Best Practices in the Field of Cyberjustice

by

Nicolas W. VERMEYS[1] and Karim BENYEKHLEF[2]

Introduction

For decades, if not centuries[3], governments have sought new ways to solve to age-old problem of access to the courts. Indeed, costs and delays have long plagued most legal systems[4], making it increasingly difficult for individuals to have their "day in court". Although numerous legislative changes have been made to address this problem, they seem to have had little to no impact on the overall issue[5]. Today, with the advent of what is often referred to as the "technological revolution"[6], that is to say the birth of the microprocessor and all that followed[7], many have wondered if IT couldn't succeed where legislation has failed, i.e. if bringing new and innovative technologies into the courtroom could possibly make the judicial process more efficient and,

---

[1] Professor at the *Université de Montréal*'s *Faculté de droit*, Associate Director of the *Cyberjustice Laboratory*.

[2] Professor at the *Université de Montréal*'s *Faculté de droit*, Director of the *Centre de recherche en droit public* and of the *Cyberjustice Laboratory*.

[3] See Jacques Krynen, *L'empire du roi*, Paris, Gallimard, 1993, p. 267.

[4] *Id*. See also Raymond BORDEAUX, *Mémoire sur la réformation de la justice*, Évreux, Imprimerie de Auguste Hérissey, 1857, pp. 229-230.

[5] See, for example, Mélanie BEAUDOIN, "Réforme du *Code de procédure civile* : Pour une amélioration de la justice", (2008) 40-1 *J. du Bar*. 7.

[6] See Roger Brownsword, *Rights, Regulation, and the Technological Revolution*, Oxford, Oxford University Press, 2008, p. 2 and ss.

[7] See Gordon E. MOORE, "The Microprocessor: engine of the technology revolution", (1997) 40(2) *Communications of the ACM* 112.

therefore, less costly. This relatively recent notion has spawned a series of new technology-driven procedural models or "cyberjustice" [8].

The term "cyberjustice" refers to the integration of information and communication technologies to dispute resolution processes, whether they be judicial or extrajudicial. In its broadest sense, cyberjustice implies the networking of all stakeholders in the informational chain for judicial cases. This is what is commonly known as an *integrated justice system*[9]. But, at its basic core, cyberjustice is simply the use of technology for procedural and evidentiary purposes.

That being said, a shift to a more technologically advanced court system, like any other fundamental change in how legal processes are viewed and conducted, is a complex issue that necessitates careful planning. As demonstrated by the failure of both Ontario's *Integrated Justice Project*[10] and Holland's *HBS Project*[11], moving towards cyberjustice is not as easy as buying the necessary hardware and software. Numerous factors, often having little to do with technology, need to be taken into account. The current paper aims to shed some light on these factors by establishing some basic "best practices" in the field of cyberjustice, that is to say a series of important steps that those in charge of enacting technological change need to take to ensure that their system doesn't become just another failed experiment[12]:

- Be aware of the impacts of technological changes on human behaviour;
- Be aware of the impacts of technological changes on legal rituals and practices;
- Identify the true impacts of technological changes on processes;
- Use an incremental or modular approach to technological change;
- Be aware of the possible implications of outsourcing;
- Identify possible compatibility issues with existing technology and practices;
- Identify factual needs, not theoretical wants;
- Use a collaborative approach;

---

[8] See, for example, Karim BENYEKHLEF and Fabien GÉLINAS, "Online Dispute Resolution", (2005) 10(2) *Lex Electronica*, p. 6, http://www.lex-electronica.org/articles/v10-2/Benyekhlef_Gelinas.pdf.

