Canadian Journal of Law and Technology

Volume 12 | Number 1 Article 1

1-1-2014

Legislating Trust

John D. Gregory

Legislating Trust

John D. Gregory[*]

As governments in Canada and elsewhere have considered statutes to ensure that electronic communications are legally effective, they have invariably had to face questions about the reliability of those communications. Can we trust electronic messages, documents, and signatures? Are they the same in law as if they were on paper? What conditions should be imposed in order to give us the right assurances that we can trust them? To answer these questions properly, we need to understand the nature of "trust" and the extent to which legislation can be a source of it, and what other sources should be enlisted to allow prudent legal operations in the digital age.

INTRODUCTION

In this article I raise and suggest answers to a number of questions that arise out of the use of electronic communications. Can we trust electronic messages, documents, signatures? Are they the same in law as if they were on paper? What conditions should be imposed in order to give us the right assurances that we can trust them?

I will be describing the legal policy responses to the ubiquity of electronic communications, with particular reference to electronic commerce and electronic government, and with a focus on how legislation works in this context.

I. WHAT IS TRUST?

Trust may be understood to be a feeling, a state of mind, about a situation or about a course of action, and often about other people. (If "hell is other people", that is particularly true if one can't trust them!) It is a feeling of predictability, of certainty — an anticipation that responses to one's own actions will be in a foreseeable and acceptable range.

But let's look at that statement again: "a feeling of predictability, of certainty" — which may concord with popular expression — "I feel sure of this" — but which disguises the rational content of the process. It is not just or even primarily a feeling; it is the result of a calculation. It is an evaluation. It is a judgment. Information security specialists speak of a "threat-risk analysis" (a TRA) — the key word being "analysis".

---

[*] General Counsel, Justice Policy Development Branch, Ministry of the Attorney General (Ontario).The opinions expressed in this article are not necessarily those of the Ministry. This paper is an updated version of one given as part of the "Distinguished Speakers" Series held by the Law & Technology Institute at the Schulich School of Law on October 25, 2012.

One may have a gut reaction, but in commercial or official matters at least, one seldom leaves it at that; one adds an intellectual component.[1] As a result, trust is not likely to be absolute, both because it is a state of mind and because it is a kind of prediction, as well as being about people, who change. A synonym for "trust" can be "assurance" — whose cognates are "sure" and "secure". This article will discuss the relationship between security and trust, and where the law has been going on security.

One hears in this universe of discourse about "levels of assurance". There are a lot of them, though for ease of discussion and classification and regulation, they are usually in a low fixed number like three or four. They are not, however, hard boundaries; it is a continuum: fifty shades of trust.

II. BENEFITS OF TRUST

What is trust for? Why do we care? Trust provides personal, social, and economic benefits. The personal benefits are obvious: reduction of stress is perhaps the main one. As a social benefit, people get along where there is trust. Trust is the foundation for cooperation, which allows a society to function.

James Surowiecki in *The Wisdom of Crowds* says "Societies and organizations work only if people cooperate. It's impossible for a society to rely on law alone to make sure citizens act honestly and responsibly . . . The interesting thing is that we cooperate with strangers."[2]

On the economic side, predictability means more confidence to build teams (and other economic units) and to make deals, to commit one's resources to the future, and to depend on other people to keep their word. The security expert Bruce Schneier describes the large number of people and institutions he has to trust in order to do a simple repair to his home plumbing: the plumber, not to rob him, not to attack his wife; the banks to clear his payment; the regulators to certify the competence of the plumber; and others.[3]

The ability to have confidence in decisions increases the speed at which one can make decisions. That leads to faster transactions, and this turnover increases prosperity. It is a bit like the money supply, where the speed of circulation of money helps measure the health and the functioning of economy. So building trust leads to wealth creation. The opposite is also true: if we have to check everything on an individual basis, if we cannot count on economic as well as personal cooperation, things bog down (or never get started.)

---

1 Some current popular writing on the theme of the speedy and the analytical response to situations includes Malcolm Gladwell, *Blink: The Power of Thinking without Thinking* (Penguin, 2005) and Daniel Kahneman, *Thinking, Fast and Slow* (Doubleday, 2011).

2 James Surowiecki, *The Wisdom of Crowds* (Doubleday, 2004) at 116-117.

3 Bruce Schneier, *Liars and Outliers* (Indianapolis: John Wiley and Sons, 2012), at 1. See also Amelia H Boss, "Searching for Security in the Law of Electronic Commerce" (1999) 23 Nova L.R.583 at 591, online: Selected Works <http://works.bepress.com/cgi/viewcontent.cgi?article=1003&context=amelia_boss> for another broad description of the elements of trust and security ["Searching for Security"].

III. SOURCES OF TRUST

Where does trust come from? A number of sources have been suggested, which differ in scope and nature and thus effectiveness.[4]

Personal/Moral: One is taught good behaviour and moral standards as a child. The moral theme common to most if not all cultures is the golden rule, the exercise of which would lead to being trustworthy. The lesson carries one through to trusting family and friends, and possibly people of one's own culture even though the general rule is not so limited. In practice, lack of familiarity (note the root of that word, "family") can diminish trust. Social scientists have found that the practical limit to personal spheres where knowledge can become trust is somewhere between one hundred and fifty and five hundred people.[5]

Social: The social basis for trust can be more widespread. It is based on reputation. It is in one's interest to be trustworthy because a bad reputation can hurt one's life chances and economic chances. The effect of reputation is wider now than in the past, with the Internet and search engines and effective permanence of traces of one's life, which can themselves include comments by others.[6]

Institutional: This class of incentives to be trustworthy includes pressure from private organizations that people may belong to and want to keep on the good side of — including being a member. It also notably includes the law. The state sanctions certain kinds of untrustworthy behaviour, notably by criminal prohibition on fraud and other forms of dishonesty. The law also enforces promises (contracts) and protects reasonable expectations — of conduct, of privacy, of rewards. Its application can be as broad in scope as a country, but some areas of trustworthy conduct are more enforceable by law than others. Given the theme and title of this article, we will be coming back to this area in some detail.

Technological: Schneier calls this class "security systems". Such systems can enforce trust or standards of conduct in ways that law or society cannot: by making certain actions necessarily have certain consequences, or preventing them from having others. They can for example ensure that no binding contract will be formed without consent of the parties by requiring an "I accept" click before any obligation is imposed. They can prevent unauthorized copying of music or movies by technical protection measures. They can build in "privacy by design".[7]

Security systems also include after-the-fact detection and cure procedures, such as audits or investigations, and mitigation systems to speed recovery from losses.

---

4 Schneier, *supra* note 3 at 8-9 and Part II.

5 *Ibid.* at 24 and 46 (re "Dunbar numbers").

6 Commercial examples of social reputation-building include eBay's seller rating system, Slash/dot's priority postings, and even New York Times and others' ranking of comments by readers' or editors' preferences. Reputation from such diverse sources will only be as effective as the existence of a persistent identifier allows, so one can trace elements of reputation to the same person.

7 Information and Privacy Commissioner of Ontario, *Introduction to Privacy by Design*, online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/> [Privacy by Design].

One recalls the thesis of Lessig and others in late 90s, that "code is law".[8] This was a very useful perception, that the ways in which technical systems work contain and impose norms, including some degree of trust (or assumptions about trust). Such code systems can have a very wide scope, certainly international for some purposes. Consider for example some social media's limits on permissible content, most browsers' security settings, anti-spam or anti-virus software. The ubiquity of private standards can be a policy issue: how much choice do we really have whether to participate in social media, use large search engines, and so on? And the policy content of code is not to be taken for granted, for better or worse (which is a point of view question in itself — one might like the censorship that Facebook and Apple, among others, impose.)

All of these forces work in interlocking ways to create a system where there is more or less trust. This article is about how the law works in this "ecology".

