

8-1-2002

## Global TRECs: The Regulation of International Trade in Cyberspace

J. Steele

Follow this and additional works at: <https://digitalcommons.schulichlaw.dal.ca/cjlt>

---

### Recommended Citation

Steele, J. (2002) "Global TRECs: The Regulation of International Trade in Cyberspace," *Canadian Journal of Law and Technology*: Vol. 1 : No. 3 , Article 2.

Available at: <https://digitalcommons.schulichlaw.dal.ca/cjlt/vol1/iss3/2>

This Article is brought to you for free and open access by the Journals at Schulich Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Scholars. For more information, please contact [hannah.steeves@dal.ca](mailto:hannah.steeves@dal.ca).

# Global TRECs: The Regulation of International Trade in Cyberspace

J. Steele<sup>†</sup>

## Introduction

The regulation of international commerce over open computer networks, such as the Internet, is currently receiving considerable attention from both trading nations and international organizations alike. Initiatives underway are aimed at creating a more stable and predictable environment, so that electronic commerce (e-commerce) may realize its full potential. However, opinions differ as to how much regulation is both necessary and advisable.

The World Trade Organization (WTO) is uniquely positioned to deal with trade-related aspects of electronic commerce (“TRECs”) on an international scale, however such initiatives have been limited to date.<sup>1</sup> Other international institutions, notably the United Nations Commission on International Trade Law (UNCITRAL) and the Organisation for Economic Co-operation and Development (OECD), have been active in proposing model laws and other recommendations, which in turn have been adopted domestically by nations legislating in the area of electronic commerce. However, competing approaches to the regulation of electronic trade across national boundaries necessitate supranational oversight and harmonization of the growing assortment of laws being promulgated at national levels in an effort to keep pace with the many evolving facets of e-commerce.

This paper provides an overview of trade-related aspects of electronic commerce, and examines three approaches for regulating international trade in cyberspace. A model which integrates these approaches is then proposed, emphasizing private standards of self-regulation within a broader public framework of minimal background standards. A summary of potential areas of conflict between competing regulatory approaches follows, and the paper concludes that both the WTO and the OECD have important roles to play in the development of international consensus towards a harmonized framework for the regulation of global TRECs.

## Electronic Commerce

The Internet is the great facilitator of e-commerce, enabling a “complex web of commercial activities transacted on a global scale between an ever increasing number of participants, corporate and individual, known and unknown, on global open networks”.<sup>2</sup> Continued growth of the Internet is being driven by such factors as advances in computing power (the effect of Moore’s Law<sup>3</sup>); the development of a network “critical mass” (the effect of Metcalfe’s Law<sup>4</sup>); an expanding infrastructure with developments in broadband technology (widening the lanes on the information superhighway); the addition of new data paths from alternative communication formats such as wireless (adding more lanes to the information superhighway); and reductions in the cost of going online due to greater competition among Internet Service Providers (ISPs).

E-commerce is about doing business electronically, and in the process reducing barriers such as time and distance. Lower transaction costs, rapid communications, and streamlined processes are just a few of the advantages which the Internet offers for international business. However, perhaps the greatest advantage of e-commerce today, in comparison with pre-Internet forms of electronic commerce such as electronic data interchange (EDI), is the sheer number of available participants and the effect of Metcalfe’s Law:

For traditional electronic commerce, the network is a means to move data; for Internet electronic commerce, *the network is the market*.<sup>5</sup>

This unprecedented interconnectedness on a worldwide scale has the potential to revolutionize the nature and scope of international commerce in the 21st century.

The broadest definition of electronic commerce would include any electronically-enabled business activity or process, over “open” networks such as the Internet, “closed” networks such as EDI, and credit and

---

<sup>†</sup>LL.M., 2001, Osgoode Hall Law School. Member, Law Society of Upper Canada. The author writes in the areas of e-commerce, intellectual property, international business, and corporate governance matters.

debit card transactions.<sup>6</sup> Such an “inclusive” approach has been adopted by the WTO, which defines e-commerce as “the production, distribution, marketing, sale or delivery of goods and services by electronic means.”<sup>7</sup> However, e-commerce is often understood as referring more specifically to transactions conducted over the Internet. Such an approach is taken by this paper.

E-commerce involves three types of goods: (1) digital products sold and delivered electronically; (2) physical products sold online but delivered offline; and (3) “electronic deliverables”<sup>8</sup> — products which may be delivered in either a digital or a physical format (e.g., software, music, books, and videos). In addition to goods, the Internet readily lends itself to the delivery of services which may be digitized, and trade in online services (subject to domestic licensing requirements) includes such areas as financial services, investing, legal services, gaming, medical services, and education, to name a few.

The majority of electronic commerce today occurs between parties located within common national boundaries. However, online transactions are by their very nature unencumbered by geography, allowing digital products to cross borders largely unnoticed by authorities.<sup>9</sup> When combined with declining telecommunication costs due to increased competition among ISPs, a potent combination exists which will lead to increasingly greater use of the Internet for international business transactions in the future. However, the complexities of doing business internationally become magnified when combined with the legal uncertainties of conducting business over the Internet, complicating the task of regulators currently examining the trade-related aspects of electronic commerce.

## Legal Issues

E-commerce presents legal challenges involving aspects of both private and public law, and many of the issues involved are common to both domestic and international online transactions. While this paper focuses on the realm of private international law, many of the observations made are equally applicable to domestic e-commerce transactions.

The legal challenges presented by international e-commerce expose participants to a variety of risks. Governments have a vested interest in minimizing these risks so that international online commerce may grow to realize its full potential, unencumbered by legal uncertainty. There is no central authority which oversees international e-commerce, which has largely gone unregulated as governments and institutions continue to study its nature and economic ramifications. Nevertheless, the question of *whether* to regulate the Internet has largely been supplanted by questions concerning how best to do so, which are currently under consideration by a multitude of stakeholders and interested parties.

The rapid growth of electronic commerce has resulted in greater numbers of goods and services being traded across national boundaries by an ever increasing array of businesses and consumers. By venturing into the borderless world of the Internet, many are participating in international commerce — sometimes unwittingly — for the first time. In so doing, participants become subject to a complex web of rules, regulations, restrictions and special arrangements, contained in an assortment of domestic laws, bi-lateral and regional trading arrangements, and multilateral treaties. Furthermore, a variety of novel legal issues come into play which are unique to the Internet.

All of these factors create an environment of legal uncertainty which is of concern to both participants and regulators alike. This uncertainty has a number of implications. First and foremost is the need for laws which bring more predictability to the process, by answering fundamental questions such as: (1) what makes an electronic contract binding and enforceable; (2) where does jurisdiction lie when parties to an electronic transaction are in different countries; and (3) what dispute resolution mechanisms are practical where parties may be separated by thousands of miles, and the value of the item in dispute may be small?

