4-1-2001

Internet Regulation: An Inter-American Plan

M. Leigh Macdonald

COMMENT

INTERNET REGULATION: AN INTER-AMERICAN PLAN

I. INTRODUCTION

> The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet.[1]

Legislative bodies across the globe are enacting regulatory schemes with the hope of protecting government, businesses and individuals from the dangers of the Internet. Despite adequate forethought and successful implementation of each individual scheme, the real problem with respect to Internet regulation rests in the numbers.[2] In other words, it is the combination of many different schemes that poses the greatest threat. Cultural and political distinctions undoubtedly shape these regulations, so the resulting regulations are as varied as the sponsoring countries. This variation presents confusion for Internet users and immerses them in inconsistent regulation.[3] Beyond these issues lies the stark reality that enforcement of any Internet regulation is, at best, difficult.[4]

II. BACKGROUND

In order to understand the problems associated with Internet regulation, one must first understand the composition of the Internet. The Internet disregards location. It defies traditional commercial and communication boundaries and

---

1. American Civil Liberties Union v. Johnson, 194 F.3d 1149, 1161 (10th Cir. 1999)(quoting American Library Ass'n v. Pataki, 969 F.Supp. 160, 168-69 (S.D.N.Y. 1997)).

2. *Id.*

3. *Id.*

4. Enforcement, as an aspect of international law generally, has "received a good deal of attention. Indeed, many social scientists have contended that the absence of any swift and sure way of enforcing international law means that it is not 'law'. . . ." M. O. Chibundu, *Making Customary International Law Through Municipal Adjudication: A Structural Inquiry*, 39 VA. J. INT'L L. 1069, 1079 (1999)(internal quotation marks omitted).

provides users with unprecedented connectivity. A user may easily find herself at the Internet address of someone from another state, country, or continent. An even more interesting point is that users rarely have any idea where sites originate from. User ability to transcend traditional geographic boundaries presents an array of problems. An initial glance prompts a list of concerns that does not begin to be exhaustive. Issues include the protection of privacy, consumer protection, taxation, security of electronic payments, responsibility for criminal acts and protection of intellectual property rights.

The construction of the Internet presents another obstacle to successful Internet regulation. It is a system of networks linked together in a decentralized fashion.[5] There is not a single database that controls all transmissions.[6] Instead, computers are simply linked together through connections between networks.[7] Moreover, information is transferred via the Internet in a process called "packet-switching."[8] Through this process, a single transmission may be broken up into parts.[9] These parts are then sent to the specified destination via various paths.[10] Once the parts arrive, the information is reassembled and ready for viewing by the recipient.[11] This decentralized construction renders an information and communication system that is not prone to control by a single government.[12]

Despite these hurdles, many governments are beginning to take regulatory action in an effort to protect their constituents.[13] These regulatory measures are bound to be as diverse as the cultural and political precepts that support them. The result is that Internet users are exposed to a panoply of inconsistent regulations.[14]

This comment proposes first, that the governments of the

5. American Civil Liberties Union v. Reno, 929 F.Supp. 824, 830 (E.D.Pa. 1996).
6. *Id.* at 832.
7. *Id.* at 830-31.
8. *Id.* at 832.
9. *Id.*
10. *Id.*
11. *Id.*
12. *Johnson*, 194 F.3d. at 1161.
13. Governments throughout the world are regulating or moving away from wait-and-see postures toward regulating Internet activity. Joseph M. Kelly, *Internet Gambling Law*, 26 WM MITCHELL L. REV. 117, 121-23 (2000).
14. *Johnson*, 194 F.3d. at 1161.

Americas act jointly to form an Inter-American regulatory scheme. Second, this comment discusses goals that are common to American governments. These goals offer guidance in constructing regulations. Third, this comment suggests that American governments take some initial steps to facilitate the successful implementation of a regulatory scheme for the Internet. Finally, this comment examines several issues that are likely candidates for regulation.

III. AN INTER-AMERICAN SCHEME

The age-old adage states that two are better than one. In this case, many are better than one. Any single American government will face such extreme enforcement issues as to render an otherwise effective regulatory scheme powerless.[15]

Given the global nature of the Internet, regulations that attempt to regulate a small group of people will fall sorely by the wayside. National legislation is fraught with extra-territorial and enforcement concerns.[16] Legislation at the sub-national level is even more extraterritorial in nature.[17] Any regulatory scheme

---

15. This is illustrated well by Australia's legislation geared at a website-rating scheme. It goes so far as to discuss enforcement measures that will be taken against violators outside Australian soil. Of course, critics question the Australian government's ability to act on those measures. It is certainly fair to wonder how the Australian government expects to effectively enforce such an extra-territorial measure. Broadcasting Services Amendment Bill 1999, *at* http://www.ozemail.com/~mbaker/amended.html (last visited Jan. 25, 2001) [hereinafter Aussie Bill].

