de l'article

Malgré la présence de la technologie dans tous les aspects de la vie sociale, ses effets sur le système judiciaire sont sous-théorisés. L' « ère digitale », l'accès à l'information numérique et son utilisation sans entraves auront des effets inédits sur les valeurs fondamentales de l'indépendance judiciaire et de l'impartialité, ainsi que sur l'équilibre délicat entre le respect de la vie privée et le principe de la publicité des débats. La technologie, et l'énorme augmentation de la disponibilité d'information de nature et de qualité variées, déforme tant le processus judiciaire que ses résultats. Il est donc d'une importance primordiale d'identifier les grands enjeux qui ressortent de l'utilisation croissante de la technologie et d'élaborer un fondement théorique pour examiner la tension continue entre le droit à la vie privée et la transparence en milieu judiciaire. Il arrive trop souvent que l'appareil judiciaire oppose le droit à la vie privée au principe de la publicité des débats et accepte une vision culturelle restreinte de ce que constitue le droit à la vie privée et son impact sur le processus judiciaire. Plus particulièrement, cet article étudie les effets de l'informatisation des documents des tribunaux pour déterminer pourquoi une compréhension contextuelle du droit à la vie privée est désirable, et ce, malgré la préférence actuelle pour l'ouverture et la transparence. En effet, si nous reconcevons le droit à la vie privée dans le contexte électronique, il peut être considéré comme un allié de la transparence dans le système judiciaire.

THE JUDICIAL SYSTEM IN THE DIGITAL AGE: REVISITING THE RELATIONSHIP BETWEEN PRIVACY AND ACCESSIBILITY IN THE CYBER CONTEXT

*Karen Eltis**

Despite technology's reach into all parts of social life, its effects on the judiciary have been under-theorized. The "Digital Age", and unfettered usage and access to digital information, will have untold effects on core values of judicial independence, impartiality and the delicate balance between privacy and the "open court" principle. Technology—as well as the dramatically increased availability of information of all kinds and quality—is distorting the judicial process and its outcomes. It is of primary importance, therefore, to identify the broad issues that emerge from the growing use of technology, and to provide a theoretical basis for adjudicating the ongoing tension between privacy and transparency in the judicial setting. Too often the judiciary pits privacy against the "open court" principle and accepts a culturally narrow view of what constitutes privacy and how it affects the judicial process. In particular, this article investigates the effects of online court documents to establish why, despite the current preference for openness and transparency, a contextualized understanding of privacy is desirable. Indeed, if we rethink privacy within the cyber context, it can be considered an ally of openness in the court system.

Malgré la présence de la technologie dans tous les aspects de la vie sociale, ses effets sur le système judiciaire sont sous-théorisés. L' « ère digitale », l'accès à l'information numérique et son utilisation sans entraves auront des effets inédits sur les valeurs fondamentales de l'indépendance judiciaire et de l'impartialité, ainsi que sur l'équilibre délicat entre le respect de la vie privée et le principe de la publicité des débats. La technologie, et l'énorme augmentation de la disponibilité d'information de nature et de qualité variées, déforme tant le processus judiciaire que ses résultats. Il est donc d'une importance primordiale d'identifier les grands enjeux qui ressortent de l'utilisation croissante de la technologie et d'élaborer un fondement théorique pour examiner la tension continue entre le droit à la vie privée et la transparence en milieu judiciaire. Il arrive trop souvent que l'appareil judiciaire oppose le droit à la vie privée au principe de la publicité des débats et accepte une vision culturelle restreinte de ce que constitue le droit à la vie privée et son impact sur le processus judiciaire. Plus particulièrement, cet article étudie les effets de l'informatisation des documents des tribunaux pour déterminer pourquoi une compréhension contextuelle du droit à la vie privée est désirable, et ce, malgré la préférence actuelle pour l'ouverture et la transparence. En effet, si nous reconcevons le droit à la vie privée dans le contexte électronique, il peut être considéré comme un allié de la transparence dans le système judiciaire.

* Associate Professor, University of Ottawa Faculty of Law, *Section de droit civil*; Visiting Scholar, Columbia Law School; Past Senior Adviser, National Judicial Institute.

Citation: (2011) 56:2 McGill LJ 289 ~ Référence : (2011) 56 : 2 RD McGill 289

Introduction

> "It seems as though everybody is talking about 'privacy', but it is not clear exactly what they are talking about"
>
> Daniel J. Solove[1]

Technology plays an incontrovertibly central role in contemporary judicial work and life, both on and off the bench. Along with tremendous benefits, it imports substantial new challenges that increasingly impact upon courts, litigants, and witnesses. Notwithstanding its growing relevance, the question of technology's ramifications on the courts has thus far evaded scholarly inquiry almost entirely. As a result, they are left with little choice but to attempt to fit new technologies into outdated regimes and practices.[2]

Issues such as online court records and privacy, *ex parte* electronic communication, inadvertently e-mailed draft decisions, and the challenge to judicial independence posed by government-owned and operated court servers,[3] are arising with greater frequency. These challenges have prompted courts to revisit the conventional construction of fundamental concepts such as disclosure, accountability and the delicate balance between foundational values such as transparency and privacy.[4]

In an effort to alert courts to up-and-coming matters deriving from the use of technology, this article will concern itself first with identifying emerging issues arising from technological change generally. It will then proceed to address the challenges that electronic court records raise, particularly, the inadvertent disclosure of personal information in ways unanticipated by existing rules, and the resulting affront to the very access to justice that digital files were meant to promote. Canada's Privacy

---

1 *Understanding Privacy* (Cambridge, Mass: Harvard University Press, 2008) at 5 [Solove, *Understanding Privacy*].

2 *C.f.* Daniel J Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74:2 Fordham L Rev 747. (Solove observed that "many judicial misunderstandings stem from courts trying to fit new technologies into old statutory regimes built around old technologies" at 773).

3 See *R v Lippé*, [1991] 2 SCR 114 at 137-38, 64 CCC (3d) 513. Lamer CJC, as he then was, defined judicial independence as "independence from the government", but interpreted "government" broadly enough to include "any person or body, which can exert pressure on the judiciary through authority under the state" (*ibid*).

4 See The Honourable Mr Justice T David Marshall, *Judicial Conduct and Accountability* (Scarborough: Carswell, 1995); Martin L Friedland, *A Place Apart: Judicial Independence and Accountability in Canada* (Ottawa: Canadian Judicial Council, 1995).

Commissioner pointed to this emerging predicament, indicating, "The open-court rule—which is extremely historically important—has become distorted by the effect of massive search engines."[5] In an effort to address the problem in the judicial context, this piece proposes an alternative, complementary understanding of the relationship between privacy and access in light of technological change.

With an eye towards generating practical recommendations in a crucial area previously unexplored in Canadian legal literature, this paper will adopt the following structure: Part I will provide a general introduction to the principal issues that emerging and existing technologies raise for judges and other participants in the justice process.[6] Because these cannot all be thoroughly addressed within these pages, the objective is not to provide a comprehensive survey. Instead, a few observations will be made in an effort to weave Parts II and III—which develop the questions of electronic court records, access, and privacy—into a wider fabric of reflection. Part II will then turn to online court documents more pointedly, explaining why the current presumption in favour of openness yields unsatisfactory results in light of technological change. It will proceed with an exploration of the issues surrounding the balance between the judicial system's commitment to access, transparency, and accountability; and its fundamental obligation to protect litigants, witnesses, and others. Having already exposed the ills of unfettered access in terms of quantity of information, rather than relevance or quality, this article, in Part III will then posit an understanding of privacy in this context—as part of access rather than adversative to it.[7]

I. The Impact of Technology on Courts and the Judiciary: An Overview

Before the day now known as 9/11 became forever etched in the world's collective memory, a meeting of the Judicial Conference headed by Chief Justice Rehnquist, as he then was, was scheduled for 11 September 2001.[8] The gathering in question was to address a much-decried US government proposal to monitor federal judges' electronic communications

---

5 Kirk Makin, "Online Tribunal Evidence Leaves Citizens' Data open to Abuse" *The Globe and Mail* (20 August 2008) A5.

6 See generally Karen Eltis, "The Impact of New Technologies on Courts and Judicial Ethics: An Overview" in Lorne Sossin & Adam Dodek, eds, *Judicial Independence in Context* (Toronto: Irwin Law, 2010) at 337 [Eltis, "Impact of New Technologies"] (detailed analysis of how technology affects judges and judicial ethics in particular).

