International Journal of Communications Law & Policy

Special Issue Global Flow of Information, Autumn 2005

TO SIGN OR NOT TO SIGN ON THE ELECTRONIC DOTTED LINE: THE UNITED STATES, THE RUSSIAN FEDERATION, AND INTERNATIONAL ELECTRONIC SIGNATURE POLICY

By Lyombe Eko[1] and Natasha Tolstikova[2]

ABSTRACT

This article compares the regulation of electronic signatures (e-signatures) in the United States and the Russian Federation as unique forms of communication that are the subject of international policy transfer through the framework of the United Nations Commission on International Trade Law (UNCITRAL). The aim was to determine the extent to which American and Russian legislation on e-signatures adhere to, or incorporates e-signature principles set forth in, the UNCITRAL Model Law on Electronic Signatures. It was found that the U.S. has embraced UNCITRAL e-signature principles and actively promotes their globalization. In contrast, the Russian Federation adopted a posture that is at variance with UNCITRAL's globalist principles, opting for a closed, home–grown e-signature system. The e-signature policies of the U.S. and the Russian Federation are consistent with each country's historical, political, and economic realities. Thus, even in an age of globalization, nation states succeed in putting their national imprint on the Internet in general, and on e-commerce in particular.

INTRODUCTION

In October 2004, the American Federal Bureau of Investigation (FBI), announced that 30 members of an Eastern European cybercrime ring had been arrested following a three-year joint investigation with the British National Hi-Tech Crimes Unit.[3] The FBI claimed that these cyber-crooks from the Russian Federation and other parts of the former Soviet Union cracked into the computer systems of banks, financial institutions, credit card processing companies and Internet service providers. They then wrote computer viruses that would "take over" the computers. From their Eastern European base, these criminals proceeded to "phish," that is to deceive computer users into believing that the criminals represented the companies whose computers they had compromised or taken over. They then fraudulently obtained passwords, credit card numbers, and other private data.[4] The FBI blamed the success of these cyber-criminals

[1] School of Journalism and Mass Communication, University of Iowa, E322 Adler Journalism Building, Iowa City, Iowa 52242. E-mail: Leo-eko@uiowa.edu.
[2] Department of Communication and Journalism, University of Maine, 5724 Dunn Hall, Orono, Maine 04469-5724. E-mail: Natasha@maine.edu.
[3] *See* John Swartz, *Crooks Slither into Net's Shady Nooks and Crannies*, USA TODAY, Oct. 21, 2004 at 1b.
[4] *See* Jeremy Wagstaff, *Gone Phishing: Web Scam Takes Dangerous Turn*, WALL ST. J., May 27, 2004 at B1.

on poor computer and Internet security, and the ease with which the Internet could be used to commit crimes around the world.[5]

Barely two months later, the Russian Interior Affairs Ministry announced the conclusion of its investigation into the largest credit card fraud case in the country's history. In effect, the Russian police and the Federal Security Bureau (FSB) had broken a syndicate that hacked into the computers of large banks, stole databases, and then used stolen client information to manufacture fraudulent Visa, MasterCard and American Express credit cards which were subsequently sold to criminals in several countries. This resulted in the theft of thousands of identities, which were then used to make fraudulent purchases around the world.[6]

These two cases show two dimensions of a major international issue – cyber insecurity.[7] The transformation of the Internet into a global information, multi-communication and e-commerce space in the 1990s led to a need for increased security, which is operationalized as confidentiality, integrity, and availability of computer systems and databases.[8] One solution was the use of e-signatures in communications and e-commerce. Electronic signatures range from typed e-mail signatures to digital signatures (a unique string of numbers or characters, or a combination of both) that are linked to another series of numbers generated through complex mathematical algorithms or operations made possible by encryption technology.[9]

Electronic signatures are a by-product of technological and media convergence – the amalgamation of the traditional media of mass communication with information and telecommunication technologies. As such, they are unique "invisible and inaudible" elements of the communication "infrastructure" that facilitate the smooth running of virtually all "visible and audible" information and communication systems.[10] Electronic signatures are crucial for the problem-free operation of organizational and mass communication systems, intranets, circuit and packet-switched telecommunications, satellite and terrestrial communication, as well as interpersonal communication. The

[5] *See* John Swartz, *supra* note 3.

[6] *See Special Services Expose the Largest Credit Card Fraud in Russia's History*, PRAVDA.RU, Dec. 22, 2004 (Dmitry Sudakov trans.), *available at* http://english.pravda.ru/accidents/21/96/383/14751_cards.html (last visited on Aug. 15, 2005); *see also* CHARLES PFLEEGER & SHARI L. PFLEEGER, SECURITY IN COMPUTING 589 (3d ed.) (2002).

[7] *See* PFLEEGER & PFLEEGER, *supra* note 6 (suggesting that computer crime is a complicated international problem and that computer security regulation is an international issue).

[8] *Id.* at 9, 314-323 (stating that the security requirements for computer and databases include: physical database integrity (the physical database is free of technical problems), logical database integrity (the structure of the database is intact), element integrity (the data contained in the database are accurate), auditability (the ability to track who has accessed or modified elements in the database), access control (users are allowed access only to authorized data), user authentication (every user is positively identified), and availability (this is the opposite of "denial of service" since users can access both the database and all data that they are authorized to have access)).

[9] *See* Gregory Passman, *The Electronic Age is almost Upon* Us, 229 N.Y. L. J. 1 (2003); *see also* PFLEEGER & PFLEEGER, *supra* note 6, 80-82.

[10] In the traditional Source Message Channel Receiver (SMCR) model of communication, electronic signatures play a crucial role. They would be used to encode the message before it is sent through the communication channel and used again to decode the message such that it makes sense to the receiver. For a description of the SMCR model. *See* JOSEPH STRAUBHAAR & ROBERT LAROSE, MEDIA NOW: COMMUNICATIONS MEDIA IN THE INFORMATION AGE 15 (2000).

importance and ubiquitous nature of e-signatures make them crucial parts of the infrastructure in global communications and e-commerce. Hence, the United Nations has sought to transfer the e-signature policy developed under the ambit of UNCITRAL to its 191 member-countries.

Additionally, convergence of information and telecommunication and mass media technologies has facilitated both the globalization of the world's economic and communications systems, and the growth of global media conglomerates. It has also led to the globalization of cybercrime.

For cybercrime to attack global communications and electronic trade requires secure and stable infrastructure, as well as a predictable international e-commerce regulatory regime. Electronic signatures provide security– *i.e.* confidentiality, availability, integrity, and reliability – on the Internet, which has become a multi-billion dollar communication and economic space.

* * *

The aim of this article is to compare and contrast the regulation of e-signatures in the United States and the Russian Federation from an international policy transfer perspective. In other words, we will attempt to determine how each country's e-signature policy– *i.e.* their respective choices of technology, governmental control, and internationality – incorporate or reflect the principles set forth by UNCITRAL as a *sine qua non* for harmonious global e-commerce.

The framework for comparison of the U.S. and Russia is developed from the UNCITRAL Model Law on Electronic Signatures. It contains the following elements: technological neutrality, non-discrimination between domestic and foreign e-signatures, and the international origin of the Model Law.[11] Additionally, the e-signature statutes of the U.S and Russia are compared and contrasted with a view to determining if policy was transferred from the U.N. to both countries, as evidenced by their adherence or non-adherence to the UNCITRAL principles.

The research questions that guide this study are as follows:

1. Does the U.S, the world's richest nation, regulate e-signatures differently from the Russian Federation?
2. Are the e-signature regulatory regimes of both countries the result of policy transfer from UNCITRAL?

This article suggests that in light of developments in the field of telecommunications, the UNCITRAL Model Law on Electronic Signatures follows the international communication modeldeveloped in the nineteenth century. This model consisted of the harmonization and interconnection of transborder communication systems through multilateral agreements. Furthermore, international institutions such as the International Telecommunication Union (ITU) transferred policies developed by powerful countries to weaker ones, with the tacit agreement of the latter.[12] The aim of the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures is the harmonization and standardization of contemporary

[11] *See* G.A. Res. 56/80, U.N. GAOR, 85th Sess., Supp. No. 17, annex, Guide to Enactment, para 27, U.N. Doc. A/RES/56/80 (2001), *available at* http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (last visited Aug. 15, 2005).

[12] *See* ROBERT FORTNER, INTERNATIONAL COMMUNICATION 73-75 (1993).

international e-commerce policy in order to transform the Internet into a global open-market system. We submit that the U.S., which is known for its isolationist and unilateralist posture in international affairs, actively promotes UNCITRAL's model law on e-commerce because the law is an instrument of globalization that supports its free-trade values.