Note that all these factors work whatever the medium of communication. They are not special to electronic communication, or to economic activity more than to other kinds. Some of the most visible developments in technology in the past 25 or 50 years have been in information technology, but the principles have been the same forever. I can trust my neighbour's moral upbringing and the general disrepute he would bring upon himself if he were to come into my house uninvited and take away my property. The law prohibits that. But I may also invest in a lock on the door, as a technological contribution to my trust of my neighbour.

One might say that the technology operates in the absence of trust, or substitutes for trust, but it is also usefully true to say that it creates trusted conduct, conduct that allows one to make decisions about one's own conduct with some confidence. It is a contributor to a system that encourages trust.

IV. WHAT IS DIFFERENT ABOUT E-COMMUNICATIONS?

Given that we have been living in a society and an economy that has depended on trust (contributed by all of these factors) for a long time, what do electronic communications bring that changes the calculation and that leads to proposals for law reform?

A lot of the nervousness comes from the intangibility itself: where *is* an electronic document? What is it? I can see the computer but I can't see the document. Some kind of software hocus-pocus produces words on a screen or on a printer, but how do I know they will be the same tomorrow or the same for the person I send them to? Computers crash. Formats go strange. Storage media deteriorate. And the malleability of the words and numbers: they are easy to change and it can be hard to detect the change. Why would I trust any particular expression of them?

Lack of familiarity is probably the key difference between paper and electronic documents. We have had several centuries of fairly widespread and more recently universal literacy to learn what makes documents trustworthy and how to

---

8 Lawrence Lessig, *Code and other laws of cyberspace* (2000) online: <http://code-is-law.org/>, and second edition *Codev2* (2006) online: <http://codev2.cc/>; Joel Reidenberg, "Governing Networks and Cyberspace Rulemaking" (1996) 45 Emory Law Journal 911, online: Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=11459>.

build systems — verification systems and document handling procedures — to increase that feature. We do not know as much about e-communications, and the technology is evolving so quickly that what we knew a few years ago may not be valid any more. The result is some nervousness, especially with the constant news of threats, breaches, malware, and so on in both private and public sectors. It is not surprising that people appeal to law to help.

V. TRUST AND THE LAW

How was the law asked to help restore and underpin trust, and how did it, and how should it? These questions will occupy me for the rest of this article.

We should not forget (building on Schneier's list mentioned above) that a lot of law of general application contributes to trust and arguably is intended to promote trust. One thinks of the criminal law (from anti-theft to safe driving rules) but also of regulatory law, aiming to protect us from harmful pharmaceuticals and bad meat and to promote trusted standards in education.

We should also keep in mind enabling legislation that ensures legal effect to certain kinds of civil activity. We expect that our rights will be meaningful and enforceable, and deal with more confidence with people because of that expectation. However, as Surowiecki says, surely correctly: "the measure of success of laws and contracts is how rarely they are invoked."[9]

Let us take a quick look at how the law affects trust now in commercial matters, since e-commerce is much of my theme. At present, and for communications in any medium, the law puts the risk of invalidity, of unreliability, of fraud, on the person who relies on the communication. That person has to bear his, her, or its losses unless he, she, or it can prove that someone else was responsible for the mistake or fraud — and even then the negligent party or the rogue may not be available or in a position to compensate for the loss.

The law does provide some rules to help raise the level of assurance, i.e. trust, in the communications used in transactions. It may require such communications, in order to be legally effective, to be in certain forms. For example, it may be that a document must be in writing, like a guarantee or a land transfer (until recently at least) or a notice of a rent increase. One does not have to trust to memory, one has a written record. It may be that a document must be signed to be effective against the person who signs, again like a guarantee or perhaps an application for a benefit. One does not have simply to allege that a document came from or was agreed to by a person; that person has left an identifiable mark on the document. It may be that the law will give effect to a document only if it is an original, and not a copy, in order to reduce the risk of forgery.

Could electronic communications be used to fulfill these legal form requirements? It appeared that these rules to create trust in the paper world would serve as legal barriers to the development of electronic commerce.

The early attempts to get around these perceived barriers were in private law, through contracts. Businesses that set up systems for electronic data interchange would enter into "trading partner agreements" that set out how the communications would work, who was responsible for what, and when they were to be considered

---

9 Surowiecki, *supra* note 2 at 124.

reliable enough to act on. The agreements usually provided that the e-communications would be considered in writing and often signed as well, where the law required such matters.[10]

Other methods of building trust were for parties to post the terms of their contracts, or the choice of relevant law, on web sites by way of making it clear what they considered the binding rules. Some merchants operated within defined systems that set out known rules for their members. One thinks of credit cards, whose issuers developed rules for "card not present" transactions that were created for phone orders but that became very important in online sales. Industry-wide voluntary codes or standards also were developed to provide a trusted framework for e-commerce. The Payment Card Industry Data Security Standards (PCI/DSS) is a prominent current example, to reduce the risk of the loss of personal data used in credit card transactions.[11]

While these methods were successful to some extent, there was always some doubt whether parties could by contract draft around requirements that were set out by statute. Agreeing that a computer communication was in writing did not necessarily satisfy the legal rule. Even more open to doubt were private agreements on what was admissible in evidence, given that the courts and judges are jealous of their independence in making such decisions. More was needed to remove the barriers, while maintaining the level of trust in business transactions that the requirements served.

The United Nations Commission on International Trade Law (UNCITRAL) came to the rescue with its Model Law on Electronic Commerce, adopted in 1996.[12] The Model Law was implemented in many countries.[13] It is the leading global standard and has done much to facilitate worldwide e-commerce, especially business-to-business (B2B). In Canada, the common law provinces and the territo-

---

10 Electronic Messaging Services Task Force, Section of Business Law, American Bar Association, "Model Electronic Data Interchange Trading Partner Agreement" (1990) 45 *The Business Lawyer* 1645, and EDI Council of Canada, *Model Form of Electronic Data Interchange Trading Partner Agreement and Commentary* (Toronto, 1990). See A. H. Boss, "Electronic Data Interchange Agreements: Private Contracting Towards a Global Environment" (1992) Northwestern Journal of International Law and Business 31 at 58, online: Northwestern Law <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njilb>.

11 Payment Card Industry Security Standards Council, *Data Security Standards*, online: <https://www.pcisecuritystandards.org/security_standards/>.

12 *Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law*. GA Res. 51/162, UN GAOR, 51st Sess., Supp. 17, U.N. Doc. A/RES/51/162 (1997), online: United Nations <http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf> [*U.N. Model Law on Electronic Commerce*].

13 Status of the UNCITRAL Model Law on Electronic Commerce (chart), online: United nations <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html>.

ries all have some variant of the *Uniform Electronic Commerce Act*[14] designed to implement the Model Law, and Quebec has its own statute still consistent with the Model Law's principles.[15]

These statutes helped create trust that e-communications could satisfy the legal form requirements that had been imposed on a world that dealt only with paper. They did so by establishing "functional equivalents" to the paper-based rules, methods by which an electronic record could perform the same legal policy function as the paper record and thus be held to satisfy the same rule — and create the same degree of trust. Thus an electronic document could satisfy the requirement that something be in writing if it were "accessible so as to be usable for subsequent reference".[16] The function of the writing requirement was to serve as memory of the information in the document, so if the information was accessible for subsequent reference, that function had been served. One did not have to trust to human memory; a computer's memory would serve just as a paper record did.

In the same way, UNCITRAL decided that the reason to require an original document was to help assure its integrity, that it had not been altered since put into its final form. An electronic document that could provide reasonable assurances of its integrity could thus perform the same function and meet the requirement for an original. What was reasonable in such an assurance depended on the circumstances.[17]

The operation became a little harder in deciding how to satisfy a signature requirement. The analysis really raised a new question: what is a signature? People had thought that they knew the answer until e-signatures came along to complicate things. Some of the new questions:

- How is a signature linked to a person? It used to be that it came from a pen at the end of the person's arm.
- Is the question whether a document is signed (for the purpose of a law requiring a signature) distinct from the question of who signed it? Can one answer "Yes" to the first question but "I don't know" to the second?
- Does a signature attest to the integrity of the signed document? Common lawyers and civil lawyers had vigorous debates on that question at UNCITRAL.
- Does the legal effect of a signature depend on how reliable it is? To this question, we now turn.