7 Drawn from the broader dignity-based civilian understanding of privacy.

8 The Judicial Conference of the United States is the principal policy-making body for the federal court system. The chief justice serves as the presiding officer of the Conference.

and Internet use.[9] In the midst of vocal protest,[10] monitoring software was installed in order to surveil the Internet use of federal judges and judicial employees.[11] The proposal, touted by Congress as a push for efficiency,[12] was said to represent a significant threat to judicial independence and a

---

9 See Judicial Conference of the United States, *Report of the Proceedings of the Judicial Conference of the United States*, (Washington, DC: Administrative Office of the US Courts, 2001), online: <http://www.uscourts.gov/judconf/sept01proc.pdf> [*JCUC Report 2001*]. I have argued elsewhere that email eavesdropping presents novel challenges that need to be addressed with the *Charter* in mind: Karen Eltis, "La surveillance du courrier électronique en milieu du travail: le Québec succombera-t-il à l'approche américaine?" (2006) 51:3 McGill LJ 475 [Eltis, "La surveillance du courrier électronique"]; See also Karen Eltis, "The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Caselaw in Canada and Israel—Should Others Follow Suit?" (2003) 24:3 Comp Lab L & Pol'y J 487 [Eltis, "Privacy in the Workplace"].

10 See Robyn Weisman, "Judges Battle to Limit Workplace Monitoring", *Newsfactor* (21 September 2001), online: <http://web.archive.org/web/20011009102454/newsfactor.com/perl/story/13682.html>. See also Stefanie Olsen, "Judges Back Down on Workplace Monitoring", *CNET News* (10 September 2001), online: <http://news.cnet.com/2100-1023-272865.html>; Electronic Privacy Information Center, "EPIC Urges Federal Judiciary to End Workplace Monitoring", *Epic Alert* 8:16 (6 September 2001) online: <http://www.epic.org/alert/EPIC_Alert_8.16.html>.

11 See Gina Holland, "Panel Endorses Monitoring of Judges", *The Washington Post* (13 August 2001) online: <http://www.washingtonpost.com>. See also Administrative Office of the US Courts, News Release, "Federal Judges Issue Internet Use Policy for US Courts" (13 August 2001), online: Electronic Frontier Foundation <http://w2.eff.org/Privacy/Workplace/Judiciary/20010813_aousc_monitoring_pr.html>; Brian Krebs, Judicial Policy Board Votes by Mail on Web Monitoring", *Government Technology* (18 September 2001) online: <http://www.govtech.com/gt/5940?topic=117680>.

12 See Hardeep Kaur Josan & Sapna K Shah, "Internet Monitoring of Federal Judges: Striking a Balance Between Independence and Accountability" (2002) 20:1 Hofstra Lab & Emp LJ 153 at 158:

> The aim of the Initial Policy is twofold: (1) to secure the courts' computers by protecting them from viruses and hackers and (2) to ensure that employees [including the judges themselves] do not waste time browsing the Internet for leisure.

But further on Josan & Shah noted:

> Most critics were outraged with the proposed policy that all judiciary employees, including judges, must waive all expectations of privacy in communications made when using office equipment, including computers.
>
> Judges have criticized the monitoring on grounds that it is an invasion of privacy and that it may violate the [Electronic Communications Privacy Act] ECPA (*ibid* at 160 [footnotes omitted]).

Eventually a more moderate position emerged, see "Judges Ease Surveillance of Web Use" *The New York Times* (20 September 2001) online: <http://query.nytimes.com>.

manifest violation of the separation of powers between the judiciary and the legislature, and indeed of institutional independence.[13]

The federal judiciary's experience in the United States indicates that the idea of monitoring judges' Internet and email use for content is far from theoretical.[14] The installation of monitoring software on judges' computers is no longer unprecedented and therefore must be soberly addressed.[15] Moreover, since technology creates new criteria for measuring

---

[13] Judicial independence also significantly refers to *institutional independence*: see *Beauregard v Canada*, [1986] 2 SCR 56, 30 DLR (4th) 481. On the separation of powers and the judicial branch generally, see Cheryl Saunders, "Separation of Powers and the Judicial Branch", online: (2006) 11:4 Judicial Review 337 <http://www.adminlaw.org.uk/docs/Professor%20Cheryl%20Saunders%20-%20July%202006.doc>. More specifically, in the Canadian context, s 11(d) of the *Charter*, seeking to guarantee a fair hearing by an impartial and independent tribunal, encompasses a constitutional protection against judicial bias. Independence refers to freedom from interference of the executive or legislative branch. This aspect does not concern us at present because it relates to the tribunal's institutional, administrative, and fiscal independence, rather than that of individual judges: see generally *Valente v R*, [1985] 2 SCR 673, 24 DLR (4th) 161.

In the United States, guidelines were later adopted in this context: see Administrative Office of the US Courts, News Release, "Judicial Conference Approves Recommendations on Electronic Case File Availability and Internet Use" (19 September 2001), online: US Courts <http://www.uscourts.gov/Press_Releases/jc901a.pdf>. See also *JCUS Report 2001*, *supra* note 9 at 43 ("Use of Internet"). For a more detailed discussion of this report, see Josan & Shah, *supra* note 12.

[14] See Philip L Gordon, "Judge Leads Fight for Workplace Privacy" *The Denver Post* (20 September 2001) B-07, online: <www.denverpost.com>.

[15] See Michael Geist, *Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance* (Ottawa: Canadian Judicial Council, 2002) at 41, online: Canadian Judicial Council <www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_en.pdf>, citing "Court Technology Security: A Report of the Judges Technology Advisory Committee to the Canadian Judicial Council" (30 November 2001) at Table 2-7:

> 62 percent of respondents indicated that log-in and account activity by judges or judicial staff was monitored 29 percent of respondents indicated that dial-in and e-mail usage by judges or judicial staff was monitored 33 percent of respondents indicated that Internet usage by judges or judicial staff was monitored.

He then noted:

> The data was particularly troubling in light of responses regarding the adequacy of notice and implementation of computer and e-mail monitoring. Only 50 percent of respondents indicated that they had been informed that their computer activities may be monitored, only 33 percent of users were required to sign an Appropriate Use Agreement before receiving access to the computer system, and a paltry 5 percent of respondents indicated that their opening log-on screen clarified the expected use of the computing equipment by judges and judicial staff. Furthermore, with only 14 percent indicating that the judges or judicial staff are involved in the monitoring activity, it be-

judicial productivity, judicial dockets can be monitored with great ease, and expectations of judges' workload and performance can vary as a function of technological advances.[16] This is arguably doing violence to both independence and impartiality.[17] Similarly, government ownership of court servers may foster a perception of infringement upon the separation of powers, thus prompting some Canadian courts to take active measures towards electronically distinct servers and technical support.[18]

Let us now fast forward to 2006, to the trial of 9/11 bombing suspect Zacarias Moussaoui.[19] With the aim of promoting transparency generally, and responding to public interest in the trial specifically, the United States District Court for the Eastern District of Virginia decided to "broadcast" the proceedings on the Internet. Testimony, evidence, and related material were made available to the general public in the interest of a public trial.

Information of this nature (e.g., trial proceedings, court records) has always been public—with excellent reason. The distinction between the past and present circumstance lies in the new conception of "accessibility"; namely, now there is an audience of incalculable numbers with indiscriminate access. Individuals gain access to sensitive, personal information—oftentimes anonymously—in an unprecedented fashion. What is

---

> came apparent that the judiciary was not involved in the implementation aspect of the monitoring activities (*ibid* at 42 [footnotes omitted]).

16 See Canadian Judicial Council, *Computer Monitoring Guidelines*, (Ottawa: Canadian Judicial Council, 2002) at paras 3-4, online: Canadian Judicial Council <http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_GuidelinesCM_2002_en.pdf> [*Monitoring Guidelines*]:

> [3] As an overriding principle, any computer monitoring of judges, and judicial staff who report directly to judges, must have a well defined and justifiable purpose that does not encroach on deliberative secrecy, confidentiality, privacy rights or judicial independence.
>
> [4] Content-based monitoring of judges and judicial staff is not permissible under any circumstances. Prohibited activities include keystroke monitoring, monitoring e-mail, word processing documents or other computer files, and tracking legal research, Internet sites accessed, and files downloaded by individual users.

17 See generally Geist, *supra* note 15.

18 For example, see the guidelines set out by the Canadian Judicial Council: Canadian Judicial Council, *Model Judicial Acceptable Use Policy for Computer Technology*, (Ottawa: Canadian Judicial Council, 2003) in Canadian Judicial Council, *Blueprint for the Security of Judicial Information*, 2d ed (Ottawa: Canadian Judicial Council, 2006) at 66, online: Canadian Judicial Council <http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_SecurityBlueprint_2006_en.pdf>.

19 *United States v Moussaoui*, 483 F (3d) 220 (4th Cir 2007) (available on WL Can) [*Moussaoui*].

more, they can subsequently engage in intimidating or even threatening behaviour, if not identity theft,[20] facilitated by said anonymity.