Part I of this article discusses efforts by the U.N. and the U.S. to bring the regulation of e-commerce within the ambit of a harmonized and globalized international trade-law regime. Part II discusses the legal and policy-transfer perspectives on this subject. Part III then surveys the American regulation of e-signatures within the context of the country's neo-mercantilist regulatory policy, while Part IV discusses the history and political context of information technology and Internet regulation in the Russian Federation. Finally, Part V compares and contrasts the regulatory regimes of the U.S and Russia in light of the UNCITRAL Model Law on Electronic Signatures.

The aim of this comparison is to demonstrate that the coincidence of policy options between the U.N. and the U.S. in matters of e-commerce and e-signatures does not result from policy transfer from the U.N. (UNCITRAL) to the U.S. Despite the noble ideals of its promoters, the transfer of e-signature policy by the U.N. and the U.S. is a complex affair. This is because not only does law possess a social context, but each new technology regulation creates its own new socio-cultural context.[13]

The Internet, Electronic Commerce & Electronic Signatures: A Global Perspective

The Internet is an interconnected, redundant, "system of systems" or network of computer networks exchanging information in self-contained packets.[14] It spans the length and breadth of the globe. The invention in 1990 of the World Wide Web made the Internet a truly global phenomenon.[15] The Internet was transformed, in a relatively short period, into a virtual, interactive, global, multi-communication platform. No other communication medium has had such an explosive growth in such a short time.[16] Within a short period of time, the Internet became such a highly commercialized, corporate-

[13] See David Nelken, Comparatists and Transferability, in PIERRE LEGRAND AND RODERICK MUNDAY (EDS.) COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 437,452 (2003).

[14] See NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, ARPANET HOST-TO-HOST ACCESS AND DISENGAGEMENT MEASURES 2-3 (1978). See also, DEPARTMENT OF DEFENSE, DOD SCIENCE AND TECHNOLOGY SUCCESS STORIES (1998) (Technologies developed by the Department of Defense, namely, packet-switching, Transmission Control Protocol/Internet Protocol (TCP/IP) paved the way for the World Wide Web).

[15] See TIM BERNERS-LEE, THE WORLD WIDE WEB, A PERSONAL HISTORY (Last visited on October 2, 2005) <http://www.w3.org/people/Berners-lee> See also European organization for nuclear Research (CERN) <http://www.public.web.cern.ch/public/ACHIEVEMENTS/web.html> (WEB SITE NOT FOUND)last visited August 12, 2002.

[16] See Robert Cailliau, A Little History of the World Wide Web (1995) at <http://www.w3.org/History.html> (Last modified Nov. 24, 2002, Last visited on October 2, 2005)(The World Wide Web Protocol was invented in 1990 and by 1993, there were 50 Hyper Text Transfer Protocol (HTTP) servers in the world. Only 0.1% of National Science Foundation traffic was on HTTP in March 1993. Today, http is the norm).

dominated multi-communication sphere– the virtual walled domain of global commerce and capitalist economics[17] – that some scholars decried its excessive commercialism and consumerism. [18] The theoretical and ideological underpinnings of the role of the Internet in the global society in general and the global economy in particular came from the U.S., where ideological concepts such as the "computer networks," the "information society," the "information superhighway," the "global information infrastructure," and the "new economy" were coined.[19]

The political, economic, and cultural differences between the nations of the world have given rise to a number of Internet regulatory models that correspond with their respective political, economic, social and cultural contexts and realities.[20] This is especially true of electronic or e-commerce: trade, banking, fund transfers, publishing, auctions, gaming, and myriad other business transactions and economic relationships that take place in whole or in part on the Internet.

The Clinton Administration conceptualized the Internet as an open, capitalist market place, and set the tone for global e-commerce. In 1997, the administration offered the world its vision of the Internet as a market-driven multi-communication space, and appealed to governments to assume a minimalist regulatory posture towards e-commerce,[21] thereby giving Adam Smith's invisible hand a chance to work its magic in the new multi-communication space.

The linkage of information and communication technologies with the free market was officially endorsed by the U.N., and globalized within the framework of UNCITRAL. Under the aegis of the U.S., the world's principal hegemony,[22] UNCITRAL advanced, and the United Nations General Assembly adopted, model laws on e-commerce and e-signatures. These model laws essentially globalized the free-trade values of the Commerce Clause of the U.S. Constitution[23] – namely, the elimination of impediments to the smooth flow of goods and services between the states.

---

[17] See generally DAN SCHILLER, DIGITAL CAPITALISM: NETWORKING THE GLOBAL MARKET ECONOMY (1999).

[18] See Robert LaRose and Matthew S. Easton, Is Online Buying out of Control? Electronic Commerce and Consumer Self-regulation, 46 JOURNAL OF BROADCASTING AND ELECTRONIC MEDIA 549 (2002).

[19] See ROBERT BURNETT & P. DAVID MARSHALL WEB THEORY 128 (2003)(Suggesting that the ideology of information technology originated within the free market context of United States through federal governmental and private industry initiatives).

[20] See Lyombe Eko, Many Spiders, One World Wide Web: Towards a Typology of Internet Regulation, 6 COMM. L. & POL'Y 448 (2001)(Suggesting that the Internet is regulated world wide according to a five-part typology: Internationalist, neo-Mercantilist, Culturalist, Gateway & Developmentalist).

[21] See WILLIAM J. CLINTON AND ALBERT GORE, JR., A FRAMEWORK FOR ELECTRONIC COMMERCE 5 (1997)(This *laissez-faire* approach would be global, merchantilist, decentralized, contractual, competitive, transparent and protective of intellectual property).

[22] See Sandra Braman, The Process of Emergence, in SANDRA BRAMAN (ED.) THE EMERGENT GLOBAL INFORMATION POLICY REGIME 1-11 (2004) (Suggesting that all nations are not the same on the world stage).

[23] United States Constitution, Article 1, § 8. cl. 3.

As a result of the so-called "dot-com revolution,"[24] e-commerce quickly evolved to include sophisticated world-wide business-to-consumer and business-to-business commercial transactions ranging from global commodity features and off-shore banking to complex transnational transactions involving pornography and pharmaceutical products.

With the collapse of communism and the Soviet Union, the Russian Federation tentatively allowed the Russian Institute for Public Networks (RIPN) to be connected to the Internet in 1992. Russia soon joined the global Internet governance and management system created by the U.S. government and contracted, first to the Internet Agency for Assigned Names and Numbers (IANA), and subsequently to its successor the Internet Corporation for Assigned Names and Numbers (ICANN). [25]

The Internet and the Policy Transfer Perspective

The work of the U.N. and other international organizations in setting global standards for human rights, good governance, transparency and accountability in financial management, institution-building in the developing and transitional (mostly Eastern European) countries of the world, and the harmonization and standardization of international trade law, among other activities, has been described as policy or legal transfer.[26] The policy transfer perspective refers to "a process in which knowledge about policies, administrative arrangements, institutions and so on, in one time and/or place is used in the development of policies, administrative arrangements and institutions in another time or place."[27] Powerful nations or international organizations generally transfer policies to poorer nations making the transition from communism or authoritarianism to democracy, mostly in Eastern European countries. Policy transfer takes place within the framework of political or economic cooperation, assistance, or development aid.[28] Thus, policy transfer usually takes place in situations involving unequal power dynamics. David Nelken, who prefers the term "legal transfer," rightly states that policy or legal transfers are generally imposed as part of colonial domination (and post-independence neo-colonial arrangements), or are otherwise invited, adopted or borrowed for purposes of change. He adds that policy and legal transfer results from

[24]See Matthew P. McAllister and Joseph Turow, New Media and the Commercial Sphere: Two Intersecting Trends, Five Categories of Concern, 46 JOURNAL OF BROADCASTING AND ELECTRONIC MEDIA 505 (2002).

[25] The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for IP address space allocation, protocol parameter assignment, domain name system management, and management of the Internet root server. Information available at <http://www.icann.org/> (last visited April 2003).

[26] Id at 458-459 (Suggesting that legal transfer takes place through processes involving the spread of standards and regulations through harmonization, conventions, regional agreements and so on).

[27] See David Dolowitz & David Marsh, Who learns what from whom: A Review of Policy Transfer Literature, 44 POLITICAL STUDIES 343, 344 (1996).

[28] Id.

efforts by powerful countries to harmonize or standardize the dominant standards, rules, regulations, and policies at the international and regional levels.[29]

The U.N., through its communications activities as well as those of its specialized agencies, has been one of the main catalysts of policy transfer and globalization. Indeed, at its creation, the U.N. was viewed in part as a "communication operation of explicit global purpose."[30] The U.N.'s successful international policy and legal transfers include: the globalization of human rights, of which freedom of speech and of the press is one of the most fundamental,[31] as well as development communication.[32] Additionally, the U.N. has reshaped the economies, telecommunications policies, and institutions of dozens of developing countries through the International Monetary Fund (IMF) and The World Bank,[33] the United Nations Development Program (UNDP)[34] and International Telecommunications Union (ITU) Internet development programs.