However, legislation alone is not a complete solution, since e-commerce is changing as rapidly as the technology upon which it relies, and legislators cannot hope to match the rate of change in computing power predicted by Moore’s Law. As a result, industry self-regulation necessarily must play a large role in the field of e-commerce, if for no other reason than commercial self-interest.<sup>10</sup> In addition, the range of approaches under consideration (legislative or self-regulative) by trading nations must be harmonized on a supranational basis, otherwise the risk of further legal uncertainty will plague international e-commerce transactions in the future.

The types of legal issues which can arise when e-commerce is conducted across national boundaries include:

1. **Jurisdiction:** What forum may assert jurisdiction over the parties and their actions, both for matters of public international law (e.g., regulation) and private international law (e.g., dispute resolution)?
2. **WTO Rules:** How are the transacted items classified under WTO trade agreements (e.g., as either a “good” or a “service”), how does this affect tariff rates and market access, and does the classification change when the item is delivered online (e.g., a digital book)?
3. **Online Contracting:** Have the formal requirements for creating a binding contract been met, and if so, is it enforceable in the same manner as a traditional contract?

4. **Digital Signatures/Certification Authorities:** Is an electronic signature sufficient to create a binding contract, and how can a party's true identity be verified in the absence of a handwritten signature?
5. **Encryption:** What security level of encryption is available for parties to Internet transactions, and should any regulatory authorities have access to the code-breaking technology?
6. **Payment Systems:** If new forms of "digital cash"<sup>11</sup> are used, who is responsible for regulating them, and how should risk be apportioned between buyer and seller?
7. **Consumer Protection:** How should regulators protect consumers in the impersonal world of cyberspace, and how should regulations be harmonized with traditional consumer protection laws?
8. **Taxation:** To what degree can states collect sales taxes and duties arising from international e-commerce transactions, without harming the growth of e-commerce or distorting trade-related aspects of electronic commerce?
9. **Privacy:** How should personal information be protected once released into cyberspace, or when databases become accessible through the Internet, and to what extent should parties be able to shield their true identity?
10. **Intellectual Property:** How can intellectual property be adequately protected in an environment which permits easy duplication and near instantaneous transmission around the world, and how can laws be harmonized across national boundaries?
11. **Dispute Resolution:** What alternatives to traditional commercial dispute resolution are available for parties who may be separated by enormous distances while entering into transactions of relatively small value?

All of these cyberlaw issues, with the exception of classification under the WTO agreements and jurisdiction,<sup>12</sup> may also arise in the context of domestic e-commerce transactions. As such, legislatures around the world are scrambling to pass laws dealing with many of these issues, which in turn makes international harmonization all the more crucial.

International e-commerce transactions differ from traditional international business transactions in several key regards: (1) the parties often have no underlying business relationship; (2) the contract is usually made "on the fly" using "clickwrap"<sup>13</sup> or other types of cyber-agreements; and (3) the value of the goods or services may be so nominal as to preclude the buyer from resorting to formal dispute resolution mechanisms. The ease of doing business over the Internet is making this type of scenario more commonplace every day, accentu-

ating the need for a uniform approach for dealing with the broad range of legal issues which impact on international e-commerce.<sup>14</sup>

## Internet Regulation

Various schools of thought exist concerning regulation of the Internet. In the area of trade-related aspects of electronic commerce, this paper proposes an integrated model which combines elements of several different approaches.

### Three Approaches

Debate among legal scholars has switched from the question of *whether* to regulate the Internet,<sup>15</sup> to *how* best to do so. Assuming that such regulation is possible, the question has several dimensions in connection with electronic commerce, since Internet transactions may be either domestic or international in scope, and may involve aspects of both public and private law.<sup>16</sup>

The different visions for regulating Internet activity have been categorized into three general schools of thought.<sup>17</sup> When applied to the regulation of trade-related aspects of electronic commerce, the following three approaches are notable:

#### Traditional legal regulation:

- "top-down" public ordering<sup>18</sup>
- hierarchical rules
- control through state agencies and international institutions
- hierarchal rules
- safe harbor arrangements where necessary
- analogies to the law of the sea, and the law of outer space<sup>19</sup>

#### Technological regulation:<sup>20</sup>

- technological solutions to legal issues
- "digital libertarianism"<sup>21</sup>
- *Lex Informatica*<sup>22</sup>
- digital watermarking for copyright protection
- digital signatures to provide certainty about a party's identity
- hard encryption technology to shield privacy for legitimate purposes

#### Commercial self-regulation:

- "bottom-up" private ordering
- spontaneous coordination
- market driven codes of conduct and enforcement mechanisms
- digital *Lex Mercatoria*<sup>23</sup>

### Traditional Regulation

The traditional view of regulation holds that cyberspace should be publicly regulated by a “top-down” approach of hierarchical rules and arrangements, and that the regulation of commercial transactions in cyberspace is no different than the regulation of other types of transborder transactions. Cooperation and coordination at the international level are considered necessary for the development of a global framework which advances desirable social policy objectives. The view holds that international agreements should be negotiated, with prescriptive requirements which governments would be obliged to implement, which in turn would be administered through appropriate international institutions such as the WTO.

Different models have been considered for applying legal regulation to the Internet, including analogies to the law of the sea and the law of outer space, although neither approach would be suitable for e-commerce, given their primary focus on intergovernmental affairs. The approach taken by the European Union (EU) is most often characterized as falling into this category, however as with the other approaches, accurate characterization is a matter of degree. Categorizing approaches as being either pro-regulatory or anti-regulatory is too simplistic, and fails to take into account the balancing of policy options which is taking place with virtually every approach to regulating the Internet.

A review of the following principles enunciated in *A European Initiative in Electronic Commerce*<sup>24</sup> reveals the balancing of considerations evident in the EU approach. However, in contrast with the U.S. approach, the EU scheme is much more in favour of public regulation — when necessary:

1. **No regulation for regulation’s sake:** The freedom of electronic commerce may in many cases be effectively achieved through the mutual recognition of national rules and appropriate self-regulatory codes. Any legislation should impose the fewest possible burdens on the market, and keep pace with market developments.
2. **Based on all single market freedoms:** Equal weight must be given to all freedoms offered by the single market, i.e., the realization of the free movement of goods, persons, services and capital together with the freedom of establishment. Only in this way may the crucial objectives of coherence, predictability and operational simplicity be achieved.
3. **Taking into account business realities:** In many cases, legislation will not be necessary to confront actual or potential problems. Where necessary, legislation must seek to facilitate operations throughout the commercial chain, since it makes no sense to remove barriers in one part of the chain while leaving others untouched.

4. **Meeting general interest objectives:** A single market for electronic commerce will not develop without the effective safeguarding of recognized general interest objectives, such as privacy or consumer protection, and other public interests such as wide accessibility to networks. Without such protection, there is a real risk that national regulatory borders will remain in place as individual member states seek to safeguard the legitimate concerns of their citizens.