Not surprisingly perhaps, and as posited herein, applying the traditional standards of disclosure to the World Wide Web can and has produced unfortunate by-products ranging from identity theft to witnesses being threatened by external parties. These parties, by virtue of the medium if nothing else, now fall into a class of "interested parties" who enjoy access to the intimate details of participants in the judicial process.[21]

---

[20] See Canadian Judicial Council, *Model Policy for Access to Court Records in Canada*, (Ottawa: Judges Technology Advisory Committee, 2005), online: Canadian Judicial Council <http://ciaj-icaj.ca/english/publications/ModelPolicyAccess_CJC_Septe.pdf> [*Model Policy for Access*]. See also Rebecca Fairley Rainey, "The Jury is Out on Online Court Records", *Online Journalism Review* (25 January 2002) online: <http://www.ojr.org/ojr/law/1015015443.php>. Rainey refers to two policies issued by both the federal Judicial Conference and the California Judicial Council in which certain restrictions were placed on online posting of court records with a particular focus on limiting the personal information available in electronic versions of court records. According to Rainey, "The reasoning, in both policies, is that releasing records to a broad audience on the Internet would expose plaintiffs, defendants and jurors to the risk of identity theft through the publication of the extensive personal information collected in civil proceedings" (*ibid*).

[21] Apprehension of incidents of this very nature prompted Canada's Judges Technology Advisory Committee to issue a report entitled *Open Courts, Electronic Access to Court Records, and Privacy* ((Ottawa: Canadian Judicial Council, 2003), online: Canadian Judicial Council <http://cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_OpenCourts_20030904_en.pdf> [*Open Courts*]), which built upon an earlier report for the Administration of Justice Committee of the Council. This discussion paper assembled 33 conclusions including: that 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. See also Judges Technology Advisory Committee, *Use of Personal Information in Judgments and Recommended Protocol* (Ottawa: Canadian Judicial Council, 2005), online: Canadian Judicial Council <http://cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_UseProtocol_2005_en.pdf> [*Recommended Protocol*]. For a US perspective, see Peter A Winn, "Online Court Records: Balancing Judicial Accountability and Privacy in an Age of Electronic Information" (2004) 79:1 Wash L Rev 307. See also Lynn E Sudbeck, "Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence—An Analysis of State Court Electronic Access Policies and a Proposal for South Dakota Court Records" (2006) 51:1 SDL Rev 8; Natalie Gomez-Velez, "Internet Access to Court Records: Balancing Public Access and Privacy" (2005) 51:3 Loy L Rev 365; Andrew D Goldstein, "Sealing and Revealing: Rethinking the Rules Governing Public Access to Information Generated Through Litigation" (2006) 81:2 Chicago-Kent L Rev 375; Kristen M Blankley, "Are Public Records Too Public? Why Personally Identifying Information Should Be Removed from Both Online and Print Versions of Court Documents", Note, (2004) 65:2 Ohio St LJ 413.

Other jurisdictions such as France and its highest court (*la Cour de cassation*) have progressively favoured anonymization techniques, however partial: see the discussion of the l'Association des Hautes juridictions de cassation des pays ayant en partage l'usage du français, online: AHJUCAF <http://www.ahjucaf.org/spip.php?article6131>:

Whereas few but the most dedicated (or academically interested) individuals would take it upon themselves to conduct empirical research, the mere click of a button results in a *bilan* (taking stock) not only of decisions (previously available data) but of judges' and litigants' personal connections and associations. What is more, in contradistinction to an access to information request,[22] a search engine expedition can reap inaccurate if not misleading data—an aggregate of oft-unrelated and potentially unreliable morsels of information supposedly concerning the litigants or judge or both directly or indirectly.

With respect to judges in particular, activities or associations (such as membership in cultural or religious community) previously deemed perfectly acceptable at the very best, or innocuous, if not completely irrelevant, at the very least, now risk tainting the perception of impartiality; thereby further constricting the realm of "ethical" expression and association outside Chambers.[23]

Whereas the substantive nature of said activities and the rationale governing their tolerability has remained unchanged, the perception thereof may have. This, if only because "discrete" Internet postings (verified or false) may cumulatively serve to generate a generally unreliable, ad hoc "digital portrait" of the judge. Such data has become universally available with unprecedented ease. The Internet generally, and search engines specifically, make googling the judge a far less onerous—albeit no more dependable—activity, thus potentially giving rise to increased and presumably frivolous allegations of partiality.[24]

> *Si la jurisprudence disponible sur l'internet est progressivement anonymisée, conformément à la délibération de la Commission nationale de l'informatique et des libertés no 01-057 du 29 novembre 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence, les décisions accessibles sur l'intranet justice ne le sont pas* (*ibid* [footnotes omitted]).

So too has Belgium:

> *La publication sur internet est anonymisée (remplacement de l'identité des personnes physiques par des initiales* (*ibid* at "Belgique, Cour de cassasion").

Others such as Switzerland have yet to do so:

> *Actuellement, les décisions enregistrées dans la base de données ne sont pas anonymisées, mais figurent en texte intégral comprenant le rubrum (composition de la cour, nom du greffier, nom des parties notamment), l'état de fait, la motivation et le dispositif* (*ibid* at "Suisse, Tribunal fédéral").

22 *Access to Information Act*, RSC 1985, c A-1.

23 For a detailed discussion of the phenomenon of "googling" the judge, see Eltis, "Impact of New Technologies", *supra* note 6.

24 *Ibid*.

Not only is data purportedly pertaining to the judge's own expression and association "fair game" but also information relating to their family, colleagues, and former associates—not to speak of litigants. This information might also inadvertently be attached or be involuntarily or erroneously attributed to him.

What is more, a judge's impartiality can be brought into question for arguably improper motives[25] relating to her very identity such as gender, ethnicity, religious observance (or lack thereof), and sexual orientation—deemed "prohibited grounds" per section 15(1) of the *Charter*. Ill-intentioned individuals (from judge shoppers to prejudiced parties) can easily stage-manage Internet data to fashion the appearance of bias, using the judge's "core identity" against him. This may lead to claims discriminating against judges of certain backgrounds, the effect of which might be to exclude them from sitting, contrary to section 15(1) of the *Charter*.[26] Thus, in addition to further constricting judicial expression (whose narrowness is already decried),[27] technology may serve to reprimand a judge's very identity (gender, cultural, religious, or other)—in terms of either appointment or recusal—as cultural affiliations enter disputes in an increasingly multicultural society.[28]

Perhaps the most prominent illustration of the aforementioned (non-scholarly) "judicial profiling" is that of Justice Hazel Cosgrove, the first

---

[25] I.e., parties requesting attorneys of the same gender or cultural/religious, socio-economic background as themselves.

[26] I.e., in terms of appointment or recusal. For a general discussion of the former see Karen Eltis & Fabien Gélinas, "Judicial Independence and the Politics of Depoliticization" (2009), online Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1366242>.

[27] See John Sopinka, "Must a Judge be a Monk: Revisited" (1996) 45:1 UNBLJ Rev 167.

[28] For example, Lamer CJC, as he then was, was Catholic, and appears on Wikipedia (under current entry) as a Canadian Roman Catholic and member of the Roman Catholic Church: *Wikipedia, sub verbo* "Canadian Roman Catholics", online: <http://en.wikipedia.org/wiki/Category:Canadian_Roman_Catholics>. Consider the following:

> Lamer drew condemnation not only for supporting the striking down of Canada's abortion law in the pivotal 1988 *Morgentaler* case, but also for admitting afterward he did so on the basis of public opinion. "Had you asked me at a hearing if I was for or against (abortion), I would have said against," he said at the University of Toronto in 1998 ("Antonio Lamer 'liberated' Canada for Abortion", *Catholic Insight* 16:1 (January 2008) 29 at 30, online: <http://catholicinsight.com/online/church/biographies/article_776.shtml>).

Could his belonging to a church or his being Catholic, for that matter, constitute reason today for disqualification? An Internet search can also reveal whether a judge served in the military (Lamer CJC served as a member of the Royal Canadian Artillery and Intelligence Corps, and Dickson CJC, as he then was, served Canada in World War Two) with its own ramifications on the above-discussed).

female Supreme Court judge in Scotland, who stood accused of bias in a recent immigration case.[29] Charges that her Jewish background and membership in the International Association of Jewish Lawyers and Jurists[30] were raised as grounds for her disqualification from hearing a case involving the denial of asylum to a Palestinian refugee, Ms. Fatima Helow.[31] This claim was brought after Ms. Helow's attorneys googled the judge and found that she was a member of a Jewish professional association.[32] This information was used to attack the judge notwithstanding the fact that Ms. Helow did not claim that the judge's decision reflected any bias. While Justice Cosgrove was cleared of "lacking impartiality",[33] the mere incident stands as a warning to judges regarding the ready dissemination of personal and unrelated information over the Internet, its availability to litigants, and the potential for resulting frivolous claims or manipulation.[34]

---

29 *Helow v Scotland (AG),* [2007] CSIH 5 at para 16, [2007] SC 303 [*Helow*], aff'd [2008] UKHL 62, 2 All ER 1031 [*Helow (HL)*].