16. Enforcement actions outside a country's limit are fraught with jurisdictional issues. While no Internet-related discussion is complete without examining jurisdictional concerns, numerous articles have been written on this subject. The topic is so broad that it is more appropriately handled as a main topic. See Andrew E. Costa, *Minimum Contacts in Cyberspace: A Taxonomy of the Case Law*, 35 HOUS. L. REV. 453 (1998), for an excellent discussion of these issues.

17. Michigan has added an area to its state tax return where residents must declare and pay taxes on their Internet and mail order purchases. Recently, Texas issued new rules governing automobile sales, including those made online. The rule restated that it is illegal to sell cars in Texas without a state license. Many online auto dealers have decided not to sell cars in Texas for the time being. A Virginia winery and a California winery joined to sue the state of New York in federal court over its law prohibiting direct sales of alcohol by out-of-state vendors to residents of New York. New York is one of almost 30 states to ban such sales, and it is the fifth state to be sued over the law. In the last several months, states including California, Alaska, Iowa and Wisconsin have begun to crack down on online cigarette sales. Those states and others have asked that online cigarette stores turn over their customer lists and they have begun to pursue residents for outstanding taxes. Tory Wolverton, CNET News.com, *State officials look at new rules for e-commerce*, (Feb. 25, 2000), *at* http://dailynews.yahoo.com/h/cn/20000225/tc/20000225021.html (on file with the

that is too local in nature is likely to have little or no impact on either the intended benefactors or those who violate the regulation. Moreover, with the addition of each new regulation, the greater the "likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation."[18]

A. COMMON INTER-AMERICAN GOALS

An Inter-American regulatory scheme must represent goals common to many American governments. Common goals are easily extracted from treaties such as the North American Free Trade Agreement ("NAFTA")[19] and the Treaty Establishing a Common Market ("MERCOSUR").[20] Another helpful source for determining common goals is the Declaration of Principles ("DOP"), established by the member countries of the Free Trade Area of the Americas ("FTAA").[21]

Before reviewing goals delineated in the aforementioned sources, it is important to note that an Inter-American regulatory scheme should be flexible.[22] Flexibility is necessary given the rapid changes in computer, communications and Internet technology. Additionally, an Inter-American scheme should be responsive to public interest and encourage competition and innovation.[23] Throughout this comment, a constant focus is placed on these goals as well as those provided in NAFTA, MERCOSUR and FTAA.

Chapter One of the North American Free Trade Agreement

University of Miami Inter-American Law Review)(last visited Mar. 28, 2000).

18. *Johnson*, 194 F.3d. at 1161

19. North American Free Trade Agreement, Dec. 17, 1992, Can.-Mex.-U.S., art. 102, 32 I.L.M. 289 (1993)[hereinafter NAFTA].

20. Treaty of Asuncion, March 26, 1991, Arg. Rep. – Fed. Rep. of Brazil – Rep. of Para. – Eastern Rep. of Uru., 30 I.L.M. 1041 (1991) (establishing a Southern Common Market - Mercado Común del Sur) [hereinafter MERCOSUR].

21. Área de Libre Comercio de Las Americas, Free Trade Area of the Americas ("FTAA"), *Summit of the Americas, Declaration of Principles* (Dec. 1994), *at* http://www.ftaa-alca.org/ministerials/miami_e.asp (last visited Jan. 25, 2001)[hereinafter FTAA Principles].

22. *See* Dale Marshall & Ruben Morales, *FTAA Joint Government-Private Sector Committee of Experts on Electronic Commerce: Report With Recommendations to Ministers* (Nov. 4, 1999), *at* http://www.ftaa-alca.org/spcomm/derdoc/ec1de.doc, at *5 (last visited Jan. 25, 2001)[hereinafter Recommendations].