### Digital Libertarianism

The approach described as “digital libertarianism” holds that technological capabilities and system design choices are sufficient to impose rules on those taking part in Internet transactions.<sup>25</sup> As such, policymakers should develop an understanding of the “rule-making power” of technology, as part of any regulatory framework planned for electronic commerce.<sup>26</sup> In effect, the legal regime is hardwired or embedded right into the technology itself.<sup>27</sup> This idea of a “*lex informatica*”<sup>28</sup> for e-commerce may be contrasted with traditional legal regulation, as follows:

	Legal Regulation	Lex Informatica
Framework	Law	Architecture standards
Jurisdiction	Physical Territory	Network
Content	Statutory/Court Expression	Technical Capabilities Customary Practice
Source	State	Technologists
Customized Rules	Contract	Configuration
Customization Process	Low Cost Moderate cost standard form High cost negotiation	Off-the-shelf configuration Installable configuration User choice
Primary Enforcement	Court	Automated, self-execution

Table 1: *Features of Lex Informatica, Rule Regimes*<sup>29</sup>

Most approaches to Internet regulation focus on the notions of traditional regulation (or “public ordering”) and private self-regulation (or “private ordering”), and the idea of digital libertarianism as a comprehensive approach to Internet regulation *per se* is viewed by most as unsuitable. Nevertheless, in certain areas of Internet regulation — such as content restrictions, the treatment of personal information, and the protection of intellectual property — technological solutions may provide the sort of flexible and customizable systems needed to successfully regulate across national boundaries and policy differences.<sup>30</sup>

### Private Ordering

The “private ordering” approach favours market-driven codes of conduct and enforcement mechanisms, with minimal government regulation, as the most effective means for fostering the growth of electronic commerce. Such a “bottom-up” approach is similar to the *Lex Mercatoria* (Law Merchant), which developed among international traders during the Middle Ages to codify their customs and commercial practices, independent of local sovereign law.<sup>31</sup>

The most prominent advocate of this approach is the United States. *A Framework for Global Electronic Commerce*,<sup>32</sup> which gave the first indication of American policy in the area of international e-commerce, sets out the following five guiding principles:

1. **The private sector should lead:** Innovation, the expansion of services and participants, and the lowering of transaction costs will all depend on the Internet remaining a *market-driven* arena.
2. **No undue restrictions:** Governments should refrain from imposing new and unnecessary regulations, bureaucratic procedures, or new taxes and tariffs on commercial activities which occur via the Internet. Impeding commercial activities over the Internet will unnecessarily limit the availability, and raise the prices, of products and services to consumers the world over, and will distort development of the electronic marketplace.
3. **A predictable, consistent, and minimalist legal environment:** In some areas, government agreements will be necessary to facilitate electronic commerce. In these cases, governments should establish a predictable and simple legal environment based on a decentralized, contractual model of law *rather than a model based on top-down regulation*.
4. **Recognition of the unique qualities of the Internet:** Governments should recognize that the explosive success of the Internet can be attributed in part to its decentralized nature and *bottom-up governance*. Governments should also realize that the Internet’s unique structure poses significant logistical and technological challenges to current regulatory models, and should tailor their policies accordingly. As such, governments should encourage the evolution of industry self-regulation, and should support the efforts of private sector organizations to develop mechanisms which will facilitate the successful operation of the Internet.
5. **Facilitated on an international basis:** While recognizing differences between national legal systems, the framework supporting commercial transactions over the Internet should be governed by a set of consistent legal principles,

regardless of the country in which the buyer or seller resides.

While the private ordering approach has been gaining adherents, it remains to be seen how much businesses will voluntarily self-regulate in areas where governmental coercion is absent, as summed up in the following observation by John Dryden, Head of Information, Computer and Communications Policy for the OECD:

In fact, there is now broad consensus among the Member countries that governments should encourage the private sector to meet public interest goals where possible through codes of conduct, model contracts, guidelines, dispute resolution mechanisms and enforcement mechanisms developed by the private sector itself . . . The key question is: *are they effective?*<sup>33</sup>

## The Right Mix

### Considerations

The foregoing three approaches to regulating e-commerce over the Internet need not be exclusionary. While some regulatory models currently proposed clearly favour one approach over the others, most models recognize that a degree of co-regulation between the private sector and public institutions is not only desirable, but inevitable, with differences arising in the level of prominence enjoyed by each approach. The key issue for policymakers is determining the appropriate mix in order to achieve their regulatory goals, as illustrated by the following quote:

. . . discussions at the OECD these days tend to focus not so much on the question of “regulation” or “self-regulation”, but rather, if a mix of the two is needed, how to get the mix right. In other words, they are complementary approaches. “Co-regulation” or “integrated approach” are just two of several expressions used to try to capture the concept. The former term generally is used to refer to a situation where private and public sector partners co-operate in shaping and implementing the regulatory framework, whereas the latter refers more to the process of making the interface between regulation and self-regulation as seamless and as coherent as possible.<sup>34</sup>

The regulatory model of choice is inextricably linked to the activity being regulated. For example, even the most ardent proponents of Internet self-regulation recognize the need for traditional top-down regulation in such sensitive public policy areas as health care, finance, and content accessible by children, as well as in such traditional public law fields as criminal matters and the taxation of commerce. As such, a key consideration for policymakers is how best to combine the most suitable aspects of each approach, in order to achieve an optimal mix of ingredients which will meet their objectives in the area of international e-commerce.

The regulation of international commerce has traditionally involved a mixture of top-down regulation and business self-regulation, with government regulation often used to codify what have become generally

accepted business practices.<sup>35</sup> Two examples of hybrid approaches in the area of electronic commerce involve the safe harbor arrangement between the U.S. and EU for the protection of personal information, and the regulation of Internet domain names by the non-profit Internet Corporation for Assigned Names and Numbers (ICANN).<sup>36</sup> In the former arrangement, private companies self-certify to the U.S. Federal Trade Commission that their procedures comply with EU privacy standards,<sup>37</sup> while in the latter arrangement, ICANN privately manages the global Internet domain name system in a manner “that allows for the development of robust competition in the management of Internet names and addresses”.<sup>38</sup>

Whichever mix of approaches is adopted, caution should be exercised in favour of less rather than more regulation, due to the fact that e-commerce is still in an “embryonic stage” and “the technology and market dynamics are still casting its basic shape”.<sup>39</sup>

In addition to successfully combining different approaches to regulation, other considerations include the need for international harmonization, as well as the extent to which technology may be used to regulate international e-commerce. High on the lists of regulators are the objectives of stimulating global growth through creating an environment of security and predictability, and building consensus towards the harmonization of laws which will minimize barriers to electronic trade. Technological regulation is also bound to play an increasingly greater role in the future, due to continuing advances in communication technologies and computing capabilities as predicted by Moore’s Law.