30 See generally, Michal Navoth, "IAJLJ Membership no Proof of Judge's Partiality" *Justice* 44 (Spring 2007) 46, online: The International Association of Jewish Lawyers and Jurists <http://www.intjewishlawyers.org/docenter/frames68af.html?id=16714>.

31 See Damien Henderson, "Judge Cleared of Jewish Bias" *The Herald [Scotland]* (17 January 2007) online: HeraldScotland <http://www.theherald.co.uk>: "Lady Cosgrove's impartiality when ruling on an immigration case of a Palestinian woman was compromised by being part of the International Association of Jewish Lawyers and Jurists." See also "Scottish Jewish Judge Cleared of Bias Charges" *JTA* (13 February 2007) online: Frost's Scottish Anatomy <http://www.martinfrost.ws/htmlfiles/scotnews07/070213_bias.html>; "Accusation of Judge's Bias Rejected: Lady Cosgrove Cleared of Partiality in Palestinian Asylum Seeker Case" *The Journal Online* (17 January 2007) online: Journal Online <http://www.journalonline.co.uk/news/1003819.aspx>:

> The Association's aims include the advancement of human rights, the prevention of war crimes, the punishment of war criminals and international cooperation based on the rule of law and the fair implementation of international covenants and conventions. It "is especially committed to issues that are on the agenda of the Jewish people, and works to combat racism, xenophobia, anti-Semitism, Holocaust denial and negation of the State of Israel."

32 *Hellow*, *supra* note 29 at para 16:

> Upon receiving intimation of the judge's decision, those representing the petitioner chose, for whatever reason, to make further inquiry about the judge. By means of the Internet search engine Google they discovered information about her which was (and is) publicly available on various websites. One such website was that of The International Association of Jewish Lawyers and Jurists ("the Association"), www.intjewishlawyers.org.

33 *Helow (HL)*, *supra* note 29.

34 The judge's ethnicity is well known because she is the first Jew appointed to the Supreme Court of Scotland.

In this manner, technology can be said to reawaken and indeed transform the recurring issue of the relevance of a judge's personal traits[35] and whether a party's explicit request for a "custom-made judge" might be legitimately entertained if not approved.[36] In other words, as the debate regarding "individualized justice" or the notion of incorporating cultural sensitivity and "cultural pluralism" into the law[37] gains momentum,[38] the enhanced capability to look up and indeed "recreate" a judge's (or judicial nominee's) identity online, is bound to enliven the issue of a party's entitlement to a judge tailored to their cultural specifications.[39]

---

35 See e.g. Madame Justice Bertha Wilson, "Will Women Judges Really Make a Difference?" (1990) 28:3 Osgoode Hall LJ 507; Peter McCormick & Twyla Job, "Do Women Judges Make a Difference? An Analysis by Appeal Court Data" (1993) 8:1 CJLS 135; Constance Backhouse, "The Chilly Climate for Women Judges: Reflections on the Backlash from the *Ewanchuk* case" (Paper delivered at the workshop "Adding Feminism to Law: The Contributions of Madame Justice L'Heureux-Dubé", Ottawa, September 2002), (2003) 15:1 CJWL 167. See also Justice Maryka Omatsu, "On Judicial Appointments: Does Gender Make a Difference?" in Joseph F Fletcher, ed, *Ideas in Action: Essays on Politics ands Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999) at 176 (also citing the work of Carol Gilligan regarding social context). For a US perspective, see Carol Gilligan, *In a Different Voice: Psychological Theory and Women's Development* (Cambridge, Mass: Harvard University Press, 1993); John Gruhl, Cassia Spohn & Susan Welch, "Women as Policymakers: The Case of Trial Judges" (1981) 25:2 American Journal of Political Science 311.

36 That is to say, one whose gender and ethnicity conform to the litigant's specifications or correspond to their own portrait. See also James Stribopoulos & Moin A Yahya, "Does a Judge's Party of Appointment or Gender Matter to Case Outcomes? An Empirical Study of the Court of Appeal for Ontario" (2007) 45:2 Osgoode Hall LJ 315; Cass R Sunstein, David Schkade & Lisa Michelle Ellman, "Ideological Voting on Federal Courts of Appeals: A Preliminary Investigation" (2004) 90:1 Va L Rev 301.

37 See Pascale Fournier, "The Ghettoisation of Difference in Canada: 'Rape by Culture' and the Danger of a 'Cultural Defence' in Criminal Law Trials" (2002) 29:1 Man LJ 81; Jennifer Choi, "The Viability of a 'Cultural Defence' in Canada" (2003) 8:1 Can Crim L Rev 93.

38 For the development of cultural defences, see *ibid*.

39 Composition of juries remains, of course, a contentious matter in the United States: See e.g. *JEB v Alabama*, 511 US 127, 114 S Ct 1419 (1994); *Georgia v McCollum*, 505 US 42, 112 S Ct 2348 (1992); *Powers v Ohio*, 499 US 400, 111 S Ct 1364 (1991); *Edmonson v Leesville Concrete Co,* 500 US 614, 111 S Ct 2077 (1991); *Batson v Kentucky*, 476 US 79, 106 S Ct 1712 (1986); *McCleskey v Kemp*, 478 US 1019, 107 S Ct 1756 (1986); *Norris v Alabama*, 294 US 587, 55 S Ct 579 (1935); *Carter v Texas*, 177 US 442, 20 S Ct 687 (1900); Warren Sheri Lynn Johnson, "Litigating Racial Fairness after *McCleskey v Kemp*" (2007) 39:1 Colum HRL Rev 178; Kenneth J Melilli, "*Batson* in Practice: What We Have Learned About *Batson* and Peremptory Challenges" (1996) 71:3 Notre Dame L Rev 447; Regina Graycar, "The Gender of Judgments: Some Reflections on 'Bias'" (1998) 32:1 UBC L Rev 1; Tanya E Coke, "Justice May be Blind but is she a Soul Sister? Race Neutrality and the Idea of Representative Juries", Note, (1994) 69:2 NYU L Rev 327 ("that the public believes that all-white juries put minority defendants and victims

II. Why Does Technology Matter? The Effect of Online Court Documents on Litigants and Non-Judicial Participants

By alluding to the *Moussaoui* case at the outset, this essay has already made reference to the distortions and potential ill-effects of unfettered access to mass Internet postings of court documents. These range from extreme threats of violence and harassment by both parties and "non-parties", to more "routine" incidents of employee cyberscreening, identity theft, fraud, and spam. Examples of the former and of the latter certainly abound.[40] Whereas the above-recounted incidents in the *Moussaoui* case were isolated and presumably spontaneous, the United States Department of Justice warns of an entire web-*industry*, organized and specifically dedicated to collecting information from Internet court dossiers, with an eye towards intimidation and retaliation.[41]

Consider the following (now relatively common) occurrence of witness bullying, enabled—or at the very least assisted—by electronic records, as Snyder recounts:

> Arrested for interstate drug trafficking in New Mexico, "Stewart" agreed to cooperate with authorities and testify against his co-defendants. The government filed Stewart's plea agreement with the court, and an electronic version became available for download to the Public Access to Court Electronic Records Service ("PACER") service. Shortly thereafter, Stewart's PACER files where featured on *whosarat.com*, a website that claims to have exposed the identities of more than 4,300 cooperating witnesses and undercover agents. In an effort to intimidate Stewart from testifying, his co-defendants plastered the *whosarat.com* materials, which labeled Stewart a "rat and a snitch," on utility poles and windshields in Stewart's neighborhood, and sent them by direct mail to residents in the area.[42]

In addition to the embarrassment it can generate, free-for-all admission to court records online significantly facilitates witness-litigant bullying, and may even nourish an intimidation industry. This is certainly not to suggest that litigants could not be embarrassed, or that witnesses could not be "reached" prior to the Internet age; it is merely that these pre-existing difficulties are exponentially worsened by the indiscriminate posting of court records online, due to the nature of the networked environment.[43]

---

at a disadvantage—is reason to worry about prevalence of non-representative trial juries" at 331).

40 See e.g. Winn, *supra* note 21.

41 See e.g. David L Snyder, "Nonparty Remote Electronic Access to Plea Agreements in the Second Circuit" (2008) 35:5 Fordham Urb LJ 1263.

42 *Ibid* at 1264 [footnotes omitted].

43 See the discussion on the differences between "paper and the Net", below.

Therefore, blanket filing, although aimed at enhancing accessibility, can in fact have the opposite effect online—*inadvertently deterring participation in the justice system*—thereby frustrating the very rationale underlying access. This unintended consequence arguably speaks to a phenomenon known as "translation", coined by Justin Hughes in a different context; or, the need to find "legal tools to reach roughly the same balance of interests in the Internet that we have developed for the rest of our world."[44] The Internet begs a sober rethinking of how we define access to court information in the Internet age, and of the current balance struck between this important value and privacy.