23. *Id.*

makes clear that NAFTA establishes a free-trade area in accordance with Article XXIV of the General Agreement on Tariffs and Trade ("GATT").[24] Additionally, the chapter sets out the general objectives of the Agreement.[25] They are as follows:

> eliminate barriers to trade in, and facilitate the cross-border movement of, goods and services between the territories of the parties; promote conditions of fair competition in the free trade area; increase substantially investment opportunities in the territories of the Parties; provide adequate and effective protection and enforcement of intellectual property rights in each Party's territory; create effective procedures for the implementation and application of this Agreement, for its joint administration and for the resolution of disputes; [and] establish a framework for further trilateral, regional and multilateral cooperation to expand and enhance the benefits of this Agreement.[26]

Several goals were established by the members of MERCOSUR including the "free movement of goods and services, capital and labor; elimination of customs tariffs and non-tariff barriers and the establishment of a common external tariff; the adoption of a common trade policy; [and] the coordination of macroeconomic policies."[27]

At its 1994 Summit of the Americas, the Free Trade Area of the Americas established the following goals: "preserve and strengthen the community of democracies of the Americas; promote prosperity through economic integration and free trade; eradicate poverty and discrimination in our hemisphere; [and] guarantee sustainable development and conserve our natural environment for future generations."[28]

---

24. NAFTA, *supra* note 19.

25. *Id.*

26. *Id.*

27. Stephen P. Sorensen, *Open Regionalism or Old-Fashioned Protectionism? A Look at the Performance of MERCOSUR's Auto Industry*, 30 U. MIAMI INTER-AM. L. REV. 371 (1999)(citing Roberto Bouzas, *MERCOSUR y Liberalizacion Comercial Preferencial en America del Sur; Resultados, Temas y Proyecciones, in* NAFTA Y MERCOSUR: UN DIÁLAGO CANADIENSE-LATINOAMERICANO (Richard G. Lipsey & Patricio Meller eds., 1996)).

28. FTAA Principles, *supra* note 21.

B. INITIAL STEPS

The American Internet population, or the lack thereof in some American countries, presents an issue that must be addressed prior to enacting regulation. American governments should, collectively, encourage the development of Internet infrastructures in countries where the user populations are low.[29] Infrastructure improvements should come in the form of higher quality telecommunication frameworks, broader bandwidth and decreased connection costs.[30] Indeed, investment for this Internet infrastructure will come primarily from private sources, but government incentives for investors would likely speed the development process.[31] Additionally, governments should encourage constituent participation in the Internet marketplace.[32] Increased participation in the Internet marketplace will likely begin with users "surfing" the net, but time and encouragement should prompt online purchasing, online banking, even online start-up businesses. This additional, and international, market activity will promote competition among Internet vendors. Also, increased international market activity is supported by NAFTA, MERCOSUR and FTAA goals of free movement of goods and services, capital and labor.[33]

One excellent way for governments to encourage increased Internet use is by providing public services via electronic means. This "governments as model users" plan should include government-to-government, government-to-business and

---

29. Recommendations, *supra* note 22.

30. Bandwidth is "[t]he capacity of a medium to transmit a signal." Informally, it is the "size" of the Internet and its ability to carry users' files and messages. *See* Brendan Flushright, *Zen and the Art of the Internet - Glossary, at* http:www.cs.indiana.edu/docproject/zen/zen-1.0_16.html (last visited Jan. 25, 2001).

31. Incentives could take form in tax deductions, tax credits or supplementary funding.

32. As of 1998, only three percent (3%) of the world's Internet users were in South America. On the other hand, fifty-seven percent (57%) of those users were in North America. This gap in access to and use of information technologies between North and South America represents a major area of opportunity. In order to meet the goal of hemispheric integration, governments must strive to eradicate this divide. *See Nua Internet Surveys: Graphs & Charts - 1998, at* http://www.nua.ie/surveys/graphs_charts/1998graphs/location.html [hereinafter Nua Surveys](on file with University of Miami Inter-American Law Review)(last visited Jan. 22, 2000).

33. These goals are consistently iterated in FTAA, NAFTA and MERCOSUR documents.

government-to-individual transactions.[34] Government services provided electronically will be less costly and more efficient.[35] While governments shave the cost of providing services, users will become accustomed to conducting business activities via the Internet.[36]

Another way for governments to bolster Internet use by individuals is to make the Internet accessible from public facilities.[37] Libraries, public schools and universities, malls, and public transportation facilities are all places where individuals can gain experience with electronic communications. Ideal locations are those that have high traffic and are likely to be frequented by people who do not already own home computer equipment.