[9] According to the National Criminal Justice Association, "The term "integrated justice systems" encompasses *interagency*, *interdisciplinary*, and *intergovernmental* in- formation systems that access, collect, use, and disseminate critical information at key decision points throughout the justice process, including building or enhancing capacities to automatically query regional statewide and national databases and to report key transactions regarding people and cases to local, regional, statewide, and nation- al systems. Generally, the term is employed in describing justice information systems that eliminate duplicate data entry, provide access to information that is not otherwise available, and ensure the timely sharing of critical in- formation." See National Criminal Justice Association, *Justice Information Privacy Guidelines--Developing, Drafting and Assessing Privacy Policy for Justice Information Systems* (2002), p. 16. For more on integrated justice systems, see Karim BENYEKHLEF, "Integrated Justice Information Systems in Canada and the United States", in Georges CHATILLON and Bertrand du MARAIS (dir.), eGovernment for the Benefit of Citizens, Bruxelles, Bruylant, 2004, 183.

[10] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1. See also Carl BAAR, "Integrated Justice: Privatizing the Fundamentals", (1999) 42 *Canadian Public Administration* 42.

[11] See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 62 and ss.

[12] According to a report for the Dutch Parliament by the General Accounting Chamber, more than 50% of cyberjustice projects fail in whole or in part. See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 61.

- Identify all costs, not simply acquisition costs;
- Don't just reproduce: Innovate.

It must be pointed out that this list is the result of over 15 years of research in the field of cyberjustice by *Centre de recherche en droit public* (CRDP) researchers and their teams. It's also at the very heart of the work that is currently being done within the Cyberjustice Laboratory[13], a research infrastructure housed at the University of Montreal and operated in collaboration with McGill University. Through research stemming from both techno-legal and socio-legal standpoints, Cyberjustice Laboratory researchers hope to identify and overcome the numerous obstacles to the modernization of our legal system.

1. Be aware of the impacts of technological changes on human behaviour

In "The Whale and the Reactor", Langdon Winner explains that "[a]s technologies are being built and put to use, significant alterations in patterns of human activity and human institutions are already taking place."[14] The author goes on to state that "we usually do not stop to inquire whether a given device might have been designed and built in such a way that it produces a set of consequences logically and temporally *prior to any of its professed uses*"[15]. To illustrate this concept, professor Winner gives the example of master builder Robert Moses, who planned most of the roadways built in New York during the XXth century. Moses' designs were somewhat particular in that the height of most of his overpasses did not abide by national standards. As the story goes, this was done to ensure that those who used public transport (i.e. the poor) couldn't have access to certain areas of town such as the parks and beaches since busses were simply too high to pass under most overpasses. Moses and his rich friends could therefore enjoy these areas of town without having to suffer the less fortunate…

The obvious lesson to be learned from this egregious anecdote is that there is currently a digital divide in most societies[16], and that certain cyberjustice technologies such as efiling could make it difficult for those who are not computer literate, or don't have access to computers or broadband networks, to have access to the courts, making the problem worse, not better[17].

But there is also a second more important lesson that one must take from the Moses story, and that is that technology is not neutral and should not be thought of as such. As one author puts it:

> "Each technology has properties - affordances - that make it easier to do some activities, harder to do others. The easier ones get done, the harder ones neglected. Each has constraints, preconditions, and side effects that impose requirements and

[13] See: http://www.cyberjusticelaboratory.org.

[14] Langdon WINNER, *The Whale and the Reactor*, University of Chicago Press, Chicago, 1986, p. 11.

[15] Langdon WINNER, *The Whale and the Reactor*, University of Chicago Press, Chicago, 1986, p. 25.

[16] See: http://clinton4.nara.gov/WH/New/digitaldivide/digital3.html.

[17] See Mary Alice Robbins, "Plaintiff Sues Over Court Requiring LexisNexis for E-Filing", (2010) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202448233917&slreturn=1&hbxlogin=1.

> changes on the things with which it interacts, be they other technology, people, or human society at large."[18]

To quote Joel Reidenberg, "[t]echnological capabilities and system design choices impose rules on participants"[19], that is to say that, by digitalizing the legal process, by moving from a paper medium to an electronic medium, we are in fact changing more that the medium, we're changing habits. Digital technology, like Moses' overpasses, will dictate what we can and cannot do. If a field on an electronic form can only hold 10 characters, we cannot simply write in smaller letters like we would for a paper form, we have to limit ourselves to 10 characters.