As Lyria Bennet Moses explains in her paper on the merits of revisiting norms in light of technological change, generally: "Existing rules were not formulated with new technologies in mind. Thus, some rules in their current form inappropriately include or exclude new forms of conduct."[45] For the purposes of our discussion, an approach to posting court documents that discounts the impact of the networked environment on justice participants' rights (primarily privacy and dignity) constitutes a far elevated—and perhaps at times intolerable— "transaction cost" for access to the courts and must therefore be reconsidered. Plainly put, courts may wish to reconsider the advantages and, indeed, the constitutionality of unbridled disclosure of records online when the rationale underlying the practice is "explicitly or implicitly based on a premise that no longer exists, and [is] thus no longer justified"[46] in light of technological change. The premise here being that blanket divulgation of data promotes access, and that privacy and transparency are countervailing in the cyber context.

I argue that, in this context, unrestrained disclosure can in fact disturbingly chill access to the courts. What is more, engaging in a decontextualized "balancing exercise" between privacy and access becomes no more than an artificial enterprise if these values are not clearly defined (as shall be argued in Part III)—or worse, if they are anachronistically conceived as adversarial—in a virtual world where privacy can no longer be spatially confined; and where "wholesale access" to data produces little meaningful information. As a result, "access" may no longer serve the rationales of openness and accountability and instead undermines the very entry to justice it was intended to foster.

---

44 Justin Hughes, "The Internet and the Persistence of Law" (2002-2003) 44:2 BCL Rev 359 at 360.

45 Discussing the scope of rules, see Lyria Bennett Moses, "Why Have a Theory of Law and Technological Change?" (2007) 8:2 Minn J L Sci & Tech 589 at 595.

46 *Ibid.*

A. Paper Versus Net

In order to situate privacy and access in the online context and point to how the current "balancing" fails to achieve its purpose in light of technological change, it is useful to first consider how court documents on the Web differ from their paper counterparts. Although it is not the objective of this paper to thoroughly set out all distinctions between "paper and the Net", it is nonetheless useful to highlight a few important differences.[47]

First, court documents are no longer protected by the "practical obscurity"[48] afforded by the paper records of years past. That translates into boundless, unprecedented, and unchecked distribution, with the ills commonly associated with most "good things" in unlimited and wholesale offering.

Most significantly, it increasingly involves a loss of court control over its own materials. That is to say that once unleashed online—however inadvertently—most of these files cannot be edited, effectively redacted, or recalled; often despite the court's wishes and best efforts to do so. No case better illustrates the erosion of judicial dominion or oversight over online documents then the following matter, which arose in Israel recently.[49]

Succinctly, a man who purposefully kept his sexual orientation secret sued an Internet dating site (dedicated exclusively to same-sex couples) for refusing to delete postings by a former lover who the plaintiff alleged had assumed his online pseudonym in order to reveal his true identity and spread falsities regarding his HIV status. Following the standard practice, the pleadings were automatically and instantaneously posted online by the court system, including the very same impugned damaging details regarding the plaintiff's orientation, sexual practices and health that prompted the suit. Although the judge did order the inflammatory details be promptly redacted from the decision at A's lawyer's request, immediately following publication, the first copy of the pleadings were left "floating" around cyberspace and could neither be tracked down nor effectively eliminated. Of course counsel's tardy realization that the statement of claim would be posted online in accordance with the court's standard practice was presumably at least partially to blame for the lamentable result. However, this phenomenon is quite common, as attorneys, not unlike judges, gradually awaken to the darker side of technology—certainly at a

---

47 For a discussion on the difference between paper records and electronic records, see Winn, *supra* note 21.

48 See *United States (Deptartment of Justice) v Reporters' Committee for Freedom of the Press*, 489 US 749 at 762, 780, 109 S Ct 1468 (1989).

49 *Doe v Doe* (4 January 2007) Tel Aviv 174875/06 (Magis Ct).

far slower pace than that at which documents can be electronically filed and distributed worldwide.

What is clear from this unfortunate matter is the courts' loss of control over its own materials, contrary to one of the foundational principles of accessibility; namely, that the court controls its documents, the idea that it "[h]as a supervisory and protecting power over its own records"[50] and that the "[a]uthoring judge, not publisher, is responsible for contents of judgment."[51] It is a state of affairs that presumably undermines judicial authority, creating absurd situations in which official anonymized versions of court files coexist alongside unedited copies, floating around cyberspace, readily available and featuring all of the personal details the court deemed inappropriate and sought to delete for the litigant's protection. Moreover, whereas judges take pains to draft judgments in restrained and respectful language, lawyers—not to mention self represented litigants—are hardly as careful in phrasing their statements of claim and motions. With electronic records and e-filing, these often inflammatory declarations can be propagated on the World Wide Web for all to see. As noted, even if later "withdrawn" the damage caused is irreparable.

As Winn cautions:

> The world of electronic information is a far less forgiving place ... the simple abstract rules developed for a world of paper-based information may no longer suffice to resolve complex problems of judicial information management. ... The failure of the legal system to maintain the ancient balance between access and privacy will lead to the greatest danger of all—inhibiting citizens from participating in the public judicial system.[52]

Somewhat less dramatically, but presumably no less disruptively, Internet postings have precipitated important difficulties in the commercial (particularly the trade-secret) context.[53] Such was the case, for example, with memoranda electronically filed by the United States Federal Trade Commission ("FTC") containing sensitive facts about Whole Foods Market

---

50 *Nova Scotia (AG) v MacIntyre*, [1982] 1 SCR 175 at 189, 132 DLR (3d) 385 [*MacIntyre*].

51 See Kate Welsh, "Court Records Access in Canada" (Presentation delivered at the 6th Conference on Privacy and Public Access to Court Records, Williamsburg, 6-7 November 2008) at 15, online: The Center for Legal and Court Technology <privacy.legaltechcenter.net/privacy/Privacy%20Documents/Court%20Records%20Access%20in%20Canada.ppt>, citing *Recommended Protocol*, *supra* note 21; *MacIntyre*, *supra* note 50.

52 Winn, *supra* note 21 at 328.

53 See e.g. Lisa C Wood & Marco J Quina, "The Perils of Electronic Filing and Transmission of Documents" (2002) 22:2 *Antitrust* 91.

Incorporated in a merger matter.[54] The Commission failed to properly redact sensitive and potentially damaging business plans, including plans to close a number of stores, prior to posting the documents online. By the time the oversight was detected, and despite the FTC's best efforts, it of course was too late.

While technical or clerical errors have occurred since time immemorial, and cannot be entirely avoided (nor is it suggested that their mere likelihood impede technological progress), the magnified harms that they can cause in the Internet context must be weighted—factored into the balance and into our understanding of access and privacy.

More importantly, access is a misleading term in the Internet age. The electronic court document debate should not simply be framed in terms of the public's "right" to arbitrarily hoard information en masse, irrespective of its accuracy or relevance. Instead, precision and preservation of the integrity of data is a tremendous issue here, as the Internet, in Cass Sunstein's words, "doesn't have quality control."[55] Plainly put, as data abounds, transparency (not to mention accountability) no longer relates to the ability to gather information per se—since erroneous, misleading, or simply meaningless data posted or collected indiscriminately can surely not be said to satisfy those values traditionally underlying access. Rather, it is about triage, about the quality and accuracy of the data available to us. Only a quality-centered approach can serve the goals of transparency and accountability so dear to democracy and the justice system. Not only does unbridled admission to data frustrate access to justice by litigants or others fearing humiliation or intimidation as described above, but it also risks creating the illusion of transparency or accuracy by inundating Internet surfers with a barrage of inaccurate if not dangerously misinforming data, thus frustrating the integrity of the justice system. Online disinformation can just as readily be fostered by too much "accessibility" as by the absence of worthy data.

In the words of Ejan Mackaay, "There is, if anything, an abundance of information; amongst the overload, the problem is how to select what information you need. This depends not merely on relevance but also on reliability or trustworthiness."[56] As the old adage cautions, a little information can be more dangerous than none, particularly in light of what

---

[54] *Ibid* at 91.

[55] Noam Cohen, "Courts Turn to Wikipedia, but Selectively" *The New York Times* (29 January 2007) online: <http://www.nytimes.com>.

[56] "What's so Special About Cyberspace—Reflections on Elkin-Koren and Salzberg", online: (2006) 10:3 *Lex Electronica* at 5 <http://www.lex-electronica.org/articles/v10-3/mackaay.htm>.