---

14 *Uniform Electronic Commerce Act (Consolidation 2011)*, online: Uniform Law Conference of Canada <http://ulcc.ca/en/uniform-acts-new-order/older-uniform-acts/703-electronic-commerce/1793-uniform-electronic-commerce-act-consol-2011>.

15 *Act to create a legal framework for information technologies*, C.Q.L.R. C C-1.1, online: CanLII <http://canlii.ca/en/qc/laws/stat/cqlr-c-c-1.1/latest/cqlr-c-c-1.1.html>.

16 *U.N. Model Law on Electronic Commerce*, *supra* note 12 at art 6.

17 *Ibid.* at art 8

The function of a signature was to associate a person (or legal entity) with the information in the document.[18] Almost any method of doing that electronically might be adequate if an intention to sign could be found. But UNCITRAL was apparently concerned that "any" method might not replace the trust that the signature requirement was intended to create. The Model Law therefore went on to require that the signing method be "as reliable as appropriate in the circumstances", including among the circumstances that the parties to a document had agreed on how it should be signed electronically.[19]

Here, in my view, UNCITRAL went too far, and a number of legislators around the world went too far in copying it.[20] The UECA does not include the reliability test for signatures, for a number of reasons.

For one thing, the common law does not require a signature to be in any particular form. The written name of the signer is a standard signature, but an unreadable scrawl may also be a signature, though it needs outside evidence to show it is the signer's mark. An X on a piece of paper (or some even flimsier material) can be a signature. A person may sign by someone else: if I ask my assistant to sign my name on a contract or cheque, that is my signature not my assistant's, though there will be questions of proof if anyone questions it. Case law has held that a typed name or even a printed letterhead can be a signature for some purposes.

As a result of this flexibility, a very strong argument can be made that an electronic signature is already a valid signature, and no law reform was needed. The Law Commission of England and Wales came to this conclusion in 2001,[21] so no extra reliability standard was needed.

In any event, the range of handwritten signatures clearly extends from very reliable to not very reliable formats — but the law does not require reliability. In some cases it may impose special rules, as with wills that need two signatures of people present at the same time as witnesses, but in general, as noted earlier, the law deals with reliability by allocating risk to the person who is asked to rely on the signature. It's up to the relying party to decide if the signature is acceptable. The same test can apply to electronic as to ink-on-paper signatures.

A reliability test moves the time of the decision about the validity of a signature from the time the document is signed to the time a judge reviews it in court and decides if it was reliable enough for the purpose. The judge is not necessarily more expert or better able to make that decision than the parties, and in the meantime the law that was supposed to inspire trust has created uncertainty instead.

---

18 Christopher Reed, "What is a Signature?" (2000) 3 *Journal of Information Law and Technology*, online: University of Warwick <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/>.

19 *U.N. Model Law on Electronic Commerce*, *supra* note 12 at art 7.

20 A general discussion of the point can be found in John D. Gregory, "Must E-Signatures be Reliable?" (2013) 10 *Digital Evidence and Electronic Signature Law Review* 67, online: Digital Evidence and Electronic Signature Law Review <http://journals.sas.ac.uk/deeslr/article/view/2024/1961>.

21 Law Commission, *Electronic Commerce: Formal Requirements in Commercial Transactions: Advice from the Law Commission* (December 2001) at para. 3.39, online: Law Commission <http://lawcommission.justice.gov.uk/docs/Electronic_Commerce_Advice_Paper.pdf>.

Finally, having an external standard like reliability gives parties in bad faith, or strangers to the transaction like a trustee in bankruptcy or the tax authorities, a chance to break a contract based on that standard. Despite knowing who signed a document and what document was signed, such a person might successfully challenge a contract on the ground that the electronic signature was not sufficiently reliable for the importance of the transaction.[22] The reliability test becomes a trap for the unwary rather than a source of trust.

In 2005 UNCITRAL adopted the Convention on the Use of Electronic Communications in International Contracts, the E-Communications Convention.[23] The Convention reproduces in binding form many of the rules found in the Model Law. However, for signatures, UNCITRAL was persuaded to add an alternative to the reliability test: that the relying party has shown the origin of the document and the intention of its originator with respect to it.[24] In other words, reliability in fact can replace reliability in the abstract (even if the abstract test was "in the circumstances").

Both of these tests aim to ensure the association of the signer with the record. The policy is the same, the means are quite different. In general in this article, I am not advocating differences in policy. I do not deny that trust is important or that security is important. The article is about legislative means to those ends.

VI. TECHNOLOGY NEUTRALITY — OR NOT

Electronic signatures present an opportunity to consider a different approach to supporting trust by law. A number of people believed that the reliability test of the Model Law was not sufficiently strong. In other words they did not want to remove or amend that test, as I suggested a moment ago — a reasoning accepted by the Uniform Law Conference of Canada and the Uniform Law Commission in the United States as well.[25] They wanted to add to it, or at least define reliability more precisely. Looking at it more broadly, it can be said that they wanted not just to

---

22 Less frequently, a court may hold an e-signature to be sufficiently reliable even when the party to the transaction has decided it is not, thus compelling the party to engage in a relationship it does not trust. *Getup Ltd v. Electoral Commissioner*, [2010] FCA (Australia) 869. For more details, see my case comment on Slaw, online: Lawyers, Engineers and Technology: A Case Study <http://www.slaw.ca/2014/05/01/electronic-signatures-and-election-registration-case-comment-on-getup-ltd-v-electoral-commissioner-australia/>

23 *United Nations Convention on the Use of Electronic Communications in International Contracts*. GA Res. 60/21, UN GAOR, 38th Sess., U.N. Doc. A/Res/60/21 (2007), online with Explanatory Note: United Nations <http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf> [*Electronic Communications Convention*].

24 *Ibid.* at art 9(3)(b), "The method is either . . . (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence."

25 Uniform Law Commission, *Uniform Electronic Transactions Act* (1999) at s 7, online: Uniform Law Commission <http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf>.

remove barriers but to promote the use of electronic communications, and they were prepared to regulate to do so — to create the trust they felt was missing.

There are two main approaches to this attempt: the technology-neutral approach, where the functions or goals or characteristics are recited without saying how technically to achieve them; and the technology-specific approach, which requires the use of particular technologies to ensure trustworthiness. The Model Law on Electronic Commerce is resolutely technology-neutral.

Let us look by way of contrast at UNCITRAL's Model Law on Electronic Signatures, which was adopted in 2001 after several years of development.[26] The discussions on this second Model Law had two points of focus: what were the legal elements of reliability, and what were the consequences of achieving reliability as defined by law?[27]

A common formulation of the technology-neutral but prescriptive characteristics of an electronic signature is a four-part test originally developed by the National Institute of Standards and Technology in the US and reproduced in essence in many statutes around the world. Here is the version used in the Model Law on Electronic Signatures:

> Article 6.3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 [to be as reliable as appropriate in the circumstances] if:
>
> (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
>
> (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
>
> (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
>
> (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

A very similar recital occurs in the Electronic Documents section of Canada's federal legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[28]

Legal systems that set out these requirements generally describe a legal result for meeting them. In other words, they spell out what can be trusted about them.

---

26 *Model Law on Electronic Signatures with Guide to Enactment 2001*. GA Res. 56/80, UN GAOR, 56th Sess., U.N. Doc. A/RES/56/80, online with Guide to Enactment: United Nations <http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf> [United Nations *Model Law on Electronic Signatures*].

27 The discussions can be found in the reports on the meetings of Working Group IV (Electronic Commerce) between 1997 and 2001, online: United Nations <http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html>.