Of course, this isn't the first time the legal system is faced with such a shift in its processes. In the XVIth century, the printing press had a similar impact on our behaviour:

> "In the early days of printing […] some influential institutions […] assumed that printing was merely a powerful replacement for writing. These institutions failed to understand, however, that printing could not be controlled as easily as writing had been, and they did not recognize that printing also changed the larger environment."[20]

Like with the printing press, it will take much time for us to adapt to information technologies[21], but that is not to say that we shouldn't evolve, simply that we must carefully study how a given cyberjustice solution will cause our habits to change and if those changes are beneficial to the process and to its stakeholders.

2. Be aware of the impacts of technological changes on legal rituals and practices

Over the centuries, the legal community has incorporated a series of rituals and symbols into its practices[22]. It could even be argued that the judicial system is one of the most ritualized processes in modern society[23]. Some of these rituals serve an obvious purpose and are often intrinsically linked to some of the pillars of our legal systems (right to face one's accuser, right to be heard by an independent and impartial tribunal, right to a public trial, etc.), while others are simply the product of superstitions or dogmas from a bygone era. It is therefore imperative, before

---

[18] Donald A. NORMAN, *Things That Make Us Smart*, Reading, Addison-Wesley, 1993, p. 243.

[19] Joel REIDENBERG, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", (1998) 76 *Texas L. rev.* 553, 554. This idea was later further developed by other authors such as Lawrence LESSIG (*Code and other Laws of Cyberspace*, New York, Basic Books, 1999; reedited as *Code version 2.0*, New York, Basic Books, 2006).

[20] Ethan KATSH, *Law in a Digital World*, New York, Oxford University Press, 1995, p. 24.

[21] See Walter J. ONG, *Orality and Literacy*, Oxon, Routledge, 2000, p. 2.

[22] Peter A. WINN, "Legal Ritual", (1991) II-2 *Law and Critique* 207, 210-211. See also Antoine GARAPON, *Bien juger*, Paris, Éditions Odile Jacob, 2001, p. 221. Also see Oscar G. CHASE, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*, New York, New York University Press, 2005, p. 114 and ss.

[23] Claude GAUVARD and Robert JACOB, "Le rite, la justice et l'historien", in Claude GAUVARD and Robert JACOB, *Les rites de la justice – Gestes et rituels judiciaires au Moyen Âge occidental*, Paris, Le Léopard d'Or, 1999, p. 5, at p. 9.

implementing technological change, that we understand which ritualistic practices are inseparable from the processes they are associated with[24], and which ones can and should be discarded.

This analysis is crucial since, as Ethan Katsh put it, "new tools for communicating and working with information not only affect our ability to express ourselves, but ultimately bring about changes in what law is and does"[25].

If technology can change our actions, it can also change our institutions and, therefore, the law itself. Hence, before proceeding with the implementation of cyberjustice solutions, we must understand the logic behind the system currently in place. That is to say that we must take into account the social, cultural, and historical contexts from which our current system has emerged. The judicial process as we know it is not the result of a controlled experiment; it was not created in a vacuum. It is the product of our conscious and unconscious social and even religious choices[26], and must therefore be studied while taking into account social and cultural boundaries[27]. As one author submits:

> "Any proposal to borrow procedures from another society should prompt a cultural inquiry. One reason for this is instrumental: Will the borrowed approach work in a new social setting? Processes that are successful in one place will fail in a society where they offend deeply held values."[28]

We argue that such an enquiry should be made when procedures are borrowed from the information society as well, i.e. that it is essential to analyse our procedural rules within a cultural context in order to isolate the underlying rationale behind them before we try to implement technological changes. In other words, as long as we have not clearly established why such or such a component of our legal process works in a certain way, why people have accepted a certain method of doing things or rather why they are attached to it, we cannot hope to succeed in implementing technological solutions in order to make that component more efficient.