Daniel Solove labels the problem of "aggregation of data"[57] stemming from the Internet's "searchability". That is to say, previously *disparate* pieces of information concerning an individual floating in cyberspace can be assembled (incorrectly or even maliciously) to form a "comprehensive" digital profile of that person. Unlike an access to information request or paper record therefore, a search engine expedition can reap misleading but nevertheless persuasive data, an aggregate of unreliable yet compelling morsels concerning a given litigant, witness, or even judge—as the Cosgrove case illustrates. To paraphrase Solove, it is of a Kafkaesque rather than Orwellian privacy nightmare that we must be wary due to the cyberworld's fragmentary nature.[58]

It therefore stands to reason that a misguided insistence on unbridled access to court information and intransigence in its regard, not only fails to promote transparency in respect of quality, but also can paradoxically undermine many of the very objectives publication serves. Surely inhibiting participation cannot serve the rationale underlying systems promoting online posting, such as the US Public Access to Court Electronic Records system known as "PACER", whose stated objective was to bring "the citizen ever closer to the courthouse" via technology.[59]

What is more, distortions of court-generated information, floating around cyberspace and masquerading as "official" records can eventually risk bringing justice into disrepute. If a high court judge's reputation can be called into question (as in Justice Cosgrove's case), what can be said of precarious litigants or witnesses? It would therefore appear that an understanding of access divorced from considerations relating to the protection of litigants' rights (including privacy), is irreconcilable with transparency and accountability—failing to achieve its purpose in light of technological change[60]—and therefore must be reconsidered.

B. A Brief Aperçu of the Relevant Normative Framework

Notwithstanding the noteworthy differences between paper records and their newer, "electronic" counterparts, courts by and large continue to evaluate the effects of access with the application of a traditional balancing test. In the scales of justice "access" and the "presumption of open-

---

57 *The Digital Person: Technology and Privacy in the Information Age* (New York: New York University Press, 2004) at 149.

58 *Ibid* at 55.

59 See "Public Access to Court Documents: Better, Faster ... and Cheaper Than Ever Before" *The Third Branch* 33:4 (April 2001) 7 at 7, online: Administrative Office of the United States Courts <http://www.uscourts.gov/ttb/april01ttb/ctdoc.html>.

60 *MacIntyre, supra* note 50, and accompanying text.

ness", as traditionally understood, far outweigh privacy considerations[61]—as two recent reports on that point (one American, the other Canadian) confirm.[62]

While the objective here is not to thoroughly expose the applicable normative framework, it is nonetheless helpful to render a few of the fundamental principles. Seeking to comport with the imperatives of transparency (open court) and accountability, the starting point (in both the Canada and United States) is full access to court records. Not surprisingly then, litigants' privacy interests are normally insufficient to overcome that rule. In short, "[T]he public's right to transparent justice is an important constitutional rule and that it generally outweighs the equally fundamental right to privacy."[63] Accordingly, the "presumption of openness" may only be refuted in very limited circumstances, primarily (but not limited to) young offenders, family matters, the protection of innocent third parties, interim publication bans, and in some cases confidential commercial information.[64]

---

61 For instance, the Supreme Court of Canada identified a strong presumption in favour of publicity and openness; that said, the presumption in question can be rebutted for valid reasons such as the need to protect innocent third parties (*ibid*).

62 See *Open Courts*, *supra* note 21. The paper established "that 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" (*ibid* at 2). In the United States, Martha Steketee & Alan Carlson prepared a report for the National Center for State Courts and the Justice Management Institute basing their guidelines on certain premises, including, "the traditional policy that court records are presumptively open to public access": National Center for State Courts, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts* by Martha Wade Steketee & Alan Carlson (State Justice Institute, 2002) at 1, online: National Center for State Courts <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/tech&CISOPTR=105>.

63 Darrel Pink et al, "Session 5 Panel: Access to Judgments" (Abstract of presentation delivered at the 8th International Conference Law Via the Internet, Lexum, Montreal, 26 October 2007) online: <http://web.archive.org/web/20080622181552/conf.lexum.umontreal.ca/en/proceedings.php >, citing *Model Policy for Access, supra* note 20.

64 See Right Honourable Beverley McLachlin, "Courts, Transparency and Public Confidence: To the Better Administration of Justice" (2003) 8:1 Deakin Law Review 1 at 3-6. See also the *Dagenais/Mentuck* test for refuting the open court principle: *Dagenais v Canadian Broadcasting Corp,* [1994] 3 SCR 835, 120 DLR (4th) 12 [*Dagenais*]; *R v Mentuck*, 2001 SCC 76, [2001] 3 SCR 442, cited in McLachlin, *supra* at 5. The *Dagenais/Mentuck* test was originally developed in the context of publication bans; however, it was expanded in Re *Vancouver Sun* (2004 SCC 43, [2004] 2 SCR 332 [*Vancouver Sun*]) to include application to "all discretionary actions by a trial judge to limit freedom of expression by the press during judicial proceedings" (*ibid* at para 31). The test as cited in *Vancouver Sun* reads as follows:

At this juncture, it bears repeating that our objective is not to dispute the paramountcy of "transparent justice", open court or accessibility, but rather, to take issue with a decontextualized construction of these concepts in the cyber context; particularly vis-à-vis the court's duty to maintain control over its documents, and to protect the rights (including the right to privacy) of participants in the justice process.

The Canadian Judicial Council ("CJC") and its American counterpart have—to their credit—recognized that the Internet impact disclosure and have addressed the issue in recent publications.[65] They predominantly maintain and import the traditional paper "presumption of openness" to the Internet context subject to a number of exceptions.[66] For example, the CJC report, for its part, does laudably recommend excluding personal data identifiers and certain personal information unless required for the disposition of the case in order to accommodate privacy interests.[67]

Unfortunately these redactions often come too late, since, according to the *Model Policy for Access*,[68] parties, who are themselves responsible for documents in the file, are not aware to ask for anonymization early enough in the process. Moreover, it is important to note that redactions of "personal identifiers" are often insufficient online, either due to context (i.e., in the case of a small town where one can easily be identified by background or circumstantial information alone) or as a result of the inefficiency of the redaction software.[69]

> (a) such an order is necessary in order to prevent a serious risk to the proper administration of justice because reasonably alternative measures will not prevent the risk; and
>
> (b) the salutary effects of the publication ban outweigh the deleterious effects on the rights and interests of the parties and the public, including the effects on the right to free expression, the right of the accused to a fair and public trial, and the efficacy of the administration of justice (*ibid* at para 32).

65 See also *Model Policy for Access, supra* note 20; *Recommended Protocol, supra* note 21.

66 *Open Courts, supra* note 21; The US rule indicated in Steketee & Carlsonis to "[r]etain the traditional policy that court records are presumptively open to public access"(*supra* note 62).

67 See *Open Courts, supra* note 21 at para 119. Other exemptions include common statutory protections.

68 *Supr*a note 20 (judges are responsible for judgments).

69 In 2002 a Virginia resident created a "watchdog" website drawing attention to the online availability of personal information by publicizing the personal information obtained online of celebrities including Jeb Bush, Kelly Ripa and others. The creation of the website was in response to her discovery that her local circuit court clerk was about to place her mortgage documents online: see Andy Opsahl, "Privacy: Agencies Struggle to Redact Personal Data from Online Public Documents" *Government Technology* (8 July 2008), online: Government Technology <http://www.govtech.com/gt/375540>.

Far more importantly, the problem lies neither in the normative framework itself nor in the anonymization method, which can be improved.[70] Instead, there is a deeper underlying change needed—one to our understanding of privacy, and its relationship to access to justice and the exercise of judicial discretion.

Courts are held to protect the "discretionary privacy rights" of participants in the justice process even when that duty clashes with accessibility. They have broad powers to do so, including in cases "where the ends of justice may be subverted by disclosure or the information might be used for an improper purpose."[71] Nevertheless, individual judges remain reticent to exercise this discretion and protect litigants' privacy interests. This is presumably—at least in part—due to a culturally narrow understanding of privacy coupled with a perceived dichotomy between privacy and access, resulting in increasingly challenging and problematic situations.

Take, for instance, the *Al Telbani* case [72]. Mr. Al Telbani, a graduate student at Concordia University, was placed on Canada's no-fly list and brought a lawsuit against the Canadian government. Although Transport Canada denied him access to evidence supporting their claim that he is an "immediate threat to aviation security",[73] Mr. Al Telbani's personal information was published for all to see, as per the "open court principle", notwithstanding his request for anonymization.

Regardless of the outcome or merits of the pending case, it seems somewhat incongruous that a party to the case, Mr. Al Telbani himself, has thus far been denied seemingly necessary access to information that

---

70 Regarding pseudonyms and anonymization, see Carole Lucock & Michael Yeo, "Naming Names: The Pseudonym in the Name of the Law" (2006) 3:1 University of Ottawa Law & Technology Journal 53. Courts commonly employ pseudonyms in an effort to camouflage litigants' identities in family law matters in particular. Needless to say, however, this practice is only relevant if and when certain standards generally related to proportionality (benefits outweighing prejudicial effects) are met. See *BB c Québec (PG)*, [1998] RJQ 317 (available on WL Can) (CA). The Quebec Court of Appeal followed the two-pronged test established in *Dagenais* (*supra* note 64). These steps are as follows: first, to consider whether a publication ban is necessary to avoid a compelling risk that a trial would be inequitable; and second, to consider whether the beneficial effects of the ban would outweigh the prejudicial effects on the free expression of those who would be affected by the ban.