Furthermore, the powerful nations of the world have often used the U.N. and its specialized agencies to promote their interests, ideals, policies, and visions of the world.[35] The U.S. has perhaps used the U.N. more than any other country to promote its interests and ideals. [36] Former Secretary of State Alexander Haig told the U.N. General Assembly that U.N. ideals were also American ideals, because the U.N. charter embodies American principles.[37] Geske[38] and Wendt[39] place national interests and institutions with international structures of power and authority in one self-propagating nexus. Writing in different contexts, both authors suggest that the national interests of the U.S. and other powerful nations are in part a product of the international structures, institutions, and

---

[29] See David Nelken, Comparatists and Transferability, in PIERRE LEGRAND AND RODERICK MUNDAY (EDS.) COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 437,457-459 (2003).

[30] See Daniel Lerner, Is International persuasion Sociologically Feasible? In RONALD MCLAURIN, CARL ROSENTHAL, & SARAH SKILLINGS (EDS.) 47, 50 (1976).

[31] See Articles 13, 55, 56, 62, 68 & 76, Charter of the United Nations (1945). See also The Universal Declaration of Human Rights, A/RES/217 A (III),; U.N. Doc A/810 at 71 (1948).

[32] U.N. GAOR, Communication on Information from Non-Self-Governing Territories, U.N. Doc A/AC/35/SR 180 (1958) (The UN pioneered the use of the mass media to promote development in colonized and newly decolonized countries. This became an important objective of UNESCO). See also WILBUR SCHRAMM, MASS MEDIA AND NATIONAL DEVELOPMENT 114 (1964).

[33] See John Toye, The International Monetary Fund (IMF) and the World Bank, in JONATHAN MICHIE, THE HANDBOOK OF GLOBALISATION 360 (2003)(Stating that during the Latin American debt crisis of the 1980s, the United States "recruited the Fund, along with the Bank, to be its managers…of the prolonged debt crises which for some years threatened the survival of major Western Banks").

[34] See UNDP Sustainable Development Networking Programme <Http://www.sdnhq.undp.org/about/> - WEB SITE NOT FOUND(visited October 2004).

[35] See John Gerard Ruggie, The United States And The United Nations: Towards A New Realism, In PAUL F. DIEHL, (ED.). THE POLITICS OF INTERNATIONAL ORGANIZATIONS 396, 405 (1989) (Suggesting that at the ITU, the United states and the industrialized Western countries determine policies that further their nation interests to the detriment of poorer countries).

[36] See Donald J. Puchala, American Interests And The United Nations, In PAUL F. DIEHL, (ED.). THE POLITICS OF INTERNATIONAL ORGANIZATIONS 410-428 (1989).

[37] Id at 410.

[38] See M. Geske, Globalization Is What States Make Of It: Constructivism, U.S. Foreign Economic Policy And The Peso Crisis, 37 INTERNATIONAL POLICY 301 (2000).

[39] See A. Wendt, Anarchy Is What States Make Of It: The Social Structure Of Power Politics, 46 INTERNATIONAL ORGANIZATION 391 (1992).

processes that were created and set in motion to protect and promote these national interests.

The activities of UNCITRAL in drafting model laws on e-commerce and e-signatures are examples of unique forms of policy and legal transfer *par excellence*. In the field of information and communication technology, UNCITRAL is one of the U.N.'s main instruments of international trade policy transfer. Since the 1960s when it was created, UNCITRAL has had a mandate to work towards the progressive harmonization and unification of international trade law.[40] As early as 1985, UNCITRAL adopted a recommendation on the legal value of computer records, and the U.N. called on its member states to take action in conformity with the recommendations of the commission in order to ensure the security of computer data processing in international trade.[41]

The revolutionary expansion of the Internet around the globe and the unprecedented diffusion of e-commerce, coupled with regulatory unpredictability in the new commercial space, led the U.N. to attempt to canalize and influence global e-commerce regulation. Pursuant to this mandate, UNCITRAL set out to bring the multi-billion-dollar global e-commerce industry within the ambit of international trade law through two model laws: the UNCITRAL Model Law on Electronic Commerce,[42] and the UNCITRAL Model Law on Electronic Signatures.[43] These model laws set forth international principles, norms and standards designed to "assist in shaping a more harmonious commercial practice in cyberspace"[44] through homogenization of the regulation of global e-commerce.

The model laws are a massive policy transfer project. UNCITRAL conceptualizes its model laws– and these are drafted in the form of legislative texts that U.N. member states are urged to incorporate into their national laws – as tools for harmonizing the disparate trade laws that exist around the globe. The aim of the UNCITRAL Model Law on Electronic Commerce is "to offer national legislators a set of internationally acceptable rules as to how… a more secure legal environment may be created for what has become known as "electronic commerce.""[45] States are urged to modify or leave out some of the provisions of the model laws as they see fit. However, they are also urged to make as few changes as possible in incorporating model laws into

---

[40] G.A. Res. 2205 (XXI), UN GAOR, 21ST Session, U.N. Doc A/RES/2205 (XXI) (1966).

[41] See OFFICIAL RECORDS OF THE GENERAL ASSEMBLY, FORTIETH SESSION, A/RES/40/71 PARA 5(B) (1985).

[42] G.A. Res. 51/162, UN GAOR 51st Session, Supp. No. 17, annex, U.N. Doc, A/RES/51/162)(1996); See also DAYA KISHAN THUSU, INTERNATIONAL COMMUNICATION 265 (2000) (Electronic commerce is the "production, advertising, sale and distribution via electronic networks, specifically the Internet").

[43] G.A. Res. 56/80, UN GAOR 85th Session, Supp. No. 17, annex, U.N. Doc. A/RES/56/80 (2001)(The very definition of the term "electronic signatures" is problematic and varies from country to country. The definition is part of the analysis. Suffice it to say at this juncture that electronic signatures are numbers generated as part of data security, by special software using complex algorithms. These paperless instruments are used to authenticate business transactions).

[44] See PARA 4, GUIDE TO ENACTMENT, UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE A/RES/51/162 (1996) at <http://www.uncitral.org/eng-index.htm (last visited June. 10, 2004)

[45] id PARA 2,

their legal systems.[46] Indeed, states are "strongly encouraged to inform the UNCITRAL secretariat of any enactments of the New Model Law (or any other model law resulting from the work of UNCITRAL)."[47] In order to facilitate policy transfer, UNCITRAL offers states technical consultations and training in the preparation of legislation based on the Model Law on Electronic Signatures and Electronic Commerce among others.[48]

The main policy feature that the U.N. attempted to transfer and globalize in both of the UNCITRAL model laws dealing with the Internet is the recognition of e-signatures as "functionally equivalent to handwritten signatures."[49] UNCITRAL saw the Model Law on Electronic Commerce as a useful tool for interpreting existing international conventions and other international instruments that create legal obstacles to e-commerce, especially those that stipulate that contracts, or certain clauses thereof, be in written form.[50] The model laws are only recommendations that are not binding under international law. However, the fact that they were adopted by the U.N. General Assembly gives them a cachet of international legitimacy.

Since the U.N. adopted the UNCITRAL model laws, the U.S. and the Russian Federation, the successor state to the Soviet Union, have enacted legislation regulating e-signatures in their respective jurisdictions.[51] The U.S. passed the Electronic Signatures in Global and National Commerce (E–Sign) Act,[52] while the Russian Federation, which had divested itself of communist ideology and had become classified as an emerging market economy, [53] embraced the Internet[54] and enacted a comparable law on e-signatures, the Law on Digital Electronic Signatures.[55] These were momentous developments for global economic cooperation and trade, given the recent political, economic, cultural, and geo-strategic rivalries between the two erstwhile Cold War adversaries. However, despite their active participation in the drafting of the UNCITRAL model laws, [56] the e-signature

[46] id PARA 26.
[47] id. PARA 5.
[48] Id PARA 84.
[49] See Art. 7, G.A. Res. 51/162, UN GAOR 51st Session, Supp. No. 17, annex, U.N. Doc, A/RES/51/162)(1996).
[50] See PARA 11, GUIDE TO ENACTMENT, UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE A/RES/51/162 (1996) at <http://www.uncitral.org/eng-index.htm> (last visited June. 10, 2004) – WEB SITE NOT FOUND
[51] See Andrew Berman, International Divergence: The "Keys" to Signing on the Digital Line–The Cross-Border Recognition of Electronic Contracts and Digital Signatures, 28 SYRACUSE J. INT'L L. & COM. 125 (2001)(Describing Electronic Signatures and suggesting that a global regulatory scheme would be the best for e-commerce).
[52] 15 U.S.C § 7001 et seq (2000).
[53] See FRANK ELLIS, FROM GLASNOST TO THE INTERNET: RUSSIA'S NEW INFOSPHERE 62, 88 (1999).
[54] See *Minister Reports Communications, IT Technologies Boom in Russia in 2002*, BBC MONITORING, March 5, 2003, LEXIS-NEXIS. See also *Leading Russian Portal Posts First Profits*, BBC MONITORING, November 7, 2002, LEXIS-NEXIS.
[55] Law No. 1-FZ of January 10, 2002 on Digital Electronic Signatures, Rossiyskaya Gazeta No.6. of January 12, 2002.
[56] U.N GAOR Report of the UNCITRAL Working Group on Electronic Signatures 37th Sess. U.N.Doc A/CN.9/483 (2000) (Both The United States and the Russian Federation are members of the UNCITRAL Working Group on Electronic Signatures that drafted the model laws).

laws of both countries are so different that they warrant a heuristically stimulating comparative analysis.