3. Identify the true impacts of technological changes on processes

In order to gather information for their research, CRDP researchers regularly hold working seminars with the different stakeholders in the legal system. In one such seminar, a judge explained that he would often receive three versions of the same document from lawyers: an

---

[24] See Oscar G. CHASE, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*, New York, New York University Press, 2005, p. 11.

[25] Ethan KATSH, *Law in a Digital World*, New York, Oxford University Press, 1995, p. 25.

[26] See Oscar G. CHASE, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*, New York, New York University Press, 2005, p. 7. On the general issue of law and social change, see Harold BERMAN, *Law and Revolution*, Cambridge, Harvard University Press, 2003.

[27] See Oscar G. CHASE, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*, New York, New York University Press, 2005, p. 15.

[28] Oscar G. CHASE, *Law, Culture, and Ritual: Disputing Systems in Cross-Cultural Context*, New York, New York University Press, 2005, p. 48.

email version, a faxed version, and the "original copy" which was usually received through the mail days later. He therefore has to explain to the lawyers that these needless multiple copies cause him to waste time rereading and refiling the same document. However, since emails are not officially recognized as acceptable means of communicating court documents under Quebec's *Code of civil procedure*[29], these explanations are in vain since lawyers will always fax and/or mail a hardcopy of any electronic communication.

But this type of anecdote is not limited to Quebec procedure. Although more and more courts accept that documents be submitted electronically, some still require that a paper versions also be filed for archival reasons, specially for large files. For example, the Federal Court of Canada's website states that: "The e-filing guidelines have been amended so that e-filers do not need to furnish paper copies of most documents (this does not apply to documents over 500 pages)"[30]. Furthermore, even in those cases where paper versions of court documents are not required, there still may be someone printing the document at some point because a certain number of stakeholders have yet to become familiar enough with information technology to forgo the use of paper documents:

> "In any event, it its debatable whether this new technology will genuinely cut down on the amount of paper being stored in the registrar's office. Because of the natural tendency of individuals to prefer handling paper rather than reading off a computer screen, it stands to reason that all documents will still be filed in a paper mode or printed by one of its users. If one couples that innate tendency to want paper products in hand with the complete lack of unanimity in the various court houses with what constitutes a legitimate and reliable means of preserving documents for posterity, one can see that a real e-filing system is still a few years away."[31]

If cyberjustice solutions simply add another step to already complex procedures, they do not serve their main purpose, which is to save time and money. Therefore, before adopting a cyberjustice solution, one should ensure that the law permits the use of said solution and, more importantly, that it will simplify the process, not generate further copies of existing documents.

4. Use an incremental or modular approach to technological change

As history has taught us, when it comes to cyberjustice solutions, complete overhauls do not work[32]. They are costly, far too complex, and often lead to resistance from the main stakeholders. For example, in the mid 90's, the Ontario government launched its *Integrated Justice Project*

---

[29] R.S.Q. c. C-25, section 82.1.

[30] See : http://cas-ncr-nter03.cas-satj.gc.ca/portal/page/portal/fc_cf_en/E-Filing.

[31] Jean-Jacques Fleury, "E-Filing for the courts in Canada (an idea whose time has come): A response to a discussion paper published by the Supreme Court of Canada recommending strategies for the selection of an E.F.S.P.", in *Feasibility Report : Electronic Filing Service Provider Model*, Commissioned by the Office of the Registrar, Supreme Court of Canada September 2002, p. 231, at p. 247.

[32] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1.

(IJP), a system that "was to link Ontario's correctional system, the courts, the judiciary, the prosecution service and the police into a seamless network through which civil and criminal cases could be filed and tracked"[33]. The project was ultimately halted after six years of development. Many reasons were given for its failure including the impossibility to link certain systems and the overall difficulty of creating a system-wide network[34], but had the IJP actually corresponded to the needs of the legal system, had lawyers and judges who used the technology pressured the government to keep it in place, it could possibly have been saved. Unfortunately, most stakeholders simply found the technology too complex and were somewhat happy to see it go[35].