28 S.C.2000 c. 5, online: Department of Justice <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html> [PIPED]. Subsection 48(2) authorizes regulations on "secure electronic signatures". *The Secure Electronic Signatures Regulation*, SOR/2005-30, is on-

Put in their best light, the rules allow participants in a transaction to preserve trust because they do not need to go behind the security system (the drafters hope, in any event). They would not have to defend on substantive grounds against claims that the message was wrong or even never sent. (I have written elsewhere about "the myth of non-repudiation" and will not take up that topic here.[29])

Thus the UN Model Law rules above are part of a description of the method by which one satisfies electronically a legal requirement that information be signed. If one has those characteristics, one satisfies the requirement (unless the contrary is shown). Meeting similar requirements for an "advanced electronic signature" in the EU Electronic Signature Directive makes the signature the legal equivalent of a handwritten signature.[30] This is the least that any such law produces. Using a "secure electronic signature" under PIPEDA creates a presumption that the person purporting to sign the document did sign it.[31] Some laws presume that the signed document has not been altered since it was signed, up to the point when the secure signature was verified.

While these characteristics seem at first view to be helpful, they do not — in my opinion — turn out to be as helpful as they are alleged to be. None of the characteristics are all that solid. In particular, showing the link to an individual can be very hard, if the individual did not personally confirm the signing data — and even then, subject to what verification of identity? Systems that depend on third-party certificates of the link need to demonstrate the reliability of their procedures, which is surprisingly hard. One needs to put in evidence, at least in the face of a challenge, considerable detail about how one issues a certificate, how one verifies identity, how one deals with mistakes or changes, how one keeps the records secure. Certification authorities tend to have very detailed certification practice statements. If a signature relies on a series of certificates (one certification authority verifying the signature of another), then these statements need to be compared to see if they are consistent. Efforts have been made to standardize practices and the supporting documentation, but they have not been widely successful.

The control of the individual over the signing device is also subject to question. What of a malware attack? What of any unauthorized use without the knowl-

---

line: Department of Justice <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/FullText.html>.

29 See John D. Gregory, "The Myth of Non-Repudiation", *Slaw.ca* blog (July 2012) online: Slaw <http://www.slaw.ca/2012/07/16/the-myth-of-non-repudiation>.

30 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal [of the European Union] L 013, 19/01/2000, p. 0012 — 0020, online: European Union Law <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML> [EU E-Signature Directive]. See Article 5 for the legal effect.

31 See the *Canada Evidence Act*, R.S.C. 1985 s. E.5 (as amended in 2000), s. 31.4, online: Department of Justice <http://laws-lois.justice.gc.ca/eng/acts/C-5/page-12.html>, for the ability to create presumptions by regulation, and the *Secure Electronic Signature Regulations*, *supra* note 28, s. 5 for this presumption.

edge of the signer? How do we evaluate that risk?[32] In addition, did the computer actually send the message that the user intended to sign? How does one prove the reliability of the technology?

The additional criteria about detecting alterations to the signed text seem to rely on the use of hashing techniques usually associated with dual-key encryption signatures[33] and may not be technology-neutral at all.

In evaluating the impact of such e-signatures on trust, one must ask how sure one is that the characteristics exist. We might question the detailed formulation on its use of the word "assurance". How sure does one have to be before one has assurance? The question is similar to that posed regarding legal duties to "ensure" that something happens. Ultimately for legal purposes it is a judge who has to be sure, or who has to be persuaded that the degree of assurance attained was reasonable. It is thus subject to the same problem as the original reliability test of the Model Law on Electronic Commerce, that the parties cannot be confident in their choice of signing method. A court may ultimately overrule them on technical grounds.

Information security systems are frequently expressed as attaining particular levels of assurance, which is to say that some assertions are surer than others. This is not surprising or problematic, except when one alleges that one has created trust by this legislation. What level of trust? If that question is still open, then perhaps we should just ask it of the signature itself and all its surrounding circumstances, and not of the signature's compliance with these rules.

Although the UNCITRAL Model Law on E-Signatures is framed in technology-neutral language, a number of critics have thought that its requirements, especially those relating to the alteration of the signature or the signed document, can be met only by a system using dual-key (or public/private key) encryption in a network using trusted third parties to certify the signatories. In other words, it is a technology-specific rule relying on a public key infrastructure (PKI). A signature produced by such a system is usually called a "digital signature", though that term is unhelpfully also found as a generic synonym for any electronic signature.

It has been suggested that the partisans of technology-specific legislation have come to the discussion from a review of the technology, rather than from a view of removing barriers to e-commerce.[34] Their analysis of the technology leads them to seek a technological solution and often a regulatory solution to the vulnerabilities

---

32 Some of these questions are raised as well in my note on non-repudiation, *supra* note 29.

33 Dual-key (public key) cryptography is described at Wikipedia, "Public-key Cryptography" online, Wikipedia <http://en.wikipedia.org/wiki/Public-key_cryptography>. A short note on hashing functions in context is provided at *Key Management Infrastructures*, "Frequently Asked Questions", online: French National Department of Defence <http://www.ssi.gouv.fr/archive/en/faq/faq_igc.html#5230>.

34 See for example Boss, "Searching for Security", *supra* note 3 at 598ff; also C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure" (2000) 16 Computer Security Journal 1, online: Schneier on Security <https://www.schneier.com/paper-pki.pdf>.

they perceive.[35] Their critics have sometimes alleged that PKI is a problem in search of a solution.[36]

This is not the place to go into the details of how difficult it is to build a public key infrastructure, especially for an open system where strangers might deal with each other.[37] Proving the elements of the specified technology is still difficult too — not just the mathematics of digital signatures, but the whole system. Many of the questions raised above with respect to technology-neutral systems arise again for specific technology. If one assumes that the legislation specifying the technology replaces the need for proof, because the legislature is satisfied that it works appropriately, one is left instead with proving that one has used the right technology in the right way.

The European Union issued a Directive on Electronic Signatures in 1999 that set out criteria like those in the Model Law on E-Signatures, with very detailed requirements for "qualified certificates" linking owners of signature creation devices to their signatures, and for the issuers of those certificates.[38] It has turned out in practice that businesses have not relied as heavily as expected on the "advanced electronic signatures" so produced. It may be harder to show that a particular signature meets all the technical criteria than it is to show who signed the document in fact.

The attempt to legislate trust in this way cannot be said to have succeeded.

It is an open question how to avoid having the legislative "approval" of good security technology itself turn into a barrier to commercial trust. This is a question to which I do not claim to have definitive answers.

VII. TRUST AND LIABILITY

It may be of interest, however, to look briefly at one element of much of this legislation that aims at an aspect of trust we have not yet reviewed: liability of the participants.

Liability can be seen as an "institutional" support for trust. Liability rules ensure that someone takes on the burden of making things work in a trustworthy way or pays the cost of remedying a failure of trust. Liability rules can be efficient or disruptive. Do they put the burden of trustworthiness on the party best able to bear it, or to insure against it? Can the parties allocate the liability among themselves fairly, by contract?

As noted earlier, under our general law, the relying party takes the risk of loss from a forged or unprovable signature or document. One of the char-

---

35 For a discussion of the different approaches of lawyers and engineers, see my Slaw column, online: Lawyers, Engineers and Technology: A Case Study <http://www.slaw.ca/2011/08/25/lawyers-engineers-and-technology-a-case-study/>.

36 Jane K Winn, "The Emperor's New Clothes: The Shocking Truth about Digital Signatures and Electronic Commerce" (2001) 37 Idaho Law Review 353 at fn 4.

37 See for example Ellison and Schneier, *supra* note 35 at 1; C. Kaner, "The Insecurity of the Digital Signature" (1997), online: Bad Software <http://www.badsoftware.com/digsig.htm>.