### Suggested Model

As noted earlier, no global regulatory framework for e-commerce currently exists, nor are we close to such a framework being implemented any time soon. In the words of Dryden:

Certainly, global consensus that Internet regulation in the wide sense is desirable is not even on the horizon. It is therefore clear why self-regulatory options are so appealing as a complement to national law or European directives.<sup>40</sup>

Stakeholders are well aware of the uncertainties inherent in conducting business over the Internet, and of the necessity for developing a more secure and predictable environment in which e-commerce transactions may take place. In order to effectively address the issues noted earlier, international harmonization of differing approaches to regulation is crucial, and model frameworks such as the one proposed herein may prove useful for future discussions.

The underlying rationale for any regulatory model are the particular objectives which it serves. The objectives most often cited in the realm of global e-commerce are as follows:

- **to stimulate economic growth;**
- **to enhance user trust;**

- **to provide greater predictability;**
- **to encourage legal harmonization** (i.e., the consistent treatment of legal issues across borders);
- **to foster regulatory transparency** (i.e., all participants having full access to information about the rules and regulations, so that decisions may be based on accurate assessments of market opportunities);
- **to guarantee technical neutrality** (i.e., treating all technologies equally, in areas such as digital signatures and encryption, to foster competition and innovation);
- **to ensure non-discrimination** (i.e., avoiding distortions to trade by ensuring that e-commerce and conventional commerce are treated equally in areas such as taxation and tariffs).

With these objectives in mind, it is suggested that a framework for the regulation of international electronic commerce should incorporate the following principles, within an integrated model as shown in Figure 1:

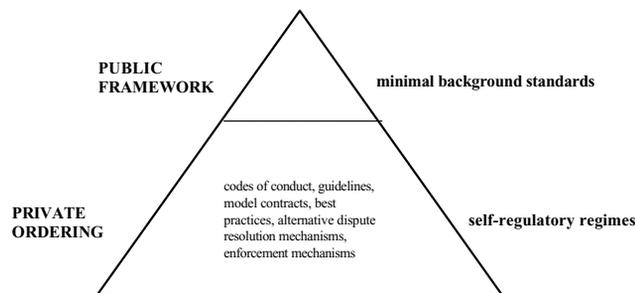


Figure 1: *Global TRECs “Integrated Model” Regulatory Framework*

1. **Global framework of minimal background standards:** a basic framework which establishes judicious and proportionate public policy limits and a stable international legal environment;
2. **Market-driven private ordering regimes:** encouragement for business to adopt effective self-regulatory programs with their own distinctive rules and dispute resolution mechanisms, within the global framework developed by policymakers;
3. **International coordination:** global harmonization of the government policies, legal regulations, and business codes of conduct which impact upon electronic commerce;
4. **Cooperative development:** the promotion and facilitation of input from the private sector; forums for public-private dialogue to determine issues and priorities; structures for policy research and analysis; workshops to educate the public

and business; and mechanisms for multilateral dialogue;

5. **Monitoring and oversight:** monitoring by authorities to determine whether self-regulatory mechanisms are meeting public interest goals in such areas as personal privacy and consumer protection, and whether more stringent public regulation is required where such programs may be falling short; legal sanctions for non-compliance;
6. **Flexible approaches:** recognition that different approaches may be needed for countries at different stages of development;
7. **Tax neutrality:** ensuring that electronic commerce receives neutral tax treatment which is no different than the treatment accorded conventional commercial transactions, and is also consistent with established internationally-accepted practices.

This form of integrated regulatory model, emphasizing private sector ordering within a broader public policy framework based on minimum background standards, is suggested because it would relieve regulators of the near impossible task of keeping pace with the rapid rate of change which e-commerce is currently undergoing.

Furthermore, a suitable regulatory model would need to be flexible enough to accommodate the different approaches which regulators will take, depending on the area of law involved. Whereas general principles may suffice in dealing with certain matters, others would require the development of new international instruments in order to effectively deal with the issues involved.

For example, the majority of issues concerning electronic commerce and intellectual property appear to be well-served through treaties administered by the World Intellectual Property Organization (WIPO),<sup>41</sup> whereas questions surrounding the issue of jurisdiction in cyberspace are in serious need of a coordinated international response.<sup>42</sup> Similarly, although progress is being made in adapting the principle of “functional equivalency” taken by the UNCITRAL Model Law on Electronic Commerce<sup>43</sup> to the domestic legislation of countries dealing with issues involving electronic contracts, much remains to be done in developing cost-effective and timely mechanisms for online dispute resolution.

A related question involves the extent to which international organizations should play a pre-eminent role in coordinating efforts to harmonize different approaches for dealing with the legal challenges presented by electronic commerce. The work of the OECD in this area, involving the analysis and development of future policy concerning e-commerce, has been extremely valuable. However, the OECD is not designed to administer or enforce the policies of international commerce since authority rests with the WTO in trade-

related matters. The WTO, on the other hand, is opposed to the creation of any new institutions for the regulation of electronic commerce.<sup>44</sup> It would therefore appear that the WTO will play a dominant role in any future framework, although certain specific areas such as intellectual property and jurisdiction would be best overseen by organizations with special expertise in those areas, such as WIPO and the Hague Conference on Private International Law.<sup>45</sup> Unfortunately, until a new round of trade negotiations is agreed upon, action by the WTO will necessarily be limited, leaving the OECD as perhaps the most suitable venue for pursuing initiatives for the harmonization of differing approaches towards regulating international electronic commerce.

Furthermore, bilateral and regional dialogue should be encouraged outside of the WTO and OECD frameworks. When conflicting approaches threaten to create new barriers to electronic commerce, such a dialogue may go a long way towards diverting trade disputes and helping to manage those conflicts which may arise.

## Managing Conflicts

Notable differences exist in the approaches to regulation taken by the two largest e-commerce trading regions — the United States, and the European Union. However, conflicts arising from such differences are far from unmanageable, as evidenced by the U.S.–EU “safe harbor” arrangement, dealing with personal data privacy.<sup>46</sup> In addition, there are clearly more similarities than differences between the approaches taken by the U.S. and the EU towards the regulation of electronic commerce.

Nevertheless, a review of policy documents<sup>47</sup> and public statements reveals the following key differences, which could lead to electronic trade disputes in the future if not properly managed:

1. **Classification of e-commerce under the WTO agreements:** The EU takes the position that e-commerce transactions should be treated as “services”, whereas the U.S. believes that a decision on classification should be deferred until the effect on market access and other trade rights can be studied in greater detail.<sup>48</sup>
2. **Privacy and the protection of personal data:** The EU has adopted a top down regulatory approach to the protection of personal data, whereas the U.S. has opted for industry self-regulation. However, the U.S. position is moving towards a combination of the two approaches, due to limited compliance by business.<sup>49</sup> As previously mentioned, a “safe harbor” agreement has been concluded which now allows U.S. companies to self-certify compliance with the privacy principles set out in the EU *Data Protection Directive* of 1998.