71 *Recommended Protocol, supra* note 21 at para 31, cited in Lucock & Yeo, *supra* note 70 at 73.

72 *Al Telbani c Canada (PG)*, 2008 CF 1318 (available on CanLII).

73 Micheal Friscolanti & Martin Patriquin, "Why Can't this Man Fly? A Judge Releases the Identity of Canada's First No-Fly Suspect", *Maclean's* (17 September 2008) online: Macleans.ca <http://www.macleans.ca>.

would permit him to refute the allegations levied against him; whereas strangers to the case—anyone for that matter—can, with the click of a button, retrieve data intimate to the plaintiff.[74]

Another case that stands out involves a Quebec woman infected with a sexually transmitted disease by a partner who allegedly lied or at the very best failed to reveal his carrier status.[75] The infected woman sued for damages in civil liability (tort). Due to the disturbing and humiliating nature of the sexual and medical details involved, the plaintiff asked the court to exercise its discretion to redact such information. She was denied on the grounds that it was not a family law but a private law (civil liability) matter and therefore not sufficiently "exceptional" to justify a publication ban (even though the plaintiff was not requesting a ban but merely de-identification).[76] It is worth mentioning that the facts were so egregious that SOQUIJ and other online databases voluntarily agreed to redact, even though they were at liberty to publish. Of course, as noted above, once one copy is released the "propagation problem" results in the coexistence of anonymized documents alongside unredacted versions. It is also noteworthy that just as in the Israeli case, the de-identification request was made late in the process; and, as has been previously seen, once the information is made available in cyberspace redaction is a virtual impossibility with control out of the hands of the courts.

When pitted *against* the open court principle, protecting litigants from consequences such as humiliation, embarrassment, or shame are looked upon with suspicion. This is again evident in various cases including the more egregious one of *X v. Société Canadienne de la Croix-Rouge*[77], where the court refused to permit a hemophiliac, infected with HIV, to use a pseudonym on the ground that to do so would "adopt a retrograde attitude toward [the] disease."[78]

---

74 Parliament, Standing *Committee on Access to Information, Privacy and Ethics*, 40th Parl, 2d Sess, No 004 (23 February 2009), online: Parliament of Canada <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=3687973&Language=E&Mode=1&Parl=40&Ses=2>. Mr Al Telbani based his claims against the Federal government on a violation of his *Charter* protected rights to privacy, due process, and free movement. See Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Supplementary Submissions to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182* (Ottawa, 2008), online: Commission of Inquiry <http://www.majorcomm.ca/en/submissions/Lata%20Pada%20-%20Supplementary%20Submissions%20re%20New%20Evidence.pdf>.

75 *JL c AN*, 2007 QCCS 3226, [2007] RJQ 1998 (Sup Ct) [*JL*].

76 *Ibid*.

77 (1992) 101 DLR (4th) 124, [1992] RJQ 2735 (CA) [cited to DLR].

78 *Ibid* at 128. See also Nathalie Des Rosiers & Louise Langevin, *Representing Victims of Sexual and Spousal Abuse* (Toronto: Irwin Law, 2002). Des Rosiers & Langevin are of

III. Rethinking Privacy, Access, and their Relationship to One Another

To what, then, might this reticence be attributed? As already noted, the answer may—at least in part—lie in our legal traditions' very understanding of privacy. The following argues that aside from being plagued by problems of clarity (as Solove has eloquently argued),[79] the concept of privacy appears to lend itself to two distinct socio-juridical narratives: the first associated with the common law view and the second with its continental (or civil law) counterpart. Accordingly—and since privacy is undoubtedly "a highly mutable concept, both historically and culturally relative"[80]—comparative inquiry can expose what may be labelled a knee-jerk "balancing" of ill-defined values that no longer serves the intended rationale.

More specifically, in the common law tradition (which predominates in the United States and Canada), an individual's right to privacy is generally assessed by reference to society's conception of the measure of privacy that one is entitled to reasonably expect. That standard is particularly awkward with said expectations rapidly eroding, ironically due to social habituation to recurring intrusions.[81] More importantly perhaps, in contradistinction to its civilian counterpart, the common law tradition seems to place great emphasis on the *territorial* aspect of privacy, that is to say special "seclusion" or "aloneness" (in American parlance, "the right to be left alone"). In consequence, it is said that the Anglo-American tradition "carve[s] out space where law may intrude, and not further" (a so called privacy zone).[82] Focusing narrowly on territorial or proprietary notions of

---

the opinion that "fear of taboos is sufficient grounds for ordering that the parties' identities be protected, whether it concerns AIDS victims or sexual abuse. The plaintiffs should not have to pay the price for changing society's attitudes" (*ibid* at 275, cited in Lucock & Yeo, *supra* note 70).

79 Solove, *Understanding Privacy*, *supra* note 1.

80 David Lyon, "Surveillance, Power, and Everyday Life" in Robin Mansell et al, eds, *The Oxford Handbook of Information and Communication Technologies* (Oxford: Oxford University Press, 2007) 449 at 459.

81 See Karen Eltis, "Can the Reasonable Person Still Be 'Highly Offended'? An Invitation to Consider the Civil Law Tradition's Personality-Rights Based Approach to Tort Privacy" University of Ottawa Law & Technology Journal [forthcoming], online: Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1304653> [Eltis, "'Highly Offended?'"].

82 Daniel Pollack, "Preface" in Daniel Pollack, ed, *Contrasts in American and Jewish Law* (Hoboken, NJ: Yeshiva University Press, 2001), online: Jewish Law Commentary <http://www.jlaw.com/Commentary/contrasts.html>. See Adrien Popovici, "Le Rôle de la Cour Suprême en Droit Civil" (2000) 34 RJT 607 at 618 [Popovici, "Rôle de la Cour Suprême"], citing W Page Keeton et al, eds, *Prosser and Keeton on the Law of Torts,* 5th ed (St Paul, Minn: West, 1984) at 866-67; Laurence H Tribe, *American Constitutional Law*, 2d ed (Mineola, NY: Foundation, 1988) at 775:

"seclusion" or both, as I have shown elsewhere,[83] derives from historically entrenched property-based reasoning that lamentably fails to capture the complexity of the privacy value in modern times and is therefore ill-suited to the cyber context.

Thus, North American scholars tend to embark on discussions of privacy with the origins of the invasion of privacy tort, born of a seminal article titled "The Right to Privacy".[84] Though seldom addressed, the historical roots of that right in common-law England are particularly instructive. Under the English common law, the right to privacy was first recognized by virtue of its intricate link to personal property. This is best evidenced by the now infamous saying, "[T]he house of every one is his castle," first coined by the House of Lords in *Semayne's Case* (now colloquially known as "a man's home is his castle").[85] This alluded to the conception that a person's right to privacy fundamentally derives from his property rights.[86] In view of that, the right to privacy was initially recognized in relation to trespass,[87] thus confirming what was, for many years, the reigning conception of privacy as rooted in ownership.[88] This brief historical aperçu at the very least elucidates the understanding of privacy as the right to be left alone in given spaces, defined externally rather than inherently to personhood.[89]

> *En droit canadien, « privacy » comprend non seulement les intrusions et divulgations violant l'intimité de chacun, mais englobe « une sphère irréductible d'autonomie personnelle où les individus peuvent prendre des décisions intrinsèquement privées sans intervention de l'État ». C'est la conception américaine de* Griswold c. Connecticut *(1965), dans un système où l'on ne connaît pas les droits de la personnalité.*

83 Eltis, "'Highly Offended?'", *supra* note 81.

84 Samuel D Warren & Louis D Brandeis, "The Right to Privacy" (1890) 4:5 Harvard Law Review 193.

85 (1604), 5 Co Rep 91a, Mich 2 Jac 1, 77 ER 194.

86 See Warren Freedman, *The Right to Privacy* (New York: Quorum Books, 1987). Freedman discusses the 1818 English case, *Gee v Pritchard* ((1818), 2 Swans 402, 36 ER 670) where the Court of Chancery restricted the publication of a personal letter "to protect a 'property right'" (*ibid* at 3). Freedman discusses other English cases where courts "based their protection of the right of privacy upon the protection of a 'property right'" (*ibid*).

87 See William L Prosser, "Privacy" (1960) 48:3 Cal L Rev 383 at 389-90; Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 311, 333).