Regulation of Electronic Signatures in the United States

As the "birthplace" of the Internet, the U.S. has put its capitalist, free-market regulatory stamp on the Web's multi-communication environment. In the U.S., e-commerce and e-signatures are regulated at both the federal and state levels. As early as 1997, the Clinton Administration offered the world a vision and framework for the expansion and regulation of e-commerce. This was a capitalist, free-market framework under which governments were to assume a minimalist regulatory posture towards electronic commerce.[57] Indeed, the administration hailed the UNCITRAL Model Law on Electronic Commerce as soon as it was adopted by the U.N. General Assembly, and urged all nations to pattern their e-commerce regulation after the UNCITRAL model law.[58]

Additionally, the Clinton-Gore framework anticipated legislation on e-signatures. It stated that there was no single "magic" technology that would provide privacy for personal information, or security for data and communications. However, it recommended a "market-driven, key management infrastructure" that could not be used by criminals and terrorists to thwart legitimate law-enforcement surveillance.[59] While the framework advocated a specific technology – key management infrastructure – for communications and data security, the development of other technologies has led the U.S. to advocate a new, technology-neutral policy.

The Clinton-Gore framework reflected America's capitalist, commercial system in which the Internet is conceptualized as a market place for all kinds of goods and services. In this neo-mercantilist scheme of things, the role of the government was limited to creating an enabling environment that not only ensured the free flow of goods, services and information on the Internet, but also took affirmative steps to remove impediments to that flow. This *laissez-faire* regulatory model combines several libertarian principles, namely First Amendment protection,[60] free trade,[61] the marketplace of ideas,[62] and the free flow of goods and services across state lines.[63] Above all, this framework represented the active Americanization of global Internet governance in the country's economic self-interest.[64] The Clinton Administration promoted the diffusion of

[57] See *supra* note 28 (Suggesting that this *laissez-faire* approach would be global, mercantilist, decentralized, contractual, competitive, transparent and protective of intellectual property).
[58] Id. at 10-11.
[59] Id. at 20 (the Clinton-Gore administration essentially recommended key recovery encryption in 1997).
[60] See Reno v. ACLU, 521 U.S. 844 (1997).
[61] See ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS 175-176, 194 (1776) (Trade is the source of law, order, good government).
[62] See Abrams v. United States, 250 U.S. 616 (1919) (The United States is a marketplace of ideas where truth and falsehood wrestle and truth carries the day).
[63] See Lyombe Eko, *Many Spiders, One World Wide Web: Towards a Typology of Internet Regulation*, 6 COMM. L. & POL'Y 448 (2001).
[64] See PETER R. MONGE & NASSIR CONTRACTOR, THEORIES OF COMMUNICATION NETWORKS 142 (2003) (Suggesting that self interest is a motivation for action in networks like the Internet).

America's free-market system around the world because it is inextricably linked to American and Western European media conglomerates and multinational corporate interests,[65] which have a stake in a seamless global economy where the fluid exchange of goods, services, information, intellectual property, and capital would increase business opportunities and profitability.[66]

The most significant piece of American legislation designed to promote e-commerce at the global and national levels is the Electronic Signatures in Global and National Commerce Act (hence the E-Sign Act).[67] The act is based on a model in which self-regulatory organizations, which are neither federal agencies nor state entities, adopt and administer rules applicable to e-commerce. Governments are not involved in the verification, notarization or acknowledgment of e-signatures.

The E-Sign Act built on regulatory activities at the state level. In effect, in 1999, the National Conference of Commissioners of Uniform State Laws (NCCUSL) and the American Law Institute approved a model law, the Uniform Electronic Transactions Act (UETA), and recommended it be enactment in all 50 states.[68] By mid-2003, virtually all states had enacted some version of UETA,[69] which, together with the E-Sign Act, constitute the edifice of e-signature regulation in the U.S. The regulation of e-commerce to promote competition in the free marketplace is part and parcel of the American constitutional and neo-mercantilist ideology.

Ironically, U.N.'s promotion of international homogenization and standardization of international trade law is tantamount to globalization of the spirit and values of the Commerce Clause of the U.S. Constitution, [70] which gives Congress the power to regulate interstate commerce – all trade that includes more than one state – and remove all impediments to that commerce. At the international level, the principal objective of the U.S. is to open up markets and avenues of capital flows around the world for American media conglomerates and multinational corporations. The UNCITRAL model law on Electronic Signatures and the E-Sign Act are intended to facilitate payment options for American companies, which do business in the global electronic market. At the same time, in a classic display of national self-interest, the U.S. jealously guards its own sovereignty and markets.[71]

---

[65] See Vincent Miller, *Stitching the Web into Global Capitalism: Two Stories, in* DAVID GAUNTLETT & ROSS HORSLEY, WEB STUDIES 171-184 (2d. ed., 2004) (Suggesting that the development is tied to commercial interests which have used it as a marketing and distribution system that lends to corporate dominance or oligopolies).

[66] See ARMAND MATTELART, THE INFORMATION SOCIETY 138 (2000) (Suggesting that the aim of the information society is to facilitate "frictionless capitalism").

[67] See 15 U.S.C. § 7001 et seq. (2000).

[68] See NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM ELECTRONIC TRANSACTIONS ACT (1999).

[69] See Uniform Electronic Transactions Act (UETA) State-By-State Enactment Chart (2003) (at http://www.bmck.com/ecommerce.uetacomp.htm.) (last visited October 20, 2003). See also Andrew Berman, *International Divergence: The "Keys" to Signing on the Digital Line–Cross–Border Recognition of Electronic Contracts and Digital Signatures*, 28 SYRACUSE J.INT'L L. & COM. 126 (2001).

[70] See U.S CONST. art. 1, § 8., cl. 3.

[71] See GEORGE SOROS, OPEN SOCIETY xv (2000) (Suggesting that the United States is willing to enter into multilateral arrangements that open world markets and protect American vested interests but the U.S. is unwilling to make compromises that affect its own internal affairs).

Political and Cultural Context of the Regulation of Electronic Signatures in the Russian Federation

When it comes to information and communication technologies, the Russian Federation has undergone a revolutionary change since it emerged from the ruins of the Soviet Union in 1991. It now has what Frank Ellis calls a "new infosphere," a radically different situation from the more than 70 years of strict governmental information control under the Soviet Communist Party.[72] A survey of the country's information technology history will shed some light on the magnitude of the Russian information revolution and provide context for the discussion of the regulation of e-signatures.

The Soviet Union was a pioneer in space exploration and satellite telecommunications research. Its early technological feats included putting the world's first artificial satellite, Sputnik, into orbit in 1957,[73] and sending a cosmonaut, Yuri Gagarin, on humankind's first orbital flight in 1961. For all their breakthroughs in space science and rocketry, the Soviets were not major innovators in computer and information technology. The country had no equivalent to the decentralized American Advanced Research Projects Agency Network (ARPANET).[74] The press in the Soviet Union was highly centralized, tightly controlled and authoritarian,[75] and media outlets such as the newspaper *Pravda* (Truth) and Radio Moscow were organs of the Communist Party that were used to disseminate the Marxist ideology of class struggle, "democratic centralism"[76] and to fight against capitalism and imperialism.[77] The mass media were also heavily used for mobilization and agitation of the masses within the framework of Marxist-Leninist ideology.[78] The Soviet Union used its mass media to spread ideological propaganda not only within the country but also around the world.[79]

History of Information and Communication Technology in the Soviet Union and the Russian Federation

Science and technology in general, and information technology in particular, were ideological weapons in the hands of the Soviet Communist Party and Soviet leaders. When the first microprocessor was invented in the U.S. in the 1940s, Stalin made it one of his top priorities to develop comparable information processing technology in the

[72] See FRANK ELLIS, FROM GLASNOST TO THE INTERNET, 38, 139 (1999).
[73] See JOHN L. MCLUCAS, SPACE COMMERCE 18-20 (1991).
[74] ARPANET is known more popularly as the precursor to the Internet.
[75] See FREDERICK SIEBERT, THEODORE PETERSON & WILBUR SCHRAMM, FOUR THEORIES OF THE PRESS (1956) (The Soviet model is described as totalitarian).
[76] See Vladimir Lenin, *State And Revolution*, *in* ARTHUR MENDEL (ED.) ESSENTIAL WORKS OF MARXISM 103, 143 (1961) (Lenin envisioned democratic centralism as the transfer all means of production, namely, private railways, factories, land and the like to nation).
[77] See Arthur Mendel, *The New Program Of The Communist Party Of The Soviet Union, in id*.
[78] See DAVID WEDGEWOOD BENN, FROM GLASNOST TO FREEDOM OF SPEECH: RUSSIAN OPENNESS AND INTERNATIONAL RELATIONS 8 (1992).
[79] See MARTIN EBON, THE SOVIET PROPAGANDA MACHINE 3 (1987) (the Soviet mass media were used for agitprop—agitation and propaganda—indoctrination, and ideological education).