Additionally, individual governments should promote electronic commerce within their countries.[38] Electronic commerce will aid countries in overcoming comparative disadvantages that accompany long distances and geographic barriers.[39] Inter-market activity will increase because the associated cost will be lower.[40] This increased international business activity is consistent with the goal of encouraging competition and innovation, as well as the goals outlined in NAFTA, MERCOSUR and FTAA.[41]

Once member governments have increased the size of the Internet audiences within their countries' physical boundaries, they should look to establishing rules. The United States has already adopted five basic tenets that guide regulatory

34. Recommendations, *supra* note 22.

35. *Id.*

36. This setting would be considerably more comfortable for new users than settings involving private entities. Given user concern about safety of information and the general unwillingness to relinquish tangible business activities, government interaction, at the onset, would likely prove beneficial.

37. This introduces an array of concerns regarding access by minors to obscene and/or indecent material. See Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, 24 F.Supp.2d 552 (E.D. Va. 1998), for a detailed discussion of this topic. *See also* Jonathan Wallace, *Purchase of Blocking Software by Public Libraries is Unconstitutional, at*
http://www.mit.edu/activities/safe/labeling/library/censorware-lib-wrong.html (last visited Jan. 25, 2001).

38. Recommendations, *supra* note 22, at 8-9.

39. *Id.* at 7-8.

40. *Id.*

41. *Id.* *See also* NAFTA, *supra* note 19; MERCOSUR, *supra* note 20; FTAA Principles, *supra* note 21.

decisions.[42] While the United States is simply one country in the mix of American governments, these tenets provide practical guidance. First, the private sector should lead.[43] Second, governments should avoid undue restriction on electronic commerce.[44] Third, where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.[45] Fourth, governments should recognize the unique qualities of the Internet.[46] Finally, electronic commerce over the Internet should be facilitated on a global basis.[47]

IV. ISSUES RIPE FOR REGULATION

A. Privacy

One issue that may require regulation is the protection of privacy.[48] In order to take full advantage of the Internet, users must feel sure that their private information will not be used for improper purposes.[49] Businesses stand at the other end of this

42. Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series, PLI Order No. G4-4040, *A Framework for Global Electronic Commerce*, 544 PLI/Pat 457, 459, Dec. 1998. These tenets were adopted by the Clinton Administration in 1998 [hereinafter Clinton Framework].

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

48. FTAA, *Joint Government-Private Sector Committee on Electronic Commerce, Protection of Privacy in Electronic Commerce* (June 16, 1999), *at* http://www.ftaa-alca.org/spcomm/notes/eci25r2e.doc (last visited Jan. 25, 2001).

49. Seventy-six percent (76%) of users express concern over sites that monitor Internet browsing. (BCG Consumer Survey). Seventy percent (70%) worry about making purchases online. (BCG Consumer Survey). Forty percent (40%) of users have provided false information at least once while registering at a Web site. (Georgia Tech Survey). Sixty-three percent (63%) of users now reluctant to provide personal information say they would divulge information if websites disclose clearly how the information will be used. (Harris/Westin Survey). Users are 2 to 3 times more willing to provide sensitive information to companies that disclose their information gathering and dissemination practices. (BCG Consumer Survey). Truste, *How Does Online Privacy Impact Your Bottom Line*, *at* http://www.truste.org/webpublishers/pub_bottom.html (last visited Jan. 25, 2001) (citing a 1998 Business Week survey) [hereinafter Bottom Line].

continuum.[50] These businesses recognize the amount of profit that can be generated through the use of private data.[51] One possible regulatory scheme permits use of private data only within the Americas. A more relaxed scheme permits users outside the Americas to use the private data of those within the Americas. However, this scheme only permits such use upon a showing that the data will be provided an adequate degree of protection.[52] Perhaps the most relaxed regulatory measure is no measure.[53] In other words, the Inter-American scheme could allow industry to regulate itself.[54] Each of these choices has pros and cons. The last alternative provides little or no security for Americans and invites industry to run rampant with private

50. "It has been estimated that, on average, companies trade and transfer personal information about every U.S. resident every five seconds." *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000) [hereinafter Shaffer](citing Jeffrey Rothfeder, Privacy for Sale 17 (1992), which notes that "there are upwards of five billion records now in the United States that describe each resident's whereabouts and other personal minutiae").

51. The collection of data by multiple vendors, coupled with subsequent cross-matching, enables businesses to create detailed portraits of individuals' lifestyles, tastes, political views and heath. Bottom Line, *supra* note 49.

52. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *at* http://europa.eu.int/comm/dg15/en/media/dataprot/law/dir9546.html (last visited Jan. 25, 2001).

53. This is the present stance of the United States. In February 2000, the EU and the United States announced a tentative agreement after two years of data protection negotiations. In the same month, however, another online privacy bill was introduced in the United States House of Representatives. Rep. Frelinghuysen (R-NJ) introduced the Online Privacy Protection Act of 2000 on January 31. It is the companion to a bill filed in the Senate last April by Sen. Burns and Sen. Wyden. Rep. Rodney Frelinghuysen's bill, HR 3560 IH, joins a growing list of other pending bills that would regulate privacy practices of web sites and online services. The bill requires web sites and online services to provide notice of what personal information they collect, how they use it, and how they share it with others. Additionally, individuals must be given the opportunity to opt out of having their personal information disclosed to others, for purposes unrelated to those contained in the notice. The bill also requires web sites and online services to provide individuals both a description and copies of their personal information. Finally, the bill requires web sites and online services to protect the confidentiality of personal information. Tech Law Journal, *Another Online Privacy Bill Introduced in House* (Feb. 8, 2000), *at* http://www.techlawjournal.com/privacy/20000208.html (on file with University of Miami Inter-American Law Review)(last visited Mar. 29, 2000).

54. The United States has adopted this self-regulatory standard primarily because private sector investment has supported the irrepressible growth of the Internet. *See* Jonathan P. Cody, *Protecting Privacy Over The Internet: Has The Time Come To Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1190 (1999).

data.[55] While inaction regarding some issues is likely the best alternative, privacy protection is not one of them. Inaction and the resulting user privacy invasions are completely counter to the initial step of increasing user population.[56] On the other hand, the first alternative will provide greater security for Americans. However, this scheme brings with it an array of enforcement concerns, especially outside the Americas. The second alternative also provides a high level of security for Americans, but a major concern with this scheme, as well as the scheme posed first and the EU Directive, is its extra-territorial nature. The issue again becomes enforcement. Even if the Americas agree on a privacy protection scheme, the question of enforcing it in other continents still lingers.[57]

While worldwide enforcement seems unrealizable, enforcement within the Americas, based on guidelines established in an Inter-American scheme, is an effective starting point. An Inter-American scheme should acknowledge privacy protection and goals that are common to the various governments. In addition, the scheme should include an enforcement measure that can be acted upon in each American country. Indeed, this sort of directive would encompass only a portion of the world's potential privacy violations. Nevertheless, given the fact that sixty percent of today's Internet population is in North and South America, it is certainly an appropriate place to begin.[58]

An Inter-American privacy scheme should preserve basic notions of privacy. However, it should not wander far past these basic notions so as to stay within the realm of minimalist, predictable and simple.[59] First, subjects of information, should be entitled to know what information may be disclosed and to whom it may be disclosed.[60] This duty of notice may even be extended to include the duty to inform the user each time a disclosure is

55. Shaffer, *supra* note 50.

56. Nua Surveys, *supra* note 32.

57. "Without an enforceable set of rules to permit commercial predictability, certainty, and consumer confidence, the 'global market' will never achieve its potential." Shirley F. Sarna, *Advertising on the Internet: An Opportunity for Abuse?* 11 ST. JOHNS J. LEGAL COMMENT. 683, 689 (1996).

58. NUA Surveys, *supra* note 32.

59. Clinton Framework, *supra* note 42.

60. HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY: PRIVACY, ACCESS, INTELLECTUAL PROPERTY, COMMERCE, LIABILITY 132 (1996).

made.[61] Another concern with respect to privacy is the use of inaccurate information.[62] Naturally, gathered information will possess varying degrees of sensitivity.[63] Certainly, with respect to data that is more sensitive, information custodians should be bound to allow the subject to access the information and request corrections.[64] Additionally, the custodian should be required to make such corrections in a timely fashion. Another rule should center on the custodian's disclosure duties. Information may only be disseminated to those who were disclosed as recipients and only for the intended and disclosed purposes.[65] In the context of an Inter-American scheme, the importance of privacy protection cannot be understated. The goal to increase the number of Internet users in North, and especially South, America will be severely stunted if people suspect that Internet use will invade their privacy.[66] Given the proposed initial step of increasing the American Internet community, privacy protection guidelines must be implemented.