3. **Use and transfer of strong encryption technology:** The U.S. has in the past been opposed to the export of strong encryption technology,<sup>50</sup> whereas the EU favours the availability of such technology, in order to facilitate greater protection when using open networks such as the Internet.<sup>51</sup> This is in marked contrast to the general anti-regulatory position taken by the U.S. in e-commerce matters. The Americans have been very active in trying to control the spread of strong encryption technologies, although such efforts run counter to initiatives to enhance consumer confidence in electronic commerce. Ironically, the recent easing of U.S. export restrictions has come about not from a shift in policy, but due to the improved code-breaking capabilities of the U.S. National Information Service.<sup>52</sup>
4. **Digital signatures:** Differences exist both in technology and in the legal definitions used for dealing with electronic signatures;<sup>53</sup> differences which could “limit certain transactions or hinder innovation”.<sup>54</sup>
5. **Domain names:** The EU has been opposed to the manner in which the Internet domain naming system was privatized under ICANN in 1998, when the U.S. government relinquished its oversight of the system.
6. **Industry self-regulation:** The term “industry self-regulation” has different meanings when used in U.S. and EU policy documents, particularly in the areas of standardization, privacy, and consumer protection.<sup>55</sup>
7. **Legal environment:** U.S. and EU models of what constitutes a “minimalist legal environment” differ substantially.<sup>56</sup>
8. **Specific sectors:** Different approaches exist, to varying degrees, in the following sectors: consumer protection, intellectual property protection, infrastructure, security, and e-payments.<sup>57</sup>
9. **Taxation:** The EU favours a value-added tax on Internet transactions, whereas the U.S. is in favour of the Internet remaining a tax-free zone, at least for the time being.

These differences in approach may, at the very least, add to the environment of unpredictability which surrounds international e-commerce, and at worst, could lead to the creation of barriers to electronic trade. Therefore, the effective management of such differences is crucial to the future stability and growth of international e-commerce. Towards that end, the following techniques are already being employed in order to provide an “early warning” system<sup>58</sup> for identifying differences, which may then form the basis for negotiations before serious disputes arise:

- general bilateral forums for maintaining an ongoing dialogue, such as the United States Mission to the European Union;<sup>59</sup>
- special workshops between experts from both sides, to identify key issues and work towards common objectives, such as the Digital Commerce Workshop held in Brussels;<sup>60</sup>
- plurilateral forums, such as the WTO, the OECD, and meetings of the G8 economic powers; and
- safe harbor arrangements, when harmonization of different approaches is not possible.

While such a spectrum of techniques may be effective in reducing the number of disputes requiring recourse to formal dispute resolution mechanisms (such as the system for trade-related disputes under the WTO agreements), they are still not a substitute for a coordinated and harmonized model which would comprehensively deal with the international trade-related aspects of electronic commerce.

## Conclusion

Electronic commerce and the Internet have significantly expanded international trading opportunities, giving rise to a borderless world in which digital goods and services may be delivered to virtually any point on the globe, without regard to distance or jurisdiction. At the same time, as an open communications system readily accessible by millions, the Internet presents serious challenges both for those engaged in e-commerce, and for the regulators considering how best to address the novel issues involved.

Participants in e-commerce transactions require greater security and predictability, and many are looking to governments to provide legislation which will address their concerns, and will provide them with greater confidence when transacting online. However, what remains undecided is the extent to which regulation is desirable and necessary, in order to unlock the full potential of global e-commerce. Furthermore, in light of the different approaches to regulation noted herein, it remains to be seen whether international consensus towards a single harmonized approach will be possible, or whether an assortment of safe harbour arrangements will be necessary in order to fill the gaps.

The current state of affairs may be expressed as “a spectrum of views, defined at one end by a policy of light-handed facilitation, and at the other by a comprehensive regulatory and licensing regime, covering the conduct of certification authorities and the application of technical standards.”<sup>61</sup> Working against the comprehensive regulatory approach is the accelerating rate of

technological change predicted by Moore's Law, and the exponential utility of wide-ranging communication networks as predicted by Metcalfe's Law, making top-down regulation an impractical policy *per se* for dealing with the majority of issues.

Governments are therefore facing serious policy challenges in determining the right mix of public and private regulation for dealing with trade-related aspects of electronic commerce. A coordinated international approach is vital, and both the OECD and the WTO have important roles to play in the development and implementation of a harmonized approach. The stakes are high, and decisions made over the coming years will have long-lasting consequences for generations to come.

This paper has suggested that the regulatory issues identified may be dealt with through an integrated model which emphasizes private standards of self-regulation within a broader public framework of minimal background standards. However, this approach comes with one caveat: in order for private ordering to play a dominant role, self-regulation must be both meaningful and effective, otherwise more active regulation by public authorities would become necessary.

The success of self-regulation will be dependent upon mechanisms which ensure compliance by threatening enforcement, and through adequate monitoring to ensure that self-regulatory regimes are working. In addition, private ordering will need to be "linked to broadly accepted norms for privacy protection, consumer protection, and respect for international property"<sup>62</sup> in order to satisfy minimum public background standards. It is submitted that an integrated regulatory model along the lines suggested herein would go a long way towards

creating a more predictable and stable environment in which international e-commerce could flourish, without the hindrance of excessive government regulation.

## References:

"Data Encryption Standard." searchSecurity.com, nd. <[http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci213893,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html)>

"Free Trade Area of the Americas (FTAA)." *Report with Recommendations to Ministers*, Joint Committee of Foreign Experts on Electronic Commerce. 1 September 1999. <[http://www.ftaa-alca.org/SPCOMM/COMMEC\\_E.ASP#pubs](http://www.ftaa-alca.org/SPCOMM/COMMEC_E.ASP#pubs)>

"Internet may need new cyber-borders, says U.S. legal body." Yahoo! News (UK & Ireland), 17 July 2000. <<http://uk.news.yahoo.com/000717/91/adbs1.html>>

Canada, Government. "Global Electronic Commerce," *Consultations with Canadians*, Ottawa: Department of Foreign Affairs and International Trade, June 1999, online: Department of Foreign Affairs and International Trade. <<http://www.dfait-maeci.gc.ca/tna-nac/discussion/ecom2-e.asp>>

Ferguson, Keith. *The World Trade Organization (WTO) and its Multilateral Trade Agreements (GATT, GATS, TRIPS, TRIMS, etc.)*. Peninsula Peace and Justice Center (PPJC), Palo Alto, online: Peninsula Peace and Justice Center. <[http://www.peacecenter.com/issues/global/gl\\_wto.html](http://www.peacecenter.com/issues/global/gl_wto.html)>

Geist, Michael. *Internet Law in Canada* (North York: Captus, 2000).