Soviet Union. In the 1950s, the MESM (Russian acronym for "Small Electronic Computer") was developed in Kiev. This was the first computer in continental Europe.[80] The MESM was a top-secret military project known to few outside the inner circles of Soviet power. [81] The intent to achieve ideological goals through the use of information technology was reiterated in 1961 by the Soviet Communist Party's official science and technology policy. The party encouraged research efforts aimed in part at "working out the theories and principles of designing new machines, automatic and tele-mechanical systems… intensely developing radio-electronics, elaborating the theoretical foundations of computing, [systems] control and information [technology] machines and improving them technically."[82]

This was during the height of the Cold War, when the Soviet Union sought military and scientific superiority over the U.S. and its allies. The Soviet Union sought access to Western technology for purposes of technological, industrial and military development and modernization.[83] The multi-system "Minsk-222," which became the basis for the country's computer networks, was unveiled in 1966. The first virtual computer network in the Soviet Union was "Siren," an automatic flight reservation and ticketing system that was launched at the offices of Aeroflot, the Soviet national airline, in 1972.[84] Soviet information and communication technology lagged behind that of the U.S. and most of its Western allies until the momentous historical events of the 1980s and 1990s that tore the country apart.

Perestroika and Glasnost

In 1985, Mikhail Gorbachev became the general secretary of the Communist Party of the Soviet Union. He launched a political strategy of *perestroika* (radical reform or restructuring). This policy included public criticism, or *glasnost*.[85] The word *glasnost* soon came to refer to unprecedented public criticism of the government and access to information. The August 1991 *coup d'etat* attempt against Gorbachev was a turning point in the history of the Soviet Union.

---

[80] See Sergei Aleksandrovich Lebedev, Sozdatel' Pervoi V Kontinental'noi Evrope Evm [S.A. Lebedev, Inventor Of The First Electronic Computer In Continental Europe], *available at* http://www.icfcst.kiev.ua/museum/Lebedev_r.html (last visited on October 2002); See also GEORGE HUSDON, SOVIET NATIONAL SECURITY POLICY UNDER PERESTROIKA 115 (1989).

[81] See R.I. Podlovchenko, "Ocherki Istorii Informatiki V Rossii" [*Essays On The History Of Informatics In Russia*] 4 (1999), *available at* http://archive.1september.ru/inf/1999/art/ocherk1.htm (last visited September 2002); See also D.A. Pospelov, *Ocherki Istorii Informatiki V Rossii (Development Of Computer Science In Russia), in* D.A. POSPELOV AND I. FET (EDS.) ESSAYS ON THE HISTORY OF INFORMATICS IN RUSSIA 7-44 (1998).

[82] See Mendel at 473, note 75, *supra*.

[83] See ANTONY SUTTON, WESTERN TECHNOLOGY AND SOVIET ECONOMIC DEVELOPMENT (1945-1965) 318 (1973) (Despite strict export controls, the Soviet Union was able to lease or purchase computer technology from American and British companies).

[84] See Khronologia Sobytii (1970-1974) [The Chronicle of Events (1970-1974)], NOTE: The whole web site is gone; CHECK WITH AUTHORS.

[85] See DAVID LANE, SOVIET SOCIETY UNDER PERESTROIKA 13 (1992).

It also revealed the existence of a hitherto unknown Russian computer network, Relcom/Demos.[86] Since the Soviet Union did not have a unified network of computers across the country, programmers working for research, educational and some military institutions created Relcom/Demos, an unofficial network based on the Unix operating system – obtained through clandestine sources – but running on Soviet mainframe computers.[87] This unofficial network, whose mission was to tackle problems associated with Unix, soon spanned the Soviet Union. Relcom/Demos had electronic mail, access to news groups, and by 1990 had established unofficial international links.[88]

Computer programmers used this network to transmit messages across the Soviet Union during the attempted coup. Relcom/Demos allowed Boris Yeltsin to e-mail information against the coup to all parts of the Soviet Union from his refuge in the Russian parliament.[89] For its part, the KGB tried unsuccessfully to use traditional information channels to promote the coup. The Relcom/Demos network was thus the instrument that ensured the survival of the transition from communism and added a global dimension to the communication situation in the Russian Federation.[90]

Internet Regulation in Russia

Russia's embrace of capitalist America's Internet, though tentative at first, was a second revolution that showed the country had repudiated its Marxist-Leninist economic and political ideology, if not its *modus operandi*. The Internet in Russia has the following regulatory characteristics: Internet Service Providers (ISPs) are required to register with the Russian Ministry of Communications and Informatics. ISPs also need to get a license from the government. Additionally, all telecommunications businesses — cybercafés, e-mail services, call centers and the like — have to be registered.[91] Furthermore, under the Law of the Russian Federation Concerning the Mass Media, teletex, video text and other telecommunications networks are considered media of mass communication. By law, all Web sites in the .ru (Russian) domain have to be registered (for a fee) with the Ministry of Press, Television, Radio Broadcasting, and the Means of Mass Communication.[92]

In 1995, the Federal Security Bureau (FSB), the successor to the KGB's domestic service, was given statutory authority to require all Russian communication service providers to install SORM (System for Investigations and Field Operations) hardware and software that routed all their Internet traffic through FSB facilities, ostensibly for law

[86] See Rafal Rohozinski, *How the Internet did not Transform Russia*, CURRENT HISTORY, October 2000 at 334.
[87] Id. at 336.
[88] Id.
[89] Id. at 334.
[90] See Benn, note 76, *supra* at 11.
[91] Art. 15, Law No. N15-FA of February 16, 1995 "On Telecommunications" Ross. Gazeta No. 39, of 22 February 1995, (amended by Law No. N8-FA of January 16, 1999 and Law No176-FA of July 17 1999).
[92] Art. 24, Law No. 2124-1 of December 27th, 1991, Concerning the Mass Media, Ross. Gazeta of February 8th, 1992 (amended July 25, 2002) (Web page registration is not being enforced because it is impractical to do so).

enforcement purposes.[93] In 1998, SORM-2, a more advanced telecommunications and Internet surveillance system, came into use.[94] In effect, the law gives the FSB the authority and technology to route all telecommunications and Internet traffic through its facilities for purposes of monitoring, without the requirement of court orders.[95] Human rights groups claim that the deployment of the SORM and SORM-2 systems and the required registration of all telecommunications businesses and Web sites shows that the Russian Federation is still something of a police state.[96]

Old habits, techniques, methods, and systems die hard. As technologies diffuse to countries with different political, social, cultural, and historical experiences, these technologies are given what Jon Guice calls "new ideas, intentions, purposes, and contexts of use in different times and places, for different people and groups."[97] This is what happened with the Internet in Russia. Monopolistic and oligopolistic state-owned national and local telephone companies control the gateways to the Internet. In order to serve their customers, private ISPs have no choice but to purchase local exchange services from government-owned telephone companies, some of which are ISPs themselves.

Regulation of Electronic Commerce in the Russian Federation

Russia's economic and political history in the 1990s is the story of attempts at carrying out a transformation of the centralized communist command economy of the former Soviet Union into a market economy. The country went through a rather difficult market reform period marked by high inflation, corruption, and the virtual collapse of the banking system. The transformation of the economy from a highly centralized state-run command economy to a market based-economy proved to be difficult. The period was marked by a "Wild East" [98] situation where there existed a mentality of political corruption,[99] money laundering,[100] capital flight,[101] and misappropriation of communist-

[93] See *supra* note 113 at 337.

[94] See Anton A. Ivanov, *SORM Problem: Latest News*, (Russian) available at http://balfort.com/showarchive.php?id=1 (last visited June 10, 2004) (Reporting that though the Russian Supreme Court voided one minor provision of the law requiring communications companies to install, at their expense, equipment that allows the FSB to monitor and intercept Internet communications, the change the court ordered was only cosmetic. The SORM system remains in place).