38 EU E-Signature Directive, *supra* note 30.

acteristics of the attempt to be more prescriptive about electronic signatures is that it sometimes shifts that burden. I mentioned a moment ago the presumptions of attribution and sometimes of integrity of the signed document that have accompanied "secure electronic signatures". Some such systems go further and make the person who controls a signature creation device (which could simply be the person's computer) liable for documents signed with a digital signature certified to come from that person. The State of Utah was a pioneer in such statutes in the United States; its *Digital Signature Act of 1995* had such a provision, though only where the certificate was issued by a licensed certification authority regulated by the State.[39]

In other words, the government was intervening actively in the market for signatures in order to promote e-commerce, to the extent of assigning liability for private actions. The problem was that it was hard to ensure that even a regulated certification authority would get all its verification and enrollment procedures right, and that the user of the signing device would avoid all attacks on the computer, including from malware such as keyloggers and trojans. Though the mathematics of dual-key encryption is impressive, the signing is usually done by a computer accessed with a simple user name and password, and such systems can be very insecure. One skeptic said of the Utah system that he expected to see the headline "grandmother chooses weak password, loses house".[40]

Without such an assignment of liability, however, the business model of an open PKI did not make much sense. Without it, the liability normally on the relying party would focus on the third party who certified the identity of the signer. If that identification failed, to the loss of the relying party, then lawsuits would follow. Attempts were made to design PKI systems so that there was a contract between the relying party and the certification authority, so that the latter could limit its liability by agreement. Such attempts have not been very successful. As a result, not many private bodies have wanted to be in the certification business for high-value transactions.

If the model did "work", in that the allocation of liability resisted attacks both legal and popular, it is still subject to the criticism that it distorts the market to support a single technology. The distortion works in two ways (at least). First, it pushes technical innovation down the path that gets the prescribed legal benefits, and discourages innovation in what might be more fruitful but legally unrecognized directions. Second, it puts liability on par-

---

39 Utah *Digital Signature Act*, Utah Code ss. 46-3-101 to 46-3-504 (1995), enacted by Utah Laws 2005 c 61, s 46-3-401ff online: Universita Degli Studi Di Trento <http://www.jus.unitn.it/users/pascuzzi/privcomp97-98/documento/firma/utah/udsa.html>. The Act was repealed in 2000 and replaced by a version of the *Uniform Electronic Transactions Act*, *supra* note 25.

40 See C. Bradford Biddle, "Comment: Misplaced Priorities: The Utah *Digital Signature Act* and Liability Allocation in a Public Key Infrastructure" (1996) 33 San Diego L.R. 1143.

ties least able to bear it or to avoid it, compared to the general law, and requires a heavy regulatory hand to make it work.

One may compare the allocation of damage for loss of credit cards to the card issuers and not the card holders. The result is that the issuers create many verification systems based on typical use, source of claims, and so on, that individual holders would not be able to replicate.[41] Such a system is not easy to create for authentication systems generally.

In short, statutory allocation of liability as described for digital signatures legislates the winners of a competition that should be left to the market to sort out.[42] Governments do not know this kind of thing any better. Governments may help compensate for "market failure", but we do not have market failure in the world of e-signatures or e-commerce — consider the billions of dollars of transactions online, large and small, every day. Those numbers were there, though smaller, in the late 1990s when these attempts were first made. People are relying on electronic communications and they are right to do so.

One may conclude that the attempt to create trust in e-commerce through technology-specific legislation has not been a good idea. Part of the problem has been that commercial law is generally enabling and remedial, not promotional or regulatory. Commercial law rarely tries to lead commercial practice, because it does not want to restrict business innovation. Focusing on the technology from the start risks creating technology law, not commercial law, and the trust problem is not properly addressed.

Requiring PKI for commercial transactions has certainly not succeeded. PKI has its uses, however. It works fairly well in closed systems (such as within governments, or between some banks and their customers) with substantial administrative capacity. It also works well in supporting the secure socket layer (SSL) system for secure access to web sites. This system works because the Internet browsers like Chrome and Safari and Firefox build in recognized certificates that identify web sites, and addressing those sites invokes the certificates. SSL can be beaten, but it has worked satisfactorily so far.[43]

---

41 The liabilities in the credit card system have been allocated for some time, and the market lives with them. The advent of mobile payments is upsetting this market because there are a multitude of possible payment providers — telecom companies, device manufacturers, and others beyond the credit card world — and their relationships are still fluid and competitive, so the "right" allocation of liability is not known. Thus how the whole system will develop trust in its users remains to be seen.

42 C. Bradford Biddle, "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace" (1997) 34 San Diego L.R. 1225.

43 This statement was written before the recent Heartbleed defect was known: <http://heartbleed.com/>. It has caused major trauma to a number of security experts: <http://en.wikipedia.org/wiki/Heartbleed>.

I have submitted to this point that attempts to legislate trust have not succeeded in electronic commerce, whether through: technology-neutral laws like the Model Law on Electronic Signatures (not implemented in Canada and the US, by and large — the part of Quebec's framework statute that most closely tracks the MLES has not really been implemented in the past decade); or the EU Directive; or technology-specific laws like the digital signature legislation in Utah and in several countries that adopted similar legislation at the same time (Germany, Italy, and Malaysia come to mind).

Some countries enacted "hybrid" legislation, removing barriers to general e-communications and providing special treatment for especially trustworthy technology. Singapore is a leading example,[44] but there are others; to the extent that the EU Directive prohibited discrimination against ordinary e-signatures, it might be considered a hybrid as well. The question is whether there has been wide use of the secure signature techniques among unrelated parties, as the "promise" of PKI was to enable trusted high-value commerce among strangers. I have seen little evidence of such use.

VIII. OTHER SOURCES OF TRUST (SOMETIMES SUPPORTED BY LEGISLATION)

I would submit that the mistake in trying to legislate trust is to conceive of trust as an element of legal validity. It is not, or it should not be. A valid transaction need have no different features in e-commerce than in offline deals: a common understanding of the subject and the price and a common intention to contract. The form has nothing to do with it.

Similarly, the form of a signature has nothing to do with its legal effect, for handwritten as for electronic signatures. One needs context to make that judgment, context with legal content. So laws that apply only to form may miss their legal mark and not create the trust they aim for.

That does not mean that trust is unimportant, or that security can be ignored. Using e-communications may be valid in law, but is it prudent? What are the risks? What is the cost of reducing the risks to an acceptable level? How much assurance does one need before transacting? As a matter of legal validity and as a matter of trust, an electronic transaction should not need to be more reliable than its offline equivalent. The question is who determines that level of reliability and how.

While parties to commercial transactions need to have a degree of trust, it is up to them to decide if they have it or not. There are many non-legislative, non-legislatable sources of trust: personal relationships; a history of prior dealings; and diverse elements of evidence of identity, intention, or quality. Identity is often much less relevant to a transaction than solvency, for example. All of these factors apply just as much online as offline.

---

44 Singapore, *Electronic Transactions Act* (2010) Statutes of Singapore c 88 (originally enacted in 1998), online: Attorney General's Chambers, <http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=CompId%3A1f4c67a4-a626-4f42-b2ad6035d6c7d797;rec=0;resUrl= http%3A%2F%2Fstatutes.agc.gov.sg%2Faol%2Fbrowse%2FtitleResults.w3p%3Bletter%3DE%3Btype%3DactsAll>.

Looking strictly at the media of communications, it is possible to verify an electronic message by way of a phone call or fax. It is a general principle that one cannot establish trust in a channel of communication through that same channel. That would be the equivalent of saying, "trust me because I assure you that you can." What is the "level of assurance" of such a statement? Legislation that has purported to make a single communication trustworthy, for example by defining it as reliable, has turned out to need outside evidence of reliability when the original attribution has been challenged.

Another major way to develop trust is by the involvement of third parties — not as free-standing providers of identification services, as in the open PKI model, but as part of their usual activities. For example, one of the main reasons that business to consumer (B2C) e-commerce exists is because of the role of the credit card companies and the financial institutions that issue the cards. Merchants really do not care much who they sell goods or services to, if they get paid. The card issuer has an identity-based relationship with the card holder/consumer, so the merchant does not have to. The card issuers identify by proxy, but they really stand behind the solvency of the customer.