Headstar Ltd. *Global Regulation of Electronic Commerce*. Brighton: 2000, online: Headstar. <<http://www.headstar.com/research.html>>

World Trade Organization. *A Summary of the Final Act of the Uruguay Round*. Geneva: WTO, nd, online: World Trade Organization <[http://www.wto.org/wto/english/docs\\_e/legal\\_e/ursum\\_e.htm#Agreement](http://www.wto.org/wto/english/docs_e/legal_e/ursum_e.htm#Agreement)>

## Notes:

<sup>1</sup> On May 20, 1998, Members of the WTO adopted a declaration on global electronic commerce during their second Ministerial Conference in Geneva. The declaration directed the General Council to establish a work programme to examine all trade-related issues arising from electronic commerce. The work program was adopted by the WTO General Council on September 25, 1998. Recently, the Fourth (Doha) Ministerial in November 2001 endorsed the work which has been done by the work programme, and declared that WTO members maintain their current practice of not imposing customs duties on electronic transmissions, pending further discussions at the Fifth Ministerial Conference, to be held in Mexico in 2003, online: World Trade Organization, <[http://www.wto.org/tratop\\_e/ecom\\_e/ecom\\_briefnote\\_e.htm](http://www.wto.org/tratop_e/ecom_e/ecom_briefnote_e.htm)>

<sup>2</sup> European Commission, *A European Initiative in Electronic Commerce*, EC document COM97 (157), 15 April 1997, online: <<http://www.cordis.lu/esprit/src/ecomcom1.htm>>

<sup>3</sup> Gordon Moore, co-founder of Intel, observed in 1965 that the growth in semiconductor performance doubles roughly every 18 months. This prediction has proven to be remarkably accurate, and has led to the exponential growth of computing power over a relatively short period of time. An interesting example of such exponential growth is given by Ray Kurzweil in *The Age of Spiritual Machines* (New York: Viking, 1999), where the following analogy is used for advances in neuronal processing power (i.e., brainpower) over time, involving a \$1,000 personal computer:

2000 dragonfly

2008 mouse

2018 human

2028 small village (1,000 people)

2048 entire planet (10 billion people).

<sup>4</sup> Bob Metcalfe, founder of 3Com and inventor of the Ethernet protocol, postulated that the utility or usefulness of a network increases by the square of the number of people using it. The outcome is exponential growth in the value of a communications network like the Internet, and in the resulting productivity and economic gains which may be achieved.

<sup>5</sup> See *supra* note 2 [emphasis added].

<sup>6</sup> "Open" networks permit all network users to interconnect with basic network functions on an equal-access basis, whereas "closed" networks are centrally controlled and monitored.

<sup>7</sup> WTO, *Work Programme on Electronic Commerce*. WTO document WT/L/274 of 25 September 1998, online: World Trade Organization, <[http://www.wto.org/english/tratop\\_e/ecom\\_e/wkprog\\_e.htm](http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm)>

<sup>8</sup> Canada, Department of Foreign Affairs and International Trade, *Global Electronic Commerce* (June 1999), online: Department of Foreign Affairs and International Trade, <<http://www.dfait-maeci.gc.ca/tna-nac/discussion/ecom2-e.asp>>

<sup>9</sup> Even if it were technologically feasible to erect border controls, for example through the use of firewalls to monitor the flow of products delivered electronically, the creation of such "electronic borders" would have trade-diverting effects that could outweigh any tariff or other gains to be realized.

<sup>10</sup> It is worth noting that the phenomenal growth of e-commerce over the Internet has occurred notwithstanding the legal uncertainties which exist. This should be a signal to regulators that a "soft law" approach, entailing industry codes of conduct and "best practices" guidelines, may be the