[95] See Anne Nivat, *BSK, The Provider that Says, NIET*, THE UNESCO COURIER, March 2001; see also Xeni Jardin, *Will Russia's New Leader Launch Soviet-Style Regulation of the Net?*, *available at* http://www.xeni.net/docs/will_putin_regulation.htm (last visited Nov. 11, 2003).

[96] See Ivanov, supra note 92.

[97] See Jon Guice, *Looking Backward and Forward at the Internet*, 14 INFORMATION SOCIETY 201, 207 (1998)

[98] *See* Conal Walsh, *Russian Oligarchs put Screws on BP*, GUARDIAN UNLIMITED, May 9, 2004, available at http://observer-guardian.uk/business/story/06903.1212276/.00.htm (reporting that investors fear that Russia is returning to its "Wild East" where billion dollar investments vanish or evaporate).

[99] *See* Robert Orttung, *Business and Politics in the Russian Regions*, 51 PROBLEMS OF POST COMMUNISM 48 (2004) (suggesting that the oligarchs helped Yeltsin win the 1996 presidential election in exchange for huge properties from the state at minimal prices).

[100] *See Russia's Dirty Linen*, WALL STREET JOURNAL, August 30, 1999, at A26 (editorial commenting on Russian oligarchs who transferred money to various overseas destinations, including Credit Suisse-First

era public enterprises by politically well-connected and fabulously wealthy "oligarchs."[102] Among other economic abnormalities, commercial banks sprouted overnight, made billions of dollars, and disappeared just as quickly.[103] The result was a generalized lack of trust in the banking system and other sectors of the economy.[104] American-style self-regulation was not an option in this economic climate. George Soros, a wealthy global financier, calls this highly unstable period of Russian history the period of "robber capitalism."[105]

The Russian government still controls substantial parts of the economy, whereby several sectors of the oil and telecommunications industries are still monopolies. Notable other parts of the economy were privatized to well-connected, *nouveaux riches*, so-called oligarchs. The result is that for most of the 1990s, Russia had what Clifford Gaddy and Barry Ickles call a "virtual economy" far removed from a real market economy.[106] The Russian economy is largely a transitional one that is still in a state of flux. Additionally, the changing economy and diffusion of new information and communication technologies have created a digital chasm between the rural and urban sectors of the Russian population.[107]

The development of e-commerce under these conditions has been difficult and slow. Indeed, such commerce in Russia is radically different from the business model of the same name elsewhere. It is beset by numerous hurdles including the weak purchasing power of Russian consumers, the very low use of credit cards, a high level of credit card

---

Boston as part of money-laundering schemes); *see also* John Tagliabue, *Swiss Freeze 29 Bank Accounts for Russian Corruption Probe*, NEW YORK TIMES, September 4, 1999 at 1.

[101] *See Swiss Take New Look at Transfers of I.M.F. Aid for Russia*, NEW YORK TIMES, July 26, 2000 at C3 (reporting investigation by Swiss authorities of alleged misappropriation and laundering of Russian aid money through Swiss and American Banks).

[102] *See* Saeed Shah and Fred Weir, *The Russian Oligarchs are coming…but how did they make their money?* THE INDEPENDENT, July 9, 2003, *available at* <http::://www.rusnet.nl/news/2003/07/09reports/.shtml > (last modified September 2003) (reporting that the Russian oligarchs made their fortunes in the 1990s through highly controversial privatization deals in which the government sold immensely valuable assets at give-away prices to well-connected businessmen).

[103] *See generally*, ROBERT LEGVOLD, THE OLIGARCHS (2002) (recounts stories of four of the Russian "oligarchs" who created fabulous business empires worth billions of dollars out of the ruins of the Soviet economy through massive corruption and political power plays).

[104] *See* William Maley, *The Shape of the Russian Macroeconomy in* RUSSIA IN SEARCH OF ITS FUTURE (Amin Saikal and William Maley eds., 1995) 48, 53.

[105] *See* GEORGE SOROS, OPEN SOCIETY 235-264 (2000) (describing the chaotic "robber capitalism" that marked the transition from a communist command economy to a market economy).

[106] *See* Clifford G. Gaddy and Barry Ickles, *Russia's Virtual Economy*, 77 FOREIGN AFFAIRS 53 (1998) (noting that Russia's economy was based on illusions about all economic indicators ranging from taxes to prices).

[107] *See* Sergei Stafeev and Sue Webb, *Community Informatics in Russia: Needing to Make A Leap, in* CLOSING THE DIGITAL DIVIDE 63-73 (Stewart Marshall, Wallace Taylor, and Xinghuo Yu eds., 2003) (suggesting that information and communication technology is not a part of the everyday life of Russians due to economic, political and cultural factors).

fraud,[108] a poor mail and package delivery system, and above all, a lack of trust in the financial sector of the economy, especially the banks.[109]

Nevertheless Russia, like most industrialized countries, has created a regulatory framework for e-commerce. In 1993, the Russian Parliament amended the Russian Constitution to include provisions on individual privacy, namely the protection of personal data stored in computer databases in the country.[110] In 1994, the Russian Civil Code recognized business transactions involving electronic documents.[111] The next year, the Duma (Russia's parliament) passed a wide-ranging federal law on "Information, Informatization, and Protection of Information" (Information Law) that strengthened the personal privacy protections rights accorded individual Russians, vis-à-vis data collectors, analyzers and users.[112] Furthermore, non-governmental organizations and private persons involved in marketing or statistical research and data transfer are subject to compulsory licensing.[113] The law further stipulates that all Internet activity originating in Russia must be in the Russian language. The Cyrillic alphabet therefore sets the .ru domain apart from other national domains.

Comparative Analysis of Electronic Signature Regulation in the U.S. and Russian Federation within the framework of the UNCITRAL principles

American and Russian approaches to speech and communication in general and to the Internet in particular are strikingly different. These differences stem from the historical, socio-political and cultural realities of both countries. In the following section we compare and contrast the e-signature laws of both countries. The units of comparison are the UNCITRAL principles of global e-commerce set forth in the model law on e-signatures, which both countries participated in drafting and sending to the U.N. General Assembly for adoption. The aim of the comparison was to make a determination on whether each country's legislation is based in whole or in part on the UNCITRAL principles.

The U.S., Russia and UNCITRAL's E-Signature Principles

The UNCITRAL Model Law on Electronic Signatures is premised on a number of principles that are viewed as crucial for fluid, global e-commerce. This section will analyze the presence, or the absence, of the three most important principles: technological

---

[108] *See* Oksana Prokopenko, *Credit Card Fraud*, THE SOLITAIRE GAZETA, February 4, 2003 at 13 (LEXIS, Nexis Library) (reporting that credit card fraud is steadily increasing in Russia. Banks conceal crimes involving large sums. Electronic signatures using cryptography have been successful in reducing fraud).
[109] *See* INNA NAZAROVA AND IRINA LAKAEVA, OVERVIEW OF ELECTRONIC COMMERCE IN RUSSIA *at* http://www.bisnis.doc.gov/bisnis/country/001108e-commerce.htm (last visited October 11, 2003).
[110] *See* KONST. RF (1993) (as amended), Ross. Gazeta, No. 197, 25 December , 1993; No. 7 13 January, 1996; No. 31, 15 February, 1996; No. 111, 14 June, 2001.
[111] *See* Sobr. Zakonod. RF, 1994, No. 52 FZ; No. 32 (amended 2003); codified as Grazhdanskii Kodeks RF, arts 160, 434 (contracts can be completed through the exchange of electronic documents).
[112] Grazhdanskii Kodeks RF, art. 11 (1), Sobr. Zakonod. RF, 1995, No. 24 FZ; Ross. Gazeta, No. 39 22 February, 1995 (as amended by Ross. Gazeta No. 5, 15 January, 2003).
[113] *Id*, Grazhdanskii Kodeks RF, art. 11 (4).

neutrality, non-discrimination between domestic and foreign e-signatures and authentication certificates, and internationalist outlook..

a. Technology and media neutrality: This means that the law is not tied to, or does not require that esignatures be encoded in, a specific technology. This principle is contained in Article 3 of the Model Law, which states that no technology or method of creating or gaining access to e-signatures should be discounted.[114] The principle of technology neutrality is built into UNCITRAL Model Law's very definition of "electronic signatures." It states in part, "[e]lectronic signature means data in electronic form, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."[115] This definition leaves the door open to all types of reliable electronic technologies, now known or to be invented later, that can be used in the creation of e-signatures.