Another area where proxies can be important is with student loans. Student loan authorities wonder how they can enroll a student online, i.e. without ever seeing him or her in person. It is admittedly easy to deal electronically once one has met the applicant in person; one can issue him or her authentication codes that allow e-communications and electronic funds transfers. The hard part is in knowing who someone is in the first place: "On the Internet, no one knows you're a deadbeat."

The California student loan system solves this problem by farming out both identification and payment. A student who needs a loan has to have an identifier from an eligible educational institution and also an account with an approved financial institution. If both institutions acknowledge the applicant's status, then the government loan office can safely trust that identification. The process is made even safer by making the payments only to the educational institution, with the balance if any paid directly to the bank. As a result, there is very little incentive for an ineligible person to try to scam the system: there is just not much money lying around loose.

Note how trust is developed here through a kind of network, and how the payment rules supplement the trust network to reduce the risk of trusting. The proxies involved may be in the private or the public sector. Here there is an interaction. There may be legislation approving this system, but more for the purpose of authorization than to prescribe the levels of assurance.

A notable example of the use of proxy identifier is in a scheme currently being proposed by the Government Digital Service, part of the Cabinet Office in the United Kingdom.[45] It has been working to create a means by which citizens can identify themselves electronically to government in order to take advantage of a wide range of government services, without creating a national identity card or a

---

45 A selection of news items about the progress of this project is online: Government Digital Service <http://digital.cabinetoffice.gov.uk/category/id-assurance/>.

single sign-on identifier. Such all-access tokens or cards have tended to cause great concern among privacy advocates, especially in common-law countries.

The Service is proposing instead that the government will accept authentication (log-in) by means of accounts they have with non-governmental organizations, including social media. So one might be able to request a government service by using your name and log-in information from Facebook or your bank. Those institutions will not know why the government wants the authentication information, so they do not know what their members are doing with the government. There will be standards of security imposed for institutions to qualify to participate in the program.[46] This is one example of a phenomenon known as "federated identity management," in which evidence of identity from a set of more-or-less linked sources (a federation) is used to authenticate people for access to particular systems.[47]

The Government Digital Service describes this system as "less about identity, more about trust." This is an important observation: e-communications are teaching providers of goods and services what they really need to know about the people they deal with, and what can just as easily be set aside or provided in another form. Governments are making the same discoveries, with pressure from the privacy advocates.

One sees the use of proxies for enforcement of digital rights as well. One much-discussed example is the effort to make Internet Service Providers (ISPs) liable for defamation or copyright infringement on the part of their subscribers (or even for messages that pass through these intermediaries), or for content that they host. Some of these efforts have been based on the common law, but statutes have been advocated for or passed to make the ISPs serve as data storage points or even as police. Consider the "three strikes" laws against copyright infringement that require ISPs to give notice of alleged infringement to subscribers and to cut off their Internet service after three (alleged) infractions. To the extent that content owners want a "trusted" Internet, such legislation aims to increase it.[48]

---

46 It is not likely that one's Facebook credentials will meet the ultimate standards, but an e-banking authentication might do so.

47 Federated identity management is described on Wikipedia, "Federated Identity", online: Wikipedia <http://en.wikipedia.org/wiki/Federated_identity_management>. Canadian government initiatives are described at *Federating Identity Management in the Government of Canada: A Backgrounder*, online: Treasury Board of Canada Secretariat <https://www.tbs-sct.gc.ca/sim-gsi/docs/2011/fimgc-fgigc/fimgc-fgigc03-eng.asp>. The government of British Columbia has been working on the topic for some years, with the most recent development being the BC Service Card. The initiatives are online: *Provincial Identity Information Management System*, online: Office of the Chief Information Officer <http://www.cio.gov.bc.ca/cio/idim/index.page>. The American Bar Association has a task force on the topic whose site links to a number of interesting documents: *Cyberspace Law: Identity Management Legal Task Force*, online: American Bar Association <http://apps.americanbar.org/dch/committee.cfm?com=CL320041>.

48 A collection of articles on such laws, also known as "graduated response" laws, is found on TechDirt — not a neutral observer, but its news items are likely to be accurate: http://www.techdirt.com/blog/?tag=three+strikes. It may be that such laws are becoming less attractive to legislators.

This example — not really drawn from commercial law, though commercial interests are at stake — shows that trust is not evenly distributed across our society or our economy. One person's "trusted computing" (a Microsoft phrase) is another person's spyware, or interference with assumed rights.

Regulators also focus on intermediaries to generate an effect they can trust. In Canada, the Copyright Appeal Board and the Supreme Court of Canada have held that ISPs are not broadcasters for allowing access to content, though copyright owners would have liked to have them as a pressure point (or cash flow point) for their interests.[49] However, legislation requires ISPs (among others) to report any instances of child pornography they find, in order to create trust in the safety of the system.[50]

Similarly, in the US, Congress exempted intermediaries from any liability for content that originated with a third party, because they were such attractive targets.[51] This protective legislation reminds us of the connection between trust and liability mentioned earlier: imposing liability would inspire conduct of the kind the plaintiffs wanted and wanted to be able to trust. Protective legislation was based on the principle that increasing unhampered Internet activity was more important than the values promoted by imposing liability for the content of messages transported by the intermediaries.

IX. LEGISLATING THE TRUSTED FRAMEWORK VS. LEGISLATING THE TRUSTED TRANSACTION

If we want our electronic marketplace to move from mistrust to confidence, has legislation any role? Is there no middle governmental ground between the *Criminal Code* or *Sale of Goods Act* and the digital signature statutes that appear to be a bad idea? I think that there is. I am not going to describe such legislation in detail here; I have not written any (yet). I am going to point to a few key considerations for its design, and describe briefly a few promising initiatives.

I submit that the legislatures should be aiming at creating a legal framework for trust, rather than trying to govern the trusted transaction itself. Since trust, as I said at the outset, is a judgment resulting from an analysis of risk, there can be ways to affect the amount of risk in the system and the allocation of risk, without requiring the use of any technology or imposing mandatory liability. The latter ties the hands of people who may have many reasons to prefer risk to certainty (to some

---

49 *Society of Composers, Authors and Music Publishers of Canada (SOCAN) v. Canadian Association of Internet Providers*, 2004 SCC 45, online: Supreme Court of Canada <http://scc-csc.lexum.com/decisia-scc-csc/scc-csc/scc-csc/en/item/2159/index.do>.

50 The federal and Manitoba legislation are found at *Mandatory Reporting*, online: Canadian Centre for Child Protection (Cybertip), <https://www.cybertip.ca/app/en/projects-mandatory_reporting>. That site does not currently note the Ontario and Alberta statutes on the same topic.

51 Section 230 of the *Communications Decency Act, 1996*, online: Legal Information Institute <http://www.law.cornell.edu/uscode/text/47/230>. A useful explanation of the legislation is provided by the Electronic Frontier Foundation "Section 230 Protections" *Legal Guide for Bloggers*, online: Electronic Frontier Foundation, <https://www.eff.org/issues/bloggers/legal/liability/230>.

extent that is true of any entrepreneur) and who should be presumed to be competent to evaluate their risk at the transactional level.

One can look at legislative tools that operate on the civil law side (what is valid? what is effective?), the criminal side (what is prohibited?) and the regulatory side (how are things to be done?). One can decide who should be the subject, or target, of such laws: parties to transactions, intermediaries, proxies, businesses, consumers, or government. Should one impose obligations directly or enact incentives to desirable behavior? Should the rules be made at a provincial, national, or even international level?

Jeffrey Ritter, a pioneer in e-commerce law and in building trustworthy systems for business, has noted that "the posse has to stop at the river" — in other words, there are limits to what a national authority can do in the world of electronic communications, and international collaboration may be best.[52] Indeed it is not a coincidence that one finds the intellectual leadership in e-commerce law at the international level, in UNCITRAL and elsewhere. The European Union has set world standards in privacy law, though as noted earlier, its first efforts on electronic signatures did not have the expected success. So consistency with the best international thinking is nearly mandatory these days in this field.