- most suitable model for regulating e-commerce, at least until such time as it can be demonstrated that such an approach is insufficient, or that a lack of legal regulation is impacting negatively on the growth of e-commerce.
- <sup>11</sup> Wikipedia.com defines "digital cash" as: "A system that allows a person to pay for goods or services by transmitting a number from one computer to another. Like the serial numbers on real dollar bills, the digital cash numbers are unique ... and represents a specified sum of real money ... when a digital cash amount is sent from a buyer to a vendor, there is no way to obtain information about the buyer. This is one of the key differences between digital cash and credit card systems." Online: <[http://www.wikipedia.com/TERM/d/digital\\_cash.html](http://www.wikipedia.com/TERM/d/digital_cash.html)>.
- <sup>12</sup> Jurisdiction may also be an issue with certain types of domestic e-commerce transactions (e.g., inter-state, or inter-provincial transactions), however it becomes significantly more complicated when international transactions are involved, due to the absence of a common national authority or legal framework.
- <sup>13</sup> "The clickwrap contract is merely a contract by which terms are assented to through clicking an 'I Agree' button. As a result of the implementation of many Web interfaces, it is frequently difficult or even impossible to ascertain the terms of clickwrap contracts. Parallels are often drawn to the software industry and its shrinkwrap contracting practices, in which the terms of the software licence are only available to the purchaser after they open the purchased product." See M. Geist, *Internet Law in Canada* (North York: Captus, 2000) at 474.
- <sup>14</sup> It is important to note, however, the distinctions which exist between developed and developing nations. Whereas developed nations are more concerned with issues such as privacy, taxation, and consumer protection, developing nations are more concerned with matters such as affordable access to internet service providers, improved access speed, and the amount of local and native language content. See WTO, "Seminar on Electronic Commerce and Development", *supra* note 3 at 12.
- <sup>15</sup> See, for example, John Perry Barlow's *Declaration of the Independence of Cyberspace*, advocating the sovereign independence of cyberspace as a new world where traditional legal concepts have no place. Online: Electronic Frontier Foundation, <<http://www.eff.org/~barlow/Declaration-Final.html>>. For an interesting rebuttal to the "cyberspace is a place" proponents, see Jack Goldsmith, "Against Cyberanarchy", (1998) 65 University of Chicago Law Review 1199, online: The Berkman Center for Internet & Society at Harvard Law School, <<http://eon.law.harvard.edu/property00/jurisdiction/cyberanarchyedit.html>>.
- <sup>16</sup> Private law issues include matters such as contract formation, payment systems, intellectual property, consumer protection, and dispute resolution. Public law issues would include the regulation of trade and competition, criminal law, and taxation matters.
- <sup>17</sup> Michael Geist in *Internet Law in Canada*, *supra* note 13, observes that there are three visions for regulating Internet activity, which may be generally categorized as: (1) the "cyberspace is a place" approach, arguing that cyberspace is a place separate from the physical world, requiring its own laws and placing significant limitations on traditional regulatory approaches — see David Post and David R. Johnson, "Law and Borders — The Rise of Law in Cyberspace" (1996) 48:5 Stan. L. Rev. 1367; (2) the traditional functional approach, which argues that existing law can readily be applied to cyberspace — see Jack Goldsmith, "Against Cyberanarchy" (1998) 65 U. Chi. L. Rev. 1199; and (3) the "software code as law" approach, arguing that technology is rapidly replacing law as the regulator of choice — see for example, Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999); Joel Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules Through Technology" (1998) 76 Texas L. Rev. 553; and James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors" (1997) 66 U Cin L Rev. 177.
- <sup>18</sup> M. Radin and R. Wagner, "The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace," (1999) 73 Chicago-Kent Law Review, online: Social Science Research Network Electronic Library, <[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=162668](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=162668)>.
- <sup>19</sup> The regulatory models provided by law of the sea, and the law of outer space, are only starting points for discussions about international regulation of the Internet and e-commerce, since they deal with state actors rather than private entities, and are therefore unsuitable as models for the regulation of private activities over the Internet. See Shalini Venturelli, "Inventing E-Regulation in the EU & US," *Regulating the Internet: EU and US Perspectives*, 28 April 2000, online: Center for Internet Studies at the University of Washington, <<http://www.cis.washington.edu/webvision/eunetconf/>>.
- <sup>20</sup> The "software code as law" approach. See Geist, *supra* note 13 at 38–39; and James Boyle, "Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors," 66 U Cin L Rev. 177 (1997), online: Washington College of Law, <<http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm>>.
- <sup>21</sup> Boyle, *ibid*.
- <sup>22</sup> Joel Reidenberg, "Lex Informatica: The Formulation of Information Policy Through Technology," 76 Texas L. Rev. 553 (1998), online: Prof. Joel R. Reidenberg personal webpage, <[http://reidenberghome.sprynet.com/lex\\_informatica.pdf](http://reidenberghome.sprynet.com/lex_informatica.pdf)>.
- <sup>23</sup> "The Law Merchant", or the unwritten customary trading practices of international merchants, as developed from the time of the Middle Ages or earlier, and later codified into commercial laws by national legislatures. See, for example, Helen West Bradley, "History of the Law Merchant", *A Student's Course in Legal History* (1929), online: Nick Szabo's Essays and White Papers webpage, <<http://szabo.best.vwh.net/lex.html>>.
- <sup>24</sup> See *supra* note 2.
- <sup>25</sup> Reidenberg, *supra* note 22, at 575.
- <sup>26</sup> *Ibid* at 555.
- <sup>27</sup> Boyle, *supra* note 20.
- <sup>28</sup> Reidenberg, *supra* note 22.
- <sup>29</sup> *Ibid* at 566.
- <sup>30</sup> *Ibid* at 556.
- <sup>31</sup> *Ibid* at 553.
- <sup>32</sup> United States, *A Framework for Global Electronic Commerce*, The White House, 1 July 1997, online: Communications Media Center at New York Law School, <<http://www.cmcnyls.edu/Papers/WHGI-Fra.htm>>.
- <sup>33</sup> John Dryden, "The Work of the OECD on Electronic Commerce," June 2000, at 5 [emphasis added], online: Organisation for Economic Co-operation and Development, <[http://www1.oecd.org/subject/e\\_commerce/Ottawa\\_speech.pdf](http://www1.oecd.org/subject/e_commerce/Ottawa_speech.pdf)>.
- <sup>34</sup> *Ibid* at 4-5.
- <sup>35</sup> W. Maxwell and T. Newman, "The WTO Puts Electronic Commerce on the International Trade Regulation Radar," Hughes, Hubbard & Reed LLP, New York, New York, nd, online: <[http://www.hugheshubbard.com/data/whatnew/Publications \(New\)/hotdata/WTO.html](http://www.hugheshubbard.com/data/whatnew/Publications%20(New)/hotdata/WTO.html)>.
- <sup>36</sup> Henry Perritt, "The Internet is Changing the Public International Legal System," (2000) 88 Ky. L. Rev., online: Chicago-Kent College of Law <<http://www.kentlaw.edu/cyberlaw/perrittnetchg.html>>.
- <sup>37</sup> The European Commission's Directive on Data Privacy (October 1998) prohibits the transfer of personal information to countries outside the EU which do not meet the privacy standards set out in the Directive. Since the Directive's standards are higher than those imposed by U.S. law American companies doing business in Europe could face a discontinuation of data flows from overseas offices in Europe if their internal privacy standards are considered to be inadequate. Therefore, the U.S. negotiated an arrangement with the EU, beginning in July 2000, whereby American companies could self-certify compliance with the standards set out in the EU Directive, thereby protecting themselves against the risk of prosecution by European authorities. Certification must be done to the U.S. Department of Commerce on an annual basis, and there are seven "safe harbor principles" with which a company must comply. To date, few companies have actually participated in this program. Online: U.S. Department of Commerce, Export Portal, Safe Harbor Overview, <[http://www.export.gov/safeharbor/sh\\_overview.html](http://www.export.gov/safeharbor/sh_overview.html)>, and also see <<http://www.export.gov/safeharbor/USLETTERFINAL1.htm>>.
- <sup>38</sup> United States, Department of Commerce, *Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers*, 25 November 1998, online: Department of Commerce, National Telecommunications and Information Administration <<http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>>.
- <sup>39</sup> OECD, *The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda*, February 1999, at 51, online: Organisation for Economic Co-operation and Development, <[http://www1.oecd.org/subject/e\\_commerce/summary.htm](http://www1.oecd.org/subject/e_commerce/summary.htm)>.
- <sup>40</sup> Dryden, *supra* note 33 at 4.