B. Cryptography

Another issue that is prone to regulation is the use of cryptography. In order to appreciate the dilemma created by cryptographic capabilities, one should first understand the nature of the technology.

First, you should understand what cryptography is not. It is not a code.[67] "One if by land, two if by sea" is a code.[68] However, if the British had come in by parachute, no number of lanterns would have signified it correctly.[69] Disadvantages to code are its inflexible nature and the ease with which the code can be cracked.[70] Cryptography is the foundational technology for many things.[71] It provides privacy for stored records and information.[72]

---

61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. Clinton Framework, *supra* note 42.
67. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PA. L. REV. 709, 713-14 (1995).
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

It allows users to authenticate documents, thus ensuring the identity of the person sending the message.[73] Through cryptographic technology, users can ensure that a message was not tampered with prior to, during, or after transmission.[74] Cryptography also permits user anonymity.[75]

In symmetric key cryptography, the same key is used to encrypt and decrypt messages.[76] The sender and the receiver use the same key, thus the security of a symmetric key system is contingent on the secure transfer of the key between the communicating parties.[77]

Asymmetric key cryptography, or public key cryptography, is dual key.[78] There is one public key and one private key.[79] The sender uses the recipient's public key, which is not secret, to encrypt the message.[80] On the other hand, the private key, known only to the recipient, is used to decrypt the message.[81] Data encrypted with the public key can only be decrypted with the corresponding private key; knowledge of the public key does not in any way compromise the secrecy of the private key.[82] Thus, because public key cryptography does not involve a transfer of keys, it reduces one of the traditional vulnerabilities of non-computerized and computerized encryption.[83]

With all of these capabilities, cryptography is a double-edged sword. It provides security to law-abiding citizens who simply wish to ensure that their data is kept private. On the other hand, encryption poses a threat to public safety by making it easier for criminals to communicate without the possibility of law enforcement decrypting their communications. Despite this tension, the United States Commerce Department, in January

---

72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. Anjali Singhal, *The Piracy Of Privacy? A Fourth Amendment Analysis Of Key Escrow Cryptography*, 7 STAN. L. & POL'Y REV. 189, 190 (1996).
77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.*
83. D. James Bidzos & Burt S. Kalliski, *An Overview Of Cryptography*, LAN Times, Feb. 1990, at 100; Robert B. Stout, S-Coder for Data Encryption, DR. DOBBS J., Jan. 1990, at 52.

2000 and in October 2000, released new regulations to relax encryption export restraints.[84] The new regulations provide that any encryption product of any key length may be exported, after a technical review, to any end-user in Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland or any European Union member.[85] Restrictions were not removed for the seven states supporting terrorism: Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria.[86] This present regulation is much more relaxed than the previous regulation which precluded export of any encryption product with greater than a 56-bit key length.[87]

Some argue that "key escrow," or trusted third party systems, is an option for balancing public safety concerns with the need for secure data transmission.[88] These third party systems would basically serve as depositories for cryptographic keys.[89] Thus, anyone using cryptography would have to make available the means to decrypt information that they encrypted

---

84. 65 Fed. Reg. 2492 (Jan. 14, 2000)(codified at 15 C.F.R. pt. 734, 740, 740, 742, 744, 748, 770, 771, 774), *available at* http://frwebgate4.access.gpo.gov/cgibin/waisgate.cgi?WAISdocID=5722015447+0+0+0&WAISaction=retrieve (last visited Jan. 25, 2001)[hereinafter January regulation]; 65 Fed. Reg. 62600 (Oct. 19, 2000)(codified at 15 CFR pt. 732, 734, 740, 742, 744, 748, 770, 771, 774), *available at* http://frwebgate4.access.gpo.gov/cgibin/waisgate.cgi?WAISdocID+5722015447+1+2+0&WAISaction=retrieve (last visited Jan. 25, 2001)[hereinafter October regulation].

85. October regulation, *supra* note 84.

86. January regulation, *supra* note 84.

87. "In the past, the export of cryptographic products was regulated by the United States Department of State, under the authority of the International Traffic in Arms Regulations ("ITAR"), which defined cryptographic devices [sic], including software, as munitions. The ITAR prohibited export of encryption software containing key lengths greater than 40 bits." In November 1996, an executive order (Executive Order 13026) was signed [hereinafter November 1996 regulation]. Executive Order 13026 announced that the Department of Commerce, rather than the Department of State, would have jurisdiction over the export of these technologies. Under the November 1996 regulation, the export of cryptographic products were reviewed by the Bureau of Export Administration ("BXA"), which reviewed all applications to export encryption software and related technologies except for technologies developed for or adapted to military uses. The November 1996 regulation permitted tthe export of encryption products containing up to 56-bit key length Digital Encryption Standard ("DES"). An Interim Rule implementing the Executive Order became effective on December 30, 1996. *See* RICHARD RAYSMAN, PETER BROWN AND JEFFREY D. NEUBURGER, MULTIMEDIA LAW: FORMS & ANALYSIS: THE INTERNET AND ONLINE SERVICES § 10.09 (1999).