One cannot expect stakeholders to completely change their habits overnight. Change brings resistance, so it stands to reason that the more change we try to put forth, the more resistance we will face. Therefore, rather than to simply overhaul the system, we suggest an incremental or modular approach where compatible and interconnecting technological solutions are found in order to address precise problems rather than to construct complex networks. This gives stakeholders a learning curve and eases them into the process.

Of course, this approach implies that the developed technological solutions will have to be compatible and complementary in order to avoid overlapping issues. This further means that future solutions will have to build on the basis of existing modules so as to ensure compatibility and, therefore, that developers will have to share information. Although this is obviously easier said than done, as it implies negotiating with cyberjustice solution providers, it does follow the current trend of states moving towards open source solutions[36].

5. Be aware of the possible implications of outsourcing

In a paper-based system, since the medium and the information cannot be separated, whoever owns a piece of paper necessarily "owns" the data that is printed on it. However, that truism no longer holds when information is digitized, since it can migrate from on medium to another without losing its integrity. This implies that it becomes increasingly important, when court information is stored on servers that belong to a private entity, to clearly establish ownership of data.

---

[33] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1. See also Michael JORDAN, "Ontario's Integrated Justice Project: profile of a complex partnership agreement", (1999) 42 *Canadian Public Administration* 26, 29 and ss.

[34] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1. For a more detailed analysis, see Carl BAAR, "Integrated Justice: Privatizing the Fundamentals", (1999) 42 *Canadian Public Administration* 42.

[35] Sarah LYSECKI, "Integrated Justice Project 'too large, too complex, too ambitious': AG's office", (2005), available at: http://www.allbusiness.com/technology/896690-1.html.

[36] See, for example, Paul Festa, "Governments push open-source software", (2001) *cnet news*: http://news.cnet.com/2100-1001-272299.html; Jim Romeo, "Open source infiltrates government IT worldwide", (2008) *Network World*: http://www.linuxworld.net/news/2008/030108-ossi.html.

That being said, as one commentator observes, "Regardless of the fact that technical 'ownership' of the records remains with the court, there is an inevitable loss of control"[37]. He goes on to explain that:

> "a relationship with a private vendor such as LexisNexis, which might house records on its servers and use proprietary software, places lawyers and local courts at risk of being held hostage to demands for new charges and fees, and makes it difficult to change vendors or bring an e-filing system in-house in the future." [38]

The question of fees raised in the above quote is also somewhat problematic from an open court perspective. If private third parties are contracted to receive, store or otherwise administer digital court data, they will necessarily incur costs in doing so, and, therefore, charge a fee for their services either to the court itself or to litigants who wish to file court documents. For example, Montgomery County, in Texas, contracts with LexisNexis "to provide e-filing services"[39]. According to reports, "LexisNexis charges $7 for filing fees, $8 for service charges for any document filed online, and at least $10 for providing a paper invoice"[40], a situation that some find contrary to the fundamental right that is access to courts[41].

Finally, if court information is stored on servers belonging to third parties, where those servers are situated could raise certain issues. Since a server can technically be accessed from anywhere in the world, its physical site need not be within the county or district of the Court, nor does it need to be in the same country. Therefore, if a server is housed in another jurisdiction, its contents could become subject to that jurisdiction's search and seizure laws. This problem has been observed on numerous occasion by the Canadian Privacy Commissioner with regards to the US *Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001* (*USA PATRIOT Act*)[42]. As explained by the latter:

> "Under section 215 of the *USA PATRIOT Act*, the Federal Bureau of Investigation (FBI) can access records held in the United States by applying for an order of the Foreign Intelligence Surveillance Act Court. A company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it." [43]

---

[37] Andy Peters, "Proposed Ga. E-Filing Rules Raise Concerns", (2010) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471941946.

[38] Andy Peters, "Proposed Ga. E-Filing Rules Raise Concerns", (2010) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471941946.

[39] See John Council, "Federal Challenge to Texas E-Filing System Dismissed", (2011) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202480490900.