- <sup>41</sup> International cooperation towards the regulation and harmonization of standards for protecting intellectual property rights in cyberspace is evident in the WIPO Copyright Treaty (WCT, 1996) and the WIPO Performances and Phonograms Treaty (WPPT, 1996), as well as in the WTO Agreement on Trade-Related Aspects of Intellectual Property (TRIPS). The Geneva-based WIPO, an agency of the United Nations with 175 member nations, is charged with promoting the international protection of intellectual property rights. WIPO administers 21 international treaties, and its activities complement the work of the WTO by assisting members to harmonize their national legislation so that it complies with the provisions contained in TRIPS. In addition, WIPO has created an Arbitration and Mediation Center which is available to parties involved in intellectual property disputes, and has also formulated a list of recommendations regarding the misuse of trademarks on the Internet through "cybersquatting", suggesting a global domain name protection system which would include a "uniform and mandatory administrative dispute-resolution system." Online: World Intellectual Property Organization, <<http://www.wipo.org/treaties/ip/index.html>>.
- <sup>42</sup> This was the conclusion of the American Bar Association Committee on Cyberspace Law, in the ABA Jurisdiction Project *Transnational Issues in Cyberspace: A Project on the Law Relating to Jurisdiction*, (London Meeting Draft, 2000). To deal with the drawbacks of traditional approaches to jurisdiction when applied to e-commerce, the Report recommends the creation of a multinational Global Online Standards Commission (GOSC), which would develop uniform principles and worldwide standards for jurisdictional rules involving electronic commerce. Such rules would in effect establish jurisdictional "Cyber-borders" to replace the physical borders which e-commerce largely makes irrelevant. The Report also suggests using programmable electronic agents (cyberbots, or "Bots"), which would use artificial intelligence to apply such jurisdictional rules to each e-commerce transaction, and also to safeguard consumers against web sites which do not meet their own predetermined personal standards of determining jurisdiction. Online: American Bar Association <<http://www.abanet.org/buslaw/cyber/initiatives/proj-documentation.html>>.
- <sup>43</sup> The 1996 Model Law on Electronic Commerce, drafted by the United Nations Commission on International Trade Law (UNCITRAL), provides guidance for countries modernizing their domestic laws to accommodate e-commerce transactions, by eliminating incompatibilities between online contracting and domestic laws requiring paper-based documentation in commercial matters, and codifying the legal recognition of information and documents communicated electronically. Domestic laws based on the Model Law employ a "functional equivalency" approach, the recognition of electronic contracting and electronic agents, the recognition of electronic files where formerly a paper requirement existed (with the possible exception of areas such as wills and codicils, negotiable instruments, and documents transferring land), and the recognition of electronic signatures. See: United Nations, *UNCITRAL Model Law on Electronic Commerce*, General Assembly resolution 51/162 of 16 December 1996. online: United Nations Commission on International Trade Law <<http://www.uncitral.org/en-index.htm>>.
- <sup>44</sup> See *supra* note 7.
- <sup>45</sup> Established in 1893, the Hague Conference on Private International Law is an intergovernmental organization currently with 46 member nations. Its purpose is to provide a forum for the negotiation and drafting of multilateral treaties in the area of private international law. Online: Hague Conference on Private International Law, <<http://www.hcch.net/e/>>.
- <sup>46</sup> See *supra* note 37.
- <sup>47</sup> *A Framework for Electronic Commerce* (U.S.) and *A European Initiative in Electronic Commerce* (EU), *supra* notes 32 and 2.
- <sup>48</sup> United States, "Trade with the European Union: Recent Trends and Electronic Commerce Issues," General Accounting Office document GAO/T-NSIAD-00-46 of 13 October 1999 (statement before the Senate Committee on Foreign Relations, Subcommittee on European Affairs), at 8, online: U.S. General Accounting Office <<http://www.gao.gov/new.items/ns00046t.pdf>>.
- <sup>49</sup> United States, "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress," Federal Trade Commission, May 2000, online: Federal Trade Commission <<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>>.
- <sup>50</sup> "Strong" encryption refers to essentially unbreakable data encryption through the use of software and/or hardware, using a technique judged so difficult to break that the U.S. government has restricted its exportation. For example, the Data Encryption Standard (DES) takes each 64-bit block of data to be encrypted and applies a randomly-chosen 56-bit key from one of 72 quadrillion (72,000,000,000,000,000) possible keys. Although DES is considered "strong" encryption, many companies employ "triple DES", which applies three keys in succession. As with other "private key" cryptographic methods, DES requires both the sender and recipient to use the same private key in order to decrypt data. Given enough time and resources, even DES is vulnerable to code breakers, and a replacement — dubbed Advanced Encryption Standard (AES) — is currently under development. online: searchSecurity.com <[http://search-security.techtarget.com/sDefinition/0,,sid14\\_gci212062,00.html](http://search-security.techtarget.com/sDefinition/0,,sid14_gci212062,00.html)>.
- <sup>51</sup> In order for electronic commerce to flourish, strong encryption technology must be readily available to parties taking part in online transactions. Such a level of encryption is necessitated by the nature of open networks like the Internet, which pose significant security and privacy risks to data both during transmission through cyberspace and when stored on computers which are accessible through the Internet. Without the enhanced security which strong encryption provides, consumer confidence in online transactions will be suspect and the growth of e-commerce will be limited by concerns over safety and reliability.
- <sup>52</sup> See Stewart Baker, "The Legal and Policy Framework for Global Electronic Commerce," *University of California E-economy Project Background Papers*, 5-6 March, 1999, online: University of California at Berkeley <<http://e-economy.berkeley.edu/publications/summary/0399ecom.html>>.
- <sup>53</sup> The risk posed by having different approaches is noted by UNCITRAL in its Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001), which provides the following rationale for the Model Law: "The increased use of electronic authentication techniques as substitutes for hand-written signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (which may be referred to generally as 'electronic signatures'). The risk that diverging legislative approaches be taken in various countries with respect to electronic signatures calls for uniform legislative provisions to establish the basic rules of what is inherently an international phenomenon, where legal harmony as well as technical interoperability is a desirable objective." See: United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* (2001), January 2001, at 8, online: United Nations Commission on International Trade Law <<http://www.uncitral.org/en-index.htm>> (Document A/CN.9/WG.IV/WP.88).
- <sup>54</sup> See *supra* note 48 at 11.
- <sup>55</sup> Patrick Vittet-Philippe, "Towards a Common Framework for Global Electronic Commerce," in *Internet Law and Policy Forum*, 1998.
- <sup>56</sup> *Ibid*.
- <sup>57</sup> United States, United States Mission to the European Union, *U.S. and EU hold digital commerce workshop*, 17 October 2000, online: United States Mission to the European Union <<http://www.useu.be/ISSUES/ecom1017.html>>.
- <sup>58</sup> Statement by acting U.S. Undersecretary of Commerce, Robert LaRussa, "U.S. Seeks Dialogue With EU On E-Commerce," Reuters (19 July 2000), online: zdnet.com <<http://www.zdnet.com/intweek/stories/news/0,4164,2605378,00.html>>.
- <sup>59</sup> See The United States Mission to Europe (Brussels, Belgium).
- <sup>60</sup> See United States, "U.S. and EU Hold Digital Commerce Workshop," Department of Commerce, International Trade Administration, 17 October 2000, online: United States Mission to the European Union <<http://www.useu.be/ISSUES/ecom1017.html>>.
- <sup>61</sup> Australia, State of Victoria Department of State Development, *Promoting Electronic Business*, 1998, online: The Victorian Government's Repository of e-Government Resources <<http://www.go.vic.gov.au/pdfs/Comm.pdf>>.
- <sup>62</sup> Henry Perritt, "Hybrid Regulation as a Solution to Internet Jurisdiction Problems: Beyond the Hague Convention Draft," *Internet Law & Policy Forum*, September 2000, online: Internet Law and Policy Forum, <[http://www.ilpf.org/events/jurisdiction2/presentations/perritt\\_pr/](http://www.ilpf.org/events/jurisdiction2/presentations/perritt_pr/)>.