88. A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. L. FORUM 15, 24-31 (1996).

89. *Id.*

and sent via electronic means.[90] Talk of key escrow originated with plans by the United States government to act as the depository.[91] This was met with much disdain. Critics argued that the government was making itself a "big brother" and violating constitutional principles along the way.[92] Subsequent proposals have endorsed the use of private entities to act as key escrows. This is more palatable to most encryption users. The primary constitutional concerns with private key escrow relate to issues of search and seizure.[93] Opponents of key escrow argue that any type of depository is subject to unauthorized withdrawal by government agencies.[94]

An Inter-American scheme should adopt the standard recently endorsed by the United States government. That scheme should permit the export of cryptographic measures. NAFTA, MERCOSUR and FTAA all discuss the need for free movement of goods among the American countries. In particular, NAFTA established as one of its goals the need to facilitate the cross-border movement of goods and services between the territories. If the Americas are really going to form a single community, technological innovations should move freely across sovereign borders.

C. Cyber Crime

Another issue that demands regulatory attention is criminal responsibility as it relates to the Internet. The growth of the Internet brings with it super-capabilities relating to information

---

90. *Id.*

91. *Id.*

92. *Id.*

93. "[C]ritics contend that the collection and storage of private keys in the hands of government or private entities would be susceptible to technical attack as well as abuse through mistake or corruption. Given the controversy and unanswered questions, the issue of back door access through a key escrow/recovery system is typically a pivotal and hotly contested issue in any discussion involving the expansion of encryption controls." Raneta Lawson Mack, *Digital Signatures, The Electronic Economy And The Protection Of National Security: Some Distinctions With An Economic Difference,* 17 J. MARSHALL J. COMPUTER & INFO. L. 981, 996 (1999).

94. "[K]ey escrow proposals, requiring nothing more than a subpoena without a particularized search target, would easily lead to dragnet searches resulting in a significant infringement on the security and privacy of every individual communicating or transacting business on the Internet in violation of Fourth Amendment protections." Joe Baladi, *Building Castles Made Of Glass-Security On The Internet,* 21 U. ARK. LITTLE ROCK L. REV. 251, 274 (1999).

and communication. On the other hand, it also delivers an ever-increasing menu of cyber crimes. Internationally, law enforcement faces the following challenges: harmonization of countries' criminal laws; locating and identifying perpetrators across borders; and securing electronic evidence of crimes so that criminals may be brought to justice.[95] Additionally, complicated jurisdictional issues accompany the dilemma of law enforcement.[96]

One of the problems relating to computer crimes is that they are simpler to commit than traditional crimes.[97] International computer crimes can be committed from the privacy of home.[98] Hackers are not limited by the existence of physical or sovereign boundaries.[99] After all, information and property can be transmitted secretly through electronic means.[100] A hacker needs no passport and passes no checkpoints.[101] He simply uses his keyboard and mouse to gain entry.[102] Furthermore, one individual can steal, defraud or damage single-handedly.[103]

A second problem with the regulation of cyber crime is that many countries do not recognize the cyber crime threat to public safety.[104] In addition, many countries do not appreciate the need for international cooperation to effectively respond to the problem.[105] Consequently, many countries have weak laws, or no laws, against computer hacking.[106] These countries effectively

95. Department of Justice, *at* http://www.usdoj.gov/criminal/cybercrime/intl.html (on file with University of Miami Inter-American Law Review)(last visited Mar. 29, 2000)[hereinafter DOJ Cybercrime Report].

96. In response to the abundance of issues surrounding cyber crime, Former Attorney General Janet Reno has prompted meetings in which representatives from eight countries were present. These meetings were held to create realistic, workable solutions for the prevention and detection of criminal activity on the Internet. The following countries were represented: Russia, England, France, Germany, Italy, Russia, Japan, and Canada. This group is known as the G-8. *Id.*

97. Department of Justice, *at* http://www.usdoj.gov/criminal/cybercrime/agfranc.html (on file with University of Miami Inter-American Law Review)(last visited Mar. 29, 2000)[hereinafter Keynote Address].