X. STANDARDS

Besides legislation, lawmakers can encourage development of and compliance with standards and guidelines, private or public. Sometimes such documents become mandatory over time. The Organization of Economic Cooperation and Development (OECD) published Fair Information Practice "guidelines"[53] in 1980 that lie at the heart of most privacy legislation around the world. The Canadian Standard Association's Model Privacy Code became the core of Canada's federal privacy legislation, along with "substantially similar" provincial laws in several provinces.[54]

Regulations under the *Income Tax Act* give preferential status to taxpayers' electronic records that comply with the Canadian General Standards Board's Standard for Electronic Records as Electronic Evidence, and for some purposes the regulations require compliance with that standard.[55] The role of the law of evidence in

---

52 Private correspondence with the author. See online: <http://jeffreyritter.com> and Ritter, J., *Building Digital Trust* (forthcoming).

53 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)*, online: OECD, <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>. The guidelines were updated in 2013. The address here contains a link to the revised version.

54 The Code is Schedule 1 to PIPEDA, *supra* note 28. Quebec, Alberta and British Columbia have statutes designated as substantially equivalent, and Manitoba has recently passed legislation that is likely also to be designated.

55 Canada Revenue Agency, "Books and Records Retention/Destruction", Information Circular IC78-10R5, para 17–23, online: Canada Revenue Agency <http://www.cra-arc.gc.ca/E/pub/tp/ic78-10r5/ic78-10r5-10e.pdf>. See also Canada Revenue Agency

promoting trust in e-communications is a fascinating topic, though beyond the scope of the present discussion.

Some of the opposition to legislated cybersecurity rules in the United States has pointed to the array of existing standards to which businesses have bound themselves.[56] However, the variety of such standards definitely raises the question whether some mandatory minimum should be prescribed by law, even if the content remains flexible in some way. One could have a legislative guide for the minimum contents of security standards, or require adherence to some standard without saying to which, or combine rules to compel adherence to a standard that meets the legislated minimum content. If there is a single principle here, it is that one size does not fit all. One has to tailor the solution to the problem, and understand the problem correctly before starting the tailoring.

XI. APPROACHES

That said, some common approaches seem from experience more promising than others. One of them is "media neutrality" — having the same rule for the same phenomenon regardless of the medium in which it appears: paper or electronic, and within the electronic world. That is why the definition of "electronic signature" in the Canadian and American uniform e-commerce statutes refers to data in electronic form used with "intention to sign".[57] The use of the traditional word was deliberate: there was not one legal act of signing on paper and another for electronic media. There was one signature at all.

Another promising approach is "technology neutrality", already discussed. The more specific the reference to a technological solution, the more likely that solution is to be out of date almost before the law can be enforced. That does not mean that the law cannot address particular problems caused by specific technology, but the more general its language can be, the less likely one is to create loopholes that new technology with similar problems can slip through. UNCITRAL's Model Law on Electronic Signatures was intended as a technology-neutral framework, but for reasons given earlier has not widely been considered a success. PKI generally is not a technology-neutral system, though it is normally a system framework rather than transactional in focus.

If one is focusing on a middle level between national policy and the transaction, i.e. on a system, then one is more likely to prescribe or encourage a process than a result. One intends that trust in the system will increase as a result of the legislation, but without prescribing that it must. An example of this on which a lot of work is now being done, both here in Canada and internationally, is online dispute resolution (ODR). UNCITRAL has a working group that has been meeting

---

"Electronic Recordkeeping", Information Circular IC05-1R1, online: Canada Revenue Agency <http://www.cra-arc.gc.ca/E/pub/tp/ic05-1r1/ic05-1r1-10e.pdf>.

56 Jody Westby, "Rockefeller Admits Congress Lacks Foundation for Cybersecurity Legislation", *Forbes* (1 October 2012) online: Forbes <http://www.forbes.com/sites/jodywestby/2012/10/01/rockefeller-admits-congress-lacks-foundation-for-cybersecurity-legislation/>.

57 *Uniform Electronic Commerce Act*, *supra* note 14 at s 1(b) and the *Uniform Electronic Transactions Act*, *supra* note 25 at 2(8).

since 2010 on the topic.[58] The group is likely to adopt a set of procedural rules for resolving B2B and B2C small-value but high-volume disputes. The highest-profile Canadian project is British Columbia's Civil Resolution Tribunal, to become active in 2014.[59]

Having a good ODR system will promote e-commerce because people will have confidence that if things go wrong, there is a remedy. I mentioned at the outset of this article that "security systems" could enhance trust even if they worked retroactively. ODR in fact would not be strictly retroactive, since the relationship between the parties is not over until after the ODR has done its work. ODR is a combination of technology and law, and UNCITRAL is considering elements of both. They may be joined eventually by simplified rules of substantive law, again to increase confidence of the parties that their transactions will not be bogged down in foreign legal complexities but that expectations will be met.

A recent Working Paper for the UNCITRAL ODR project adds some fascinating possibilities to this topic.[60] It canvasses "private enforcement mechanisms" that might be part of an ODR system to operate outside the formal court system. Some create an incentive for the parties to conform with the results of a mediation or recommended solution. Others "automate" compliance with the outcome. The incentives discussed are ratings systems and "trustmarks," the former generated by users of the ODR service (or e-commerce site) to give their opinion of their experience, the latter generated by some neutral institution that evaluates compliance according to published standards. The paper raises some practical questions about how such systems might be made to work in an ODR e-commerce system.[61] It goes on to canvass very briefly a number of more "radical and holistic" approaches to incentives that could see a non-compliant merchant lose its domain name, be put on a black list, have its payment facility (e.g. PayPal or Amazon) be suspended, or lose membership in a business association. These methods would depend on some third-party involvement, and it is not currently clear how third parties might be persuaded to get involved in an international compliance system for this purpose.[62]

The automated compliance mechanisms would restore money to the successful customer from a merchant who did not comply with a settlement or recommendation (in the context of ODR that is not legally binding in the sense of enforceable through the courts.) The two methods discussed are chargebacks through credit

---

58 UNICTRAL Working Group III, Online Dispute Resolution, online: United Nations <http://www.uncitral.org/uncitral/commission/working_groups/3Online_Dispute_Resolution.html>.

59 Attorney General of British Columbia, *Civil Resolution Tribunal Act*, online: Ministry of Justice <http://www.ag.gov.bc.ca/legislation/civil-resolution-tribunal-act/>. See also John D. Gregory, "Canadian Initiatives in Online Dispute Resolution" (September 2012), online: http://www.euclid.ca/Korea_ODR_2012.pdf.

60 UNCITRAL Working Group III, *supra* note 58, "Online dispute resolution for cross-border electronic commerce transactions: overview of private enforcement mechanisms", Working Paper 124 prepared for the November 2013 meeting (A/CN.9/WG.III/WP.124.).

61 *Ibid.* at paras. 17–26.

62 *Ibid.* at paras. 27–29.

card issuers and escrow accounts. Both methods are known in some regions of the world and not so much in others. They too would usually involve third parties who would need to be recruited to the process, by persuasion or legislation.[63]

Those are some of the "approaches" to designing legislation that can promote trust in the system and in the processes of commerce generally. Let us look briefly at some specialized areas where these initiatives can work.