[40] See John Council, "Federal Challenge to Texas E-Filing System Dismissed", (2011) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202480490900.

[41] See John Council, "Federal Challenge to Texas E-Filing System Dismissed", (2011) *LTN*: http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202480490900.

[42] See PIPEDA Case Summary #2005-313, and PIPEDA Case Summary #2008-394.

[43] PIPEDA Case Summary #2005-313.

It must be noted that these cases related to personal data – most notably bank records – but the same problem could emerge with sealed court records or other sensitive court information.

6. Identify possible compatibility issues with existing technology and practices

As Fabien Gélinas put it: [translation] "The time has come for a new generation of open and interoperable computer tools that aim to facilitate the judicial and extra-judicial treatment and resolution of disputes"[44]. The key word in this statement is "interoperable". As more and more technological solutions are being made available, decision makers must realise that, just as you couldn't fit a Betamax tape into a VHS system, certain software and computers systems and servers simply cannot interact, which could cause serious problems.

For example, Canada's Courts Administration Service[45], which offers support to the Federal Court of Appeal, the Federal Court, the Court Martial Appeal Court of Canada and the Tax Court of Canada, is currently having trouble with incompatible efiling solutions. Whereas the Federal court of Canada's efiling solution is based on proprietary software developed by LexisNexis ®[46], the Tax Court of Canada[47] uses a far less sophisticated in-house system[48]. Since the two systems weren't developed to interact, this creates a series of problems, not the least of which is the fact that appeals from both tribunals are heard by the Federal Court of Appeals which, for obvious reasons, does not wish to adopt two distinct efiling systems.

As we previously mentioned, Compatibility issues are also among the reasons why the Ontario IJP failed. As one observer put it: "there was a profusion of software, some up-to-date and some archaic, that made it impossible to create simple links"[49].

Therefore, before implementing a cyberjustice solution, it would be wise to do a survey of all the software and hardware (computers, servers, printers, portable devices, etc.) that will need to interact with said solution to make sure that there are no compatibility issues. If such issues do appear, then the choice will be to either upgrade your current equipment or to move towards a different cyberjustice solution. Such a survey might also simply highlight the fact that the costs associated with that specific type of cyberjustice solution are currently too high.

---

[44] Fabien GÉLINAS, « Interopérabilité et normalisation des systèmes de cyberjustice : Orientations », (2006) 10 *Lex Electronica*, http://www.lex-electronica.org/articles/v10-3/gelinas.htm.

[45] http://cas-ncr-nter03.cas-satj.gc.ca/CAS-SATJ/

[46] http://www.lexisnexis.ca/depot_electronique.

[47] http://www.tcc-cci.gc.ca/submit_e.htm.

[48] For more on this issue, see Nicolas W. VERMEYS, "Code source et sources codifiées : pour une cyberjustice québécoise ouverte et accessible" (2010) 14(3) *Lex Electronica*: http://www.lex-electronica.org/fr/resumes_complets/247.html.

[49] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1. For a more detailed analysis, see Carl BAAR, "Integrated Justice: Privatizing the Fundamentals", (1999) 42 *Canadian Public Administration* 42.

7. Identify factual needs, not theoretical wants

Dory Reiling attributes most of the blame for the failure of the Dutch HBS project to "a lack of strategic orientation in the courts" which led to the delivery of a system that "could not be used because essential functionality was missing"[50], i.e. because the needs of the judiciary were not being met.

It becomes essential, when developing a cyberjustice system, to identify the needs of the main stakeholders, not just what is perceived as being useful. Since there is well-documented resistance to change in the legal field[51], the successful implementing of said change will necessarily require stakeholder approval. This approval obviously hinges on whether or not the provided cyberjustice solution corresponds to the needs of each stakeholder. Of course, different stakeholders can manifest different, sometimes opposing, needs[52]. This is when it becomes necessary to distinguish needs from wants.