98. DOJ Cybercrime Report, *supra* note 95.

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

provide a safe haven for cyber criminals.[107] This severely hampers detection and prosecution efforts.[108]

Third, law enforcement faces new procedural challenges that are nearly impossible to address without international concurrence and cooperation.[109] Consider the difficulty associated with locating a hacker whose transmission passes from his computer to a local Internet service provider, then through a telephone network, then across an ocean via satellite, and then passes through a university computer on its way to a corporate victim. To make matters worse, this hacker could be in his car, using wireless communications. How do we go about finding this individual? How do we collect the evidence and preserve it in a way that will be useful at trial?

Governments of the Americas must agree on a set of policies regarding cyber crime. Measures being taken to increase Internet use will be countered if online crime is permitted to run rampant. The G-8 produced a list of principles that is highly instructive on this issue.[110]

American governments must collectively determine what kinds of activities are considered cyber crimes.[111] Additionally,

---

107. *Id.*

108. *Id.*

109. *Id.*

110. Department of Justice, *at* http://www.usdoj.gov/criminal/cybercrime/principles.html (on file with University of Miami Inter-American Law Review)(last visited Mar. 29, 2000). Those principles are: "(1) There must be no safe havens for those who abuse information technologies. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred. (2) Law enforcement personnel must be trained and equipped to address high-tech crimes. (3) Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized. (4) Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime. (5) Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime. (6) Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the state where the data resides. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed. (7) To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence. (8) Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts."

111. FTAA Joint Government-Private Sector Committee of Experts on Electronic Commerce, Criminal and Civil Responsibility in Electronic Commerce, *at* http://www.ftaa-alca.org/SPCOMM/note_ece.asp#issue (1999)(last visited Jan. 25, 2001).

consideration should be given to what, if any, liability should be placed on Internet service providers when the applicable crime relates to the distribution of illegal material.[112] Further, these countries must decide what legal instruments are available that can be applied in a mutually agreeable way to combat criminal activity.[113]

V. CONCLUSION

Our world is shrinking. Today, private data can be shipped almost instantaneously to any corner of the globe. Cryptographic innovations permit users to communicate anonymously. This anonymity facilitates the commission of criminal acts. Additionally, cyber criminals can act from the privacy of home with just a few clicks of the mouse.[114] These are only a few of the most pressing issues presented by the Internet.

Physical boundaries are stepping aside. The Internet permits a quick and bountiful flow of information.[115] In addition, it allows consumers and businesses from different continents to interact in an unprecedented manner. A global marketplace is already emerging and is expected to grow exponentially over the coming years.[116] The unfortunate partner to this relatively new technology is the capability to commit harmful acts anonymously and quickly.[117]

In order to respond to the inevitable changes brought on by the Internet, American countries must acknowledge the age-old adage that two are better than one and regulate collectively. A cohesive American bloc will be stronger than any one American nation standing alone. In order to produce regulations that will be effective upon implementation, American countries must work together. These countries should establish regulations that are

---

112. *Id.*

113. *Id.*

114. Keynote Address, *supra* note 97.

115. *Reno*, 929 F.Supp. at 830.

116. "[Two hundred] million people will use the Internet regularly by the year 2000 and. . .electronic commerce will amount to more than three trillion U.S. dollars by the year 2005." *See* Christopher Hoffman, *Encrypted Digital Cash Transfers; Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations*, 21 FORDHAM INT'L L.J. 799, 805 (1998).

117. David A. Petti, *An Argument For the Implementation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703, 705-6 (1998).

broad enough to meet the various cultural and political differences among American governments. On the other hand, the regulations should be narrow enough to have a tangible effect. The balance has already been examined in Inter-American efforts such as NAFTA, MERCOSUR and FTAA.[118] Those agreements are highly instructive and should be used as building blocks for an effective set of Inter-American Internet regulations.

M. LEIGH MACDONALD*

118. NAFTA, *supra* note 19; MERCOSUR, *supra* note 20; FTAA Principles, *supra* note 21; Recommendations, *supra* note 22.

* Juris Doctor Candidate, May 2001, University of Miami School of Law. The author extends her gratitude to Professor Keith S. Rosenn for his guidance and encouragement. Special thanks to Brian and Jake for your endless love and support.