The U.S., technology and media neutrality

American law presents a conceptualization of e-signatures that mirrors the UNCITRAL definition. The E-Sign Act defines e-signatures as: "An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[116] This technology and medium-neutral stance is in keeping with the American statutory tradition of using broad, all-encompassing definitions to cover existing and future technologies.[117] Furthermore, the law states that in case alternative procedures or requirements for the use and or acceptance of e-signatures are needed, these alternatives "do not require or accord greater legal status or effect to a specific technology or technical specification for creating, storing, generating, receiving, communicating or authenticating electronic records or e-signatures."[118] The law thus creates a level playing field for all American technologies used in computer and database security.

The Russian Federation, technology and media neutrality

The Russian Federation conceptualizes the role and functions of e-signatures in e-commerce differently from the U.S. Russian law first recognized digital e-signatures as having legal effect in 1994.[119] In 2002, the Federal Law on Digital Electronic Signatures

[114] See Art 3, Model Law on Electronic Signatures G.A. Res. 56/80, UN GAOR 85th Session, Supp. No. 17, annex, UNCITRAL, GUIDE TO ENACTMENT: MODEL LAW ON ELECTRONIC SIGNATURES, para 27, U.N. Doc. A/RES/56/80 (2001).

[115] See Art 2, Model Law on Electronic Signatures G.A. Res. 56/80, UN GAOR 85th Session, Supp. No. 17, annex, UNCITRAL, GUIDE TO ENACTMENT: MODEL LAW ON ELECTRONIC SIGNATURES, para 27, U.N. Doc. A/RES/56/80 (2001) (hereinafter UNCITRAL GUIDE).

[116] E-SIGN Act, 15 U.S. C. § 7006 (5) (2000).

[117] *See e.g.*, Copyright Act, 17 U.S.C § 101 et. seq. (1976) (media and technology-neutral definition used in the Copyright Act).

[118] E-SIGN Act, 15 U.S. C. § 7006 (5)(2)(A)(ii) (2000).

[119] See Law No. 52-FZ of November 30, 1994, Part 1, Civil Code of the Russian Federation, Sobr. Zakonod. RF, 1994, No. 32 (amended 2003).

was enacted to address issues of Internet, computer and database security.[120] This law is tied to a specific digital technology, namely, the GOST[121] Public-Key Digital Signature Algorithm.[122] The law defines e-signatures as: "A sequence of symbols that results from cryptographic transformation of basic information with the use of a secret [private] key that allows the holder of the [open] public key to establish the integrity of the information as well as the signatory or holder of the private key."[123] Thus, by definition, Russia recognizes a specific digital technology, which is to say its own version of the so-called public-key infrastructure or "key recovery" cryptographic system. The law, which also instituted state-licensed, digital signature certification centers, injects the government directly into the stream of Internet commerce for purposes of surveillance and control.

The law sanctions the use of e-signatures as the functional equivalent of physical, handwritten signatures in electronic communication.[124] Under the law, biometric technologies such as eye-scans, the electronic analogs of handwritten signatures and the digital depiction of signatures are expressly excluded.[125] In addition, the law contains a verification provision.[126] Under these provisions, government verification centers are given the responsibility of verifying, confirming and notarizing the ownership of digital e-signatures by physical or legal persons (companies) and issuing certificates of verification of such digital e-signatures. The verification centers are persons or special Russian government departments that have the authority to confirm the signatures' authenticity and issue certificates of verification, as well as to suspend or annul digital e-signature encryption codes.

Non-discrimination between domestic and foreign electronic certificates and signatures

The UNCITRAL Model Law on Electronic Signatures stipulates that the geographical location where an e-signature is created or a certificate is issued should not be one of the factors considered when determining whether it is legally effective or valid.[127] Furthermore, the model law recommends that states enact e-signature laws that clearly stipulate that such signatures created or used outside each country shall have the same legal effect as signatures created or used within the state, if it offers substantial

[120] See Law No 1-FZ on Digital Electronic Signatures, Ross. Gazeta, January 6, 2002.
[121] *See RSA Security Inc, RSA Keon Certificate Authority Awarded Highest Common Criteria Certification Commercial Certificate Management Systems*, PR NEWSWIRE, January 27, 2003, LEXIS, News Library, Press Release (GOST is a centralized, government-controlled Public-Key management infrastructure based on encryption).
[122] *See generally*, Gregory Pressman, *The Electronic Age is Almost Upon Us*, 229 NEW YORK LAW JOURNAL S1 (2003) (describing the creation and operation of the public and private key cryptographic systems. Private keys are generated by special mathematical algorithms and enclose a numeric signature. The public-key is a separate string of numbers that allow a holder to unlock and validate the digital signature created by the related private key).
[123] *Id.* Art. 2.
[124] *Id.* Art 1. (1).
[125] *Id.* Art 1 (3).
[126] Article 8, Law No. 1 FZ On Digital Electronic Signatures, Ross. Gazeta, Jan. 6, 2002.
[127] *See* Art. 12(1)(a-b), UNCITRAL Model Law on Electronic Signatures with Guide to Enactment A/56/80 ¶ 159 (2001).

reliability.[128] Additionally, the model law makes provisions for bilateral and multilateral agreements between countries.[129]

United States and non-discrimination between domestic and foreign electronic certificates and signatures

As the leader and major beneficiary of the globalization of e-commerce and the popularization of e-signatures, the U.S., beginning with the Clinton/Gore administration, has called on countries to enact a hands-off policy towards the Internet. One feature of this policy is non-discrimination between technologies from different nations. Though the Clinton/Gore administration advocated the global adoption of key recovery encryption in its Framework for Internet Regulation,[130] that position changed with time and evolving technology. The E-SIGN Act stipulates that the U.S. would "[t]ake a nondiscriminatory approach to e-signatures and authentication methods from other jurisdictions."[131] However, the law is silent on the issue of American embargoes of encryption technology exports to Russia, China, and the "rogue" states of the world. As things stand, American companies are the major beneficiaries of global recognition of electronic certificates and signatures. It is difficult to imagine a major American bank or even the Federal Reserve Board according the same legal effect to e-signatures created in say, Burkina Faso or Burma as one created by an American securities firm.

ii. Russia and non-discrimination between domestic and foreign electronic certificates and signatures

The Russian Federation does not subscribe to the nondiscriminatory principle advanced by UNCITRAL and enacted into law in the U.S. Russia's Law on Digital Electronic Signatures stipulates that foreign public-key infrastructure certificates are accepted in Russia only under the so-called "cross-certification principle." That is, countries that want Russian certification authorities to recognize their public key certificates must sign a bilateral or multilateral agreement to that effect with the Russian Federation and agree to provide data and communications security comparable to that provided by the Russian Public Key Infrastructure.[132]

Furthermore, as part of the nationalistic posture of the Russian Federation, a 1995 presidential decree banned the use of encryption algorithms or devices that were not certified by the country's national security body, the Agency for Government Communications and Information.[133] The importation or exportation of encryption

[128] *Id.* Art. 12 (3).
[129] *Id.* Art.5 (Countries which adopt the model law as is, can modify it in the framework of bilateral and multilateral agreements).
[130] *See* WILLIAM J. CLINTON AND ALBERT GORE, JR., A FRAMEWORK FOR ELECTRONIC COMMERCE 5 (1997) (this *laissez-faire* approach would be global, merchantilist, decentralized, contractual, competitive, transparent and protective of intellectual property).
[131] 15 U.S.C. § 7031 (a)(D) (2000).
[132] Article 19, Law No. 1-FZ of January 10, 2002 on Digital Electronic Signatures, Rossiyskaya Gazeta No.6. of Jan. 12, 2002.
[133] *See supra* note 113 at 334, 338.

hardware and software without a license is against Russian law.[134] Since public-key infrastructure is not the norm in all jurisdictions, the Russian law is clearly discriminatory. It sets the country apart from the U.S. and many other nations, and goes against the grain of UNCITRAL's attempts to create a fluid, global e-commerce system.

Internationalist Outlook

UNCITRAL is an instrument in the globalization of trade. One of its mandates is to create international standards that would facilitate the smooth exchange of goods and services across all jurisdictions through technological and regulatory harmonization and unification. Essentially, countries are encouraged to adopt e-signature policies and technologies that may be different from each other but meet certain recognized, open, international, market-driven commercial standards. This "recognized international standards" principle covers international technical and commercial standards and norms adopted by governmental and intergovernmental organizations in the form of requirements, recommendations, guidelines, codes of conduct, or statements of best practices or norms.[135] It goes without saying that these international standards are capitalist, free-market standards that have a striking resemblance to the values of America's Constitutional Commerce Clause, which puts a premium on nondiscrimination in interstate commerce.