For example, during a working seminar organized in 2007 by the CRDP, participants were asked why they believed that testimony through the use of teleconferencing had not caught on, even though it presents obvious financial advantages not to mention that it saves considerable amounts of time. We were expecting arguments relating to the right to be present, to face one's accuser, etc. – i.e. arguments based on fundamental rights and legal principles. However, one participant submitted that, in criminal trials, these notions don't necessarily factor into a defendant's choice to be present. Rather, much more mundane arguments for or against videoconferencing are often submitted.

Those who chose to use videoconferencing do so, usually, to stay close to their cells at all times. This limits the chances that other inmates steal their property while they are away. On the other hand, those who insist on trekking to the courthouse do so either because it makes it easier to see their families since detention centres are often away from residential neighbourhoods, or simply because the courthouse cafeteria serves better meals than do most prisons.

So, in this case, accused didn't **need** to be physically present, they simply **wanted** to for reasons that have little to do with their fundamental rights.

8. Use a collaborative approach

When the architects that designed the Cyberjustice Laboratory first submitted their conceptual plans for its high-tech courtroom, our first observation was that they had forgotten the witness box, a particularly important component of any courtroom. They therefore added a box on the right-hand side of the judge's bench. Although this is accurate placement for most US courts, Quebec witnesses are usually seated facing the judge, between the plaintiff and defendant tables.

---

[50] Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 74.

[51] See, for example, Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 74.

[52] Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 65.

Therefore, had legal professionals not been consulted, this mistake would have gone unchecked and the result would have been a courtroom in Quebec that wasn't suited to hold Quebec cases.

One cannot criticize the architects for not knowing where a witness sits in a Quebec courtroom; they had obviously never set foot in one and their knowledge of courtroom architecture was primarily pooled from American television procedurals. They simply extrapolated their limited knowledge of a field that wasn't theirs... The same can be said for those who develop cyberjustice solutions.

Computer programmers, software and application developers and other IT professionals are obviously skilled in their respective crafts, but usually have limited knowledge of the legal process. Therefore, if the development of cyberjustice solutions is left in their hands, the result will be ill-fitting at best, and completely inadequate at worse[53]. This is why it's essential that all stakeholders be implicated in the development phase of any cyberjustice solution. Furthermore, this cannot be achieved by simply having one or two lawyers on a board with fifteen computer programmers. Lawyers, although obviously well versed in the law, cannot be expected to have the capacity to identify all the needs of judges, court administrators, department of justice officials, or clerks, nor are they qualified to establish the best ways to meet those needs[54]. Representatives from each of these groups should therefore sit at the table, as should experts in information and process management.

9. Identify all costs, not simply acquisition costs

Like any other projected change to a process, a shift towards cyberjustice needs to go through a careful and realistic cost-benefit analysis. For example, the benefits of the Ontario *Integrated Justice Project* were originally estimated at $326 million (CAN)[55], but audits and third party estimates placed actual benefits (had the project been implemented) between $180 million (CAN)[56] and $250 million (CAN)[57]. On the flip side, costs were originally estimated at $180 million (CAN), but wound up costing upwards of $350 million (CAN)[58]. As explained by Carl Baar, one reason for the revised price tag was due to not taking into account infrastructure changes necessary to implementing the system: "the initial ninety-day process of confirming cost

[53] On this issue, see Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 74.

[54] When commenting on the failure of the Ontario *Integrated Justice Project*, Dory Reiling pointed to that very fact as one of the main reasons why the project wasn't successful: "the judiciary had enunciated its needs, but the Attorney General decided about the means to meet the needs". See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 65.

[55] See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 67.

[56] See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 67.

[57] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1.

[58] Kirk MAKIN, "Computer lawsuit costs Ontario $63 million", (June 1, 2005) *Globe and Mail* A1. See also Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, p. 68.

figures revealed that an additional expenditure of $75 million would be needed to upgrade court computer hardware so that integrated justice software could operate"[59].

As alluded to earlier when discussing compatibility issues, a shift towards cyberjustice solutions will incur many hidden costs relating to hardware and software upgrades. Costs relating to the training of personnel should also be taken into account, as should costs relating to renovating courtrooms to allow network access and, most importantly, costs relating to securing said networks.