88 See Karen Eltis, "Privacy in the Workplace", *supra* note 9 at 519.

89 See Morton J Horwitz, *The Transformation of American Law, 1780–1860* (Cambridge, Mass: Harvard University Press, 1977) at 31. Horwitz observed how the conception of property changed from the eighteenth-century view that dominion over land conferred the power to prevent others' interference, to the nineteenth-century assumption that

The tendency to associate privacy with property and aloneness may not lend itself as well beyond the "physical" world (i.e., in cyberspace). Bearing more directly on the online "privacy versus accessibility" debate, this narrow, spatially-based construction might—at least in part—be responsible for judicial reticence to attach greater weight to privacy in the cyber context, particularly when it appears prima facie to compromise the rightly-cherished but ill-defined value of access.[90]

What role might the notion of seclusion play when, to quote the Supreme Court of Canada in *R v. Wise*, "many, if not the majority, of our activities are inevitably carried out in the plain view of other persons"?[91] The view taken by civilian jurisdictions in this vein is particularly enlightening. In sharp contrast to what might be characterized as the common law's libertarian—oftentimes rigid—vision of privacy, the civilian legal method, captivated by the French experience, favours a more flexible construction of actionable privacy infringements. Most importantly perhaps, privacy is considered to be a "personality right"—an idea central to the civilian tradition but alien to the common law. What that means succinctly is that privacy attaches to persons rather than property, irrespective of property or special constraints. In other words, "Personality rights focus on the *être*—the being—in contrast with the *avoir*—the having"[92] and are therefore divorced from territory. Central among these personality rights is privacy, which in turn is predicated on dignity.[93]

---

the essential attribute of property ownership was the power to develop it irrespective of the consequences to others.

90 The argument framed in terms of quality versus quantity of available information is found above at 23-25. See also Eltis, " 'Highly Offended?'", *supra note* 81.

91 [1992] 1 SCR 527 at 564-65, 70 CCC (3d) 193.

92 Adrian Popovici, *Personality Rights: A Civil Law Concept* (2004) 50:2 Loy L Rev 349 at 352, citing Alain Seriaux, "La notion juridique de patrimoine: Brèves notations civilistes sur le verbe avoir" (1994) 93:4 RTD Civ 801 at 804-806. Personality rights are also known as "droits primordiaux" by reason of their importance: see France Allard, "Les Droits de la Personalité" in Josée Payette, ed, *Personne, famille et successions*, vol 3 (Cowansville: Yvon-Blais, 2003) 61 at 61. Allard observes that these rights generally do not have any inherent monetary-pecuniary value, as they are inherent to personhood. According to Geoffrey Samuel, "for better or for worse, the concept of '*le droit subjectif*' [subjective rights such as personality rights] has little relevance in English Law": Geoffrey Samuel, "'Le droit subjectif' and English Law" (1987) 46:2 Cambridge LJ 264 at 286. Personality rights have become increasingly important in Quebec law, as Laverne Jacobs remarks: "Quebec Civil law ... over the past three decades, has increasingly placed central emphasis on the person and personality rights": Laverne A Jacobs, "Integrity, Dignity and the *Act Respecting Industrial Accidents and Occupational Diseases*: Can the Act Provide More Appropriate Compensation for Sexual Harassment Victims?" (2000) 30:2 RDUS 279 at 316.

93 Drawing on Popovici, Eltis writes, "*Le droit civil québécois demeure fidèle à la tradition civiliste, qui elle privilégie la notion de droits* subjectifs *inaliénables. Ces droits de*

Conceiving the right to privacy as a personality right predicated on dignity and free of territorial constraints allows the civilian legal method to grasp privacy as a zone of intimacy delineated not by space or ownership but by the basic needs of personhood. Instead of deriving from property or being akin to seclusion, the civilian notion of privacy relates to moral autonomy and as such is encompassed by human dignity, which inheres in legal personality and is considered an extension thereof.[94]

The civil law tradition's construction of privacy rights has been broad. Removed from the "reasonable expectations" doctrine, civilian jurisdictions' principled approach to civil liability is better able to protect individual privacy[95] in intangible spaces (such as cyberspace), regarding certain dignity-based personality rights as inalienable. As previously noted, human beings enjoy personality rights including, but not limited to, privacy by reason of their very personhood, regardless of express statutory or jurisprudential intervention, spatial, or proprietary constraints. This is of great interest on point as a flexible interpretation lends itself to the protection of privacy in an era of constant technological and social change. Moreover, the dignity-based conception seems to better comport with Charles Fried's relational understanding of privacy as "inherent to the notions of respect, love, friendship, and trust, and that close human relationships are only possible if persons enjoy and accord to each other a cer-

---

personnalité intangibles ne sauraient être assimilés aux droits propriétaires, car ils découlent de la personnalité juridique du détenteur" ("La surveillance du courrier électronique", *supra* note 9 at 495 [emphasis added, footnotes omitted], citing Popovici, "Rôle de la Cour Suprême", *supra* note 82 at 615). Gregoire Loiseau also drew on Popovici: "l'idée d'une protection de la personnalité humaine s'enracine et prend corps sous la forme de droits subjectifs" ("Des droits patrimoniaux de la personnalité en droit français" (1997) 42:2 McGill LJ 319 at 328, citing Popovici, "Rôle de la Cour Suprême" *supra* note 82 at 616).

94 *C.f.* Eric H Reiter, "Personality and Patrimony: Comparative Perspectives on the Right to One's Image" (2002) 76:3 Tul L Rev 673 at 677. See also James Q Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113:6 Yale LJ 1151 at 1161-62.

95 See Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, NY: Cornell University Press, 1992). Bennett discusses how enforcement of principles of privacy law varies considerably and is a function of culture. See also Jon Bing, *A Comparative Outline of Privacy Legislation*, 2 Comparative Law Yearbook of International Business 149-81. See also Steven Bellman et al, "Regional Differences in Privacy Preferences: Implications for the Globalization of Electronic Commerce" (2002) [unpublished, archived at Columbia University Graduate School of Business).

tain measure of privacy,"[96] than does an understanding clinging to the notion of isolation or seclusion.

As such, and for purposes of the discussion respecting paperless records, privacy may be construed as an *ally* of accessibility rather than adversative to it. It can therefore be more easily reconciled with both the court's commitment to openness and with its responsibility to protect litigants and control its own records.

In other words, courts might construe safeguarding privacy as a means of encouraging participation in the justice system in an age when so doing exposes individuals to countless risks associated with internet access to their personal information. Additionally, it may be seen as a way of enabling courts to maintain essential control over their own materials. Consequently, it is not merely that the balance between transparency and privacy has tremendously shifted online[97]—it may be that safeguarding privacy can become a way towards ensuring access to justice and willingness to participate in light of the challenges of the Internet age.

Conclusion: Privacy as an Ally of Access

We are no longer dealing with an irreducible conflict between hopelessly opposed entities (privacy and accessibility) or pointed juxtapositions with no interactions between them. Instead, the duty to protect privacy can and must be construed as part of courts responsibility to maintain access to justice and prevent disinformation.[98]

Privacy is no longer about the right to be left alone. Instead, in this web-dependent age, privacy in the electronic court records context might ultimately be *about* the very access to justice we seek to protect. As already alluded to above, unbridled postings create the illusion of "access". While third parties unrelated to the proceedings can easily collect the most intimate details concerning the litigants, witnesses, and others, participants are left unprotected; notwithstanding the court's duty towards them. Not surprisingly then, sacrificing participants' right to dignity and privacy in the justice process for the illusion of transparency, coupled with a significant loss of judicial control over how and what information is disseminated online, eventually risks fostering a disinclination to participate

---

96 "Privacy" (1968) 77:3 Yale LJ 475 (privacy is linked to respect, love, friendship and trust, and is the "oxygen" by which individuals are capable of building "relations of the most fundamental sort" at 477-78).

97 Winn, *supra* note 21.

98 In Canada, see *Open Courts*, *supra* note 21. In the United States, see Steketee & Carlson, *supra* note 62.

in the justice process. Thus, paradoxically, the very access to justice paperless records were meant to enhance, is undermined.

Perhaps the above-cited Quebec case, *JL*, best illustrates the point.[99] 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.

In light of this difficulty, this article has exposed a distinction between the civilian and common law views of privacy in the hopes that comparative inquiry can inform the "paperless records" debate. As noted, the broader, dignity-based civilian construction enables us to reframe the debate between accessibility and privacy in the Internet context.

If privacy is more broadly understood as deriving from human dignity then it can be viewed as a facilitator rather than detractor of accessibility and comport with the court's various duties (to foster transparency *and* to protect litigants and control its documents). In other words, judges would presumably be more inclined to use their discretion to protect litigants' (and other participants') privacy if doing so would not be regarded as sacrificing openness or transparency but rather as a facilitator of access and enabler of court control over its records. Those litigants and witnesses who are confident that their personal information will not be indiscriminately exposed, surely have greater incentive to participate in the justice system than those dreading humiliation, intimidation, or retribution that not even the court itself can manage.

---

[99] *Supra* note 75.