The first is the domain of security itself. If the challenge is untrustworthy technology, then one may be able to discourage its use and encourage trustworthy technology. This is of course a never-ending effort, rather than one that can be resolved by just the right statute. The history of technology security legislation is already longish. We have prohibitions on unauthorized access to computers and the theft of computer communications.[64] We have laws about the use of particular kinds of information, such as copyrighted text (one is not allowed to disable technical protection measures designed to protect it).[65] We have export controls on sensitive information and encryption systems. We have the Budapest Cybercrime Convention[66] and bills in Parliament about law enforcement access to personal information to detect crimes.[67]

The second domain is related to security: privacy. One sees the link in the description of privacy laws as "data protection" legislation (there is not a complete overlap between all privacy and all data protection statutes, but the overlap is significant). Privacy protection extends from prohibitions against "identity theft" (a popular if somewhat misleading title) to requirements to limit the collection, use, and disclosure of personal information, to a duty to keep such information secure[68] and to notify people if their personal information is compromised despite that duty.[69]

---

63 *Ibid.* at para. 30–42.

64 *Criminal Code of Canada*, RSC 1985 c C-46, s 342.1.

65 *Copyright Act*, RSC 1985, c C-42, s 41, 41.1.

66 The Council of Europe's Cybercrime Convention and supporting documents, including "Guidance Notes" about its implementation, are available at *Action Against Economic Crime*, online: Council of Europe <http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp>. Canada has signed the Convention but not yet ratified it.

67 Bill C-30, the *Investigating and Preventing Criminal Electronic Communications Act*, 1st Sess, 41st Parl, 2012 contained a number of such provisions. It is online: Parliament of Canada <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5380965>. It was later withdrawn because of controversy about its effect on privacy. Somewhat similar powers are granted in the cyberbullying statute introduced in 2013. Bill C-13, *Protecting Canadians from Online Crime Act*, 2nd Sess, 41st Parl, 2014 is online: Parliament of Canada <http://www.parl.gc.ca/LEGISInfo/BillDetails.aspx?Language=E&Mode=1&billId=6301394>.

68 See for example PIPEDA, *supra* note 28, Schedule 1, s 4.7, Principle 7: Safeguards.

69 See for example, *Personal Information Protection Act* (Alberta). SA 2003, c P-6.5, s 34; *Personal Health Information Protection Act* (Ontario), SO 2004 c3, Sched 4, s 12; *Uniform Protection of Privacy Amendment Act (Data Breach Notification)* (2010) at p

Security and privacy are sometimes at odds, however. The desire of "security" authorities for full authentication of individuals can conflict with the principle of collecting only the minimum personal information required for the purpose. Industry Canada's 2004 Principles of Authentication[70] recognized this potential, and we have seen it in law enforcement case law and legislation. A "dialogue" continues.

However, one also sees privacy interests complemented by security measures, popularly now known as "privacy by design", a concept promoted by Ontario's Information and Privacy Commissioner, Ann Cavoukian.[71] I mentioned earlier Lawrence Lessig's "code is law" principle. This is "code as law" in action, with the appropriate focus on the policy of the law expressed by the code. People's willingness to engage in electronic communications increases if they think their privacy is protected.

A third domain where legislation may be promising is the regulation of the services of "trust providers." As noted earlier, it may not be ideal to give transactions conducted through identification certifiers ("certification service providers" as UNCITRAL has called them)[72] special legal status. It may, however, make sense to set standards of trustworthiness for them to follow. One can debate whether those standards should be set by law or published as guidelines, or whether a full-fledged licensing program should be established. Different countries have tried different strategies, but if the activities of such businesses are to succeed in increasing trust in e-communications, one understands the argument that they must themselves be reliable. The Model Law on Electronic Signatures contains a number of criteria for such a standard of reliability.[73] The new EU regulation on authentication, a draft of which was released in 2012, continues a similar program.[74]

As I mentioned, none of this discussion constitutes the design of actual legislation to enhance trust, but I submit that it is laying out relevant criteria for such legislation. I might in closing mention one issue close to my own heart, or at least close to my own work: should government benefit from special rules? Is government especially trustworthy, so as to be — as has been suggested — the ultimate

---

12 ff, online: Uniform Law Conference of Canada <http://ulcc.ca/en/2010-halifax-ns/573-civil-section-documents-2010/812-uniform-protection-of-privacy-data-breach-notification-report-2010>.

70 Industry Canada, *Principles for Electronic Authentication* (2004) at 18, online: Industry Canada <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/vwapj/authentication.pdf/$file/authentication.pdf>.

71 Privacy by Design, *supra* note 7.

72 In the United Nations *Model Law on Electronic Signatures*, *supra* note 26 at article 2 (definition), article 9 (rules of conduct) and article 10 (standards of trustworthiness).

73 *Ibid.* at article 10.

74 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*, 2012/0146 (COD) at articles 15–19, online: European Union Law <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:EN:PDF> [*Proposal for Trust Services*].

identification authority? Should it have special duties or special privileges because of its position as the representative of all the people?

The *Uniform Electronic Commerce Act* allows government to impose special restrictions — "information technology requirements" — on incoming electronic communications.[75] Its consent to such communications cannot be presumed. Government needs to protect its systems, and many of these communications do not arise under a contract or by agreement at all. Many people communicate with government because they have to. They may not be concerned about harmonizing with the government's system.

It may be noted that the European Union's proposal for a new regulation on electronic authentication privileges authentication methods used for accessing public services.[76] Moreover, the main users of secure electronic signatures in Europe (and possibly elsewhere) are governments communicating with the public, or with businesses. In Canada, many corporations are required to file their tax returns electronically.[77]

Do these measures create trust or resentment? Governments in Canada had privacy obligations well before the public sector — they are held to a higher standard. They pay a lot of attention to security, national and transactional. They are to a serious extent a model user of technology, though obviously not in all domains or for all purposes. Arguably that means that they are more trusted, and that the people expect conduct that will justify that trust. How the higher standards are reflected in legislation, however, is often unclear.

XII. CONCLUSIONS

We have seen that legislation is not the primary source of transactional security, that is to say commercially effective trust, in the electronic or in the offline world, because law tends to be one size that does not fit all. There are also limits to how "granular" (i.e. case-specific) legislation can be, but one finds so many shades and notions of identity, attributes, and authority, and everyone makes his/her/its own evaluation, i.e. judgment of what and who to trust. Risk tolerance varies. Data vary. Technology evolves. In Internet-speak, YMMV![78]

Even in the time I have been paying attention to these questions, there has been a notable progression in thinking about legislation. Backing up a few years, it is fair to say that from the mid-1980s through 2000, thoughts about what law reform was needed to deal with e-commerce progressively simplified. Less and less was thought needed to remove barriers, as demonstrated by the English Law Com-

---

75 *Uniform Electronic Commerce Act*, *supra* note 14. See for example paragraphs 8(b), 9(b), 10(b), 11(c).

76 *Proposal for Trust Services*, *supra* note 74 at article 6(1)(b).

77 Canada Revenue Agency, "Mandatory Internet Filing for T2 Corporation Tax Returns", online: Canada Revenue Agency <http://www.cra-arc.gc.ca/gncy/bdgt/2009/fqt2-eng.html>. Tax filers must use tax filing commercial software certified by the government and use approved transmission methods, to ensure security.

78 Your Mileage May Vary: you may have different results in your own analysis.

mission's conclusion that no law reform at all was needed to deal with electronic signatures.

However, it is arguable that the past decade has seen the evolution of a growing theme of regulation of systems. Maybe this is due to a growing concern about cybersecurity.

Legislation can be a useful source of system security. This is not so much by requiring such things as secure electronic signatures in crucial transactions, but by encouragement of transparency, effective dispute resolution, appropriate cybersecurity against outsiders (risk from complete outsiders rather than risk from another transactional party), and similar measures outside the actual transactions where individual commercial judgments of trust would apply. Everyone will have their own threat/risk analysis, and trust threshold.

It is important to consider in the analysis all of the sources of trust I mentioned at the outset, from personal morality through reputation to institutions (notably law) to technology. Enhancements to trust may draw on all of them in different degrees for different purposes. While one cannot legislate trust, one can nourish the conditions in which it will grow, and properly designed legislation has a role to play in that nutritional exercise.

In conclusion, it would appear that law reformers like me are not going to be put out of business, but our business should be changing its focus, at least if we are going to legislate the conditions for trust.