Adequate cost-benefit analysis is especially important since studies show that many failed cyberjustice projects didn't actually fail – they were abandoned because rising development costs made politicians nervous[60] and, of course, political support is essential to getting such projects off the ground.

10. Don't just reproduce: Innovate

As stated above, once we have identified which elements of the judicial process need to be modified, and once we have understood their underlying objectives or justifications, it becomes possible to create or rather adapt technological solutions to suit the stakeholders' needs. This also implies that it might be necessary to adapt our behaviour to the changes brought forth by technology since, as one author puts it:

> "Discussion of the impact of new technologies in the courtroom is likely to, and should, force us to address fundamental issues as to whether prevailing configurations in the courtroom and its environs continue to be vital in the modern legal system" [61]

This is an important issue all too often neglected when developing cyberjustice solutions. Technology should not be seen simply as a means to reproduce the current process or to replace it, but rather as an opportunity to revisit the rationales behind our system and to create new and more efficient ways to address them. As we stated in other arenas, "[i]t is in the re-engineering of proceedings, supported by reasoning that takes the features of the new medium into account, that information technology's potential for improving the justice system will be fully unleashed"[62]. Although changing the medium does not necessarily imply changing the process, it does offer an

---

[59] Carl BAAR, "Integrated Justice: Privatizing the Fundamentals", (1999) 42 *Canadian Public Administration* 42, 60.

[60] See Carl BAAR, "Integrated Justice: Privatizing the Fundamentals", (1999) 42 *Canadian Public Administration* 42.

[61] Linda MULCAHY, "The Unbearable Lightness of Being? Shifts Towards the Virtual Trial", (2008) 35-4 *Journal of Law and Society* 464, 482.

[62] François Senécal and Karim Benyekhlef, "Groundwork for Assessing the Legal Risks of Cyberjustice", (2009) 7 *Can. J. L. & Tech.* 41, 54.

opportunity to do so. Since it's agreed by most stakeholders that the process needs changing[63], why not take this opportunity to imagine new and innovative ways to do so using technology[64]?

Conclusion

There is no adequate way to conclude a paper such as this one since the list of "best practices" we provided is almost certainly incomplete. As studies on the effects of cyberjustice continue to be published, new elements will necessarily have to be added such as risk analysis[65], and interdepartmental cooperation[66]. That being said, this preliminary list, although imperfect, does serve to demonstrated the fact that implementing cyberjustice solutions to resolve some of the justice system's woes is a complex task that should not be taken lightly.

When done right, cyberjustice serves to make the system more efficient and to increase public confidence. Of course, when done wrong, it can result in financial losses and stakeholder resistance. Which category a given project will fall under will depend on a number of factors such as those enumerated above.

On an endnote, one should never forget that the legal process involves interactions between people and information. Therefore, cyberjustice solutions should address both those components and not merely concentrate on the latter…

---

[63] See Hubert REID, *Rapport d'évaluation de la Loi portant réforme du code de procédure civile – Mémoire à la commission des institution*, january 31st, 2008. See also Mélanie BEAUDOIN, "Réforme du *Code de procédure civile* : Pour une amélioration de la justice", (2008) 40(1) *J. du Bar.* 7.

[64] This premise constitutes the second of four research areas on which Cyberjustice laboratory researchers will focus. The three remaining areas being:

- The development of legal software to replicate the legal process in a more expedient manner;
- The study of the psychological, social and cultural impediments to the implementation of cyberjustice;
- The elaboration of new procedural models to favor the implementation of justice networks.

[65] On this issue, see François Senécal and Karim Benyekhlef, "Groundwork for Assessing the Legal Risks of Cyberjustice", (2009) 7 *Can. J. L. & Tech.* 41. See also Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, pp. 62 and ss.

[66] See Dory REILING, *Technology for Justice*, Leiden, Leiden University Press, 2009, pp. 62 and ss.