The U.S. as an internationalist e-commerce power

The U.S. has been at the forefront of efforts to use the Internet as an open platform for global e-commerce. The Clinton/Gore framework for global e-commerce and the E-Sign Act are premised on a free and open international e-commerce regime. The Act gives the Secretary of Commerce the task of promoting the "acceptance and use, on an international basis, of electronic signatures" in order to facilitate the development of interstate and foreign commerce.[136] The act adopts principles from UNCITRAL's Model Law on Electronic Commerce that deal with the removal of paper-based obstacles to e-commerce such as physical signatures and notarization.[137]

However, from a global perspective, America's *laissez faire* e-commerce posture has a national security exception.[138] Despite the fact that the U.S. has eased restrictions

[134] *See* Wayne Madsen et al., *Cryptography and Liberty: An International Survey of Encryption Policy*, 16 J.MARSHALL J.COMPUTER & INFO.L., 475, 511 (1998).
[135] *See* Art. 12 (4-5), UNCITRAL Model Law on Electronic Signatures with Guide to Enactment A/56/80 ¶ 159 (2001). *See also* A/CN.98/483, ¶¶. 49, 101-104.(2000). (UNCITRAL's definition of "recognized international standards" includes voluntary standards as well as statements of accepted public and private sector technical, legal or commercial practices generally accepted as applicable internationally).
[136] *See* 15 U.S.C. § 7031(a)(1-2).
[137] *See* 15 U.S.C. § 7031(a)(2)(A).
[138] *See* F. Lynn McNulty, *Encryption's Importance to Economic and Infrastructural Security*, 9 DUKE J. COMP. & INT'L L. 427 (1999); *see also* Christopher F. Corr, *The Wall Still Stands! Complying with Export Controls on Technology Transfers in the Post-Cold War, Post 9/11 Era*, 25 HOUS. J.INT'L L. 441, 448-489 (2003)(suggesting that even though export controls have been eased, exporters of encryption

on the export or re-export of strong encryption technology that can be used in e-commerce and other activities,[139] the Russian Federation, China and other countries still face major restrictions on importing and re-exporting American strong encryption technology for national security reasons. Indeed, export or re-export from the U.S. of virtually all strong encryption technology that performs an "information security function," (read defense, espionage, and munitions-related activities) still has to be licensed or specifically approved by the Department of Commerce[140] and the Department of the Treasury.[141] Making such technology available to the foreign workforce of American companies is also subject to governmental approval. This has led to differences of opinion between the computer industry and the U.S. government over restrictions on the export of encryption technology[142] that drives the instrumentalities of e-commerce and e-signatures. The industry is especially unhappy about restrictions that have removed American strong data-encryption technologies beyond 56-bit encryption from the open international market.[143] This may explain why the Russians, perhaps for reasons of security and access, opted for their own homegrown encryption technology.

Restrictions on the export or re-export of American encryption technologies that facilitate e-commerce also demonstrate that in global e-commerce, U.S. national security interests take precedence over those of other players in international electronic trade. Ironically, the UNCITRAL model laws are silent on the subject of restriction of the export and re-export of strong or other encryption technologies.

Russia and the Internationalist Outlook principle

Russia's law on Digital Electronic Signatures is less international in outlook than the American market-based E-Sign law. While the letter of the Russian law recognizes e-signature technology and certificates resulting from bilateral agreements signed between Russia and other countries, the law is not international in scope. It is limited to the

technology are still subject to strict control. The Russian Federation was not on the list of European countries to which encryption technologies could be exported or re-exported without a license).

[139] Revisions to Restrictions on Encryption Technology, 65 Fed.Reg.62600, 62,600-02 (Oct. 19, 2000); *see also* David Sanger, *U.S. Relaxes the Limits on Exports of High-Speed Computers*, NEW YORK TIMES, July 2, 1999 at A4 (reporting that President Bill Clinton had eased some restrictions on super computer exports to Russia and China).

[140] See Department of Commerce, Export Administration Regulations: Encryption Clarifications and Revisions, 15 C.F.R. Parts 734,740, 742, 748, 770 and 774 (2003) (the Bureau of Industry and Security of the Department of Commerce regulates the export and re-export of encryption and other "dual use" products, that is software, computer code and other technical information that appears on Commerce Control List). *See also* International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq.

[141] The Trading with the Enemy Act, 50 U.S.C.App. 5; and the International Emergency Economic Powers Act, 50 U.S.C § 1701 et seq. (giving Treasury Department's Office of Foreign Assets Control authority to control financial and commercial transactions involving specific foreign countries).

[142] *See* Craig Matsumoto, *Crypto confab to debate U.S. move on exports*, ELECTRICAL ENGINEERING TIMES, Jan. 18, 1999 at 4 (reporting that data security experts were frustrated at the Clinton Administration restrictions despite easing of some 56-bit encryption rules); *see also* John Simons, *U.S. to relax restrictions on Encryption Technology*, WALL STREET JOURNAL, Sept. 16, 1999 at B6.

[143] *See* Neil Munro, *The Unhappy but Beneficial Coexistence of the FBI and the Tech Elite*, 44 COMMUNICATIONS OF THE ACM 15 (2001) (reporting on the relationship between governmental security agencies which want to restrict encryption and other high technology exports).

Russian GOST public-key infrastructure, which cannot be exported without a license. Russian law is therefore primarily aimed at controlling e-commerce and financial transactions within the borders of the Russian Federation, and not at facilitating global e-commerce.

Findings & Discussion.

This article compares the e-signature laws of the U.S. and Russia. As unique, "invisible" components of communication systems, e-signatures support and protect the "visible" communication systems that support organizational and mass communication, telecommunications and interpersonal communication. The study was carried out within the framework of the UNCITRAL Model Law on Electronic Signatures. The table below is a comparative summary of the UNCITRAL principles and their incorporation in American and Russian e-signature law. The study found that as members of UNCITRAL, the U.S. and the Russian Federation were closely involved in the drafting of the Model Laws on Electronic Commerce and Electronic Signatures. However, there are significant differences between the e-signature laws of the two countries due to their vastly different historical, political, economic, cultural, and technological contexts.

UNCITRAL Model Law Principles As Applied in American and Russian E-Signature Laws		
UNCITRAL Principles	**American Law**	**Russian Law**
Definition of electronic signatures	Broad	Narrow & technology specific
Technology/media-neutrality	Yes	No
Sphere of application	Mercantilist	Mixed
Party autonomy/freedom of contract	Yes	Yes
Non-discrimination against foreign signatures/certificates	Yes	No
Incorporation & incorporation by reference	Yes	No
Internationality	Yes	No
Self-regulation	Yes	No

American law incorporates the principles of the UNCITRAL model law by reference in its E–Sign law because the principles are completely consonant with the American Constitution.[144] Indeed, American law explicitly mentions UNCITRAL and gives the Secretary of Commerce the responsibility of actively promoting the model law around the world. The total acceptance of a U.N. model law would be highly unusual

[144] Electronic Signatures in Global and National Commerce Act, 15 U.S.C § 7031(a)(2)(A)(2000) (the Secretary of Commerce is asked to adopt principles from the UNCITRAL Model Law on Electronic Commerce to remove paper-based obstacles to electronic transactions). *See also* 6 WEST'S ENCYCLOPEDIA OF AMERICAN LAW 128 (1998) (incorporation by reference is the practice of making one document a part of another separate document by alluding to the first document in the second).

were it not for the fact that it has a clear American imprint. Thus, in matters of e-commerce and e-signatures, it can be said that the U.N. and UNCITRAL play only, to borrow David Nelken's expression, "mediating institutional roles"[145] between the U.S. and the rest of the world. The U.N. is simply a proxy for the globalization of America's capitalist free-market Internet regulatory system. The cooperative posture of the U.S. on matters of e-commerce, where its values are generally predominant, stands in stark contrast with its unilateralism in matters involving international human rights and global warming. Additionally, American law incorporates virtually all the internationalist principles advocated by the UNCITRAL model. Russian law neither mentions UNCITRAL nor incorporates its principles in any form.

The most significant difference between the two countries is their choice of e-signature technologies. American e-signature law is not tied to any specific technology while Russian law is tied to a specific homegrown technology that allows governmental access to, and surveillance of, data in the stream of e-commerce. By tying e-signatures to a specific "key recovery" infrastructure, the law essentially gives Russian intelligence and law enforcement agencies access to the plaintext of encrypted data without the knowledge and consent of the sender and receiver of the message. The provision of the law regarding governmental verification centers injects the state directly into the stream of e-commerce. By providing technical specifications for e-signatures, the Russian government is clearly providing technical solutions to what it perceives to be problems of security on the Internet. It is also making rules that have an impact on its country domain and on the Internet as a whole. Setting the technical and software standards and specifications for digital computer code is one of the most effective methods of regulating the Internet.[146]

An *ad hoc* group of American cryptographers and computer scientists, known as the Abelson Group, states that key-recovery encryption really means "any system for assuring third party (read governmental) access to encrypted data."[147] Thus, key-recovery cryptographic systems like the one specifically mentioned in Russian law virtually guarantee government access to encrypted e-signature and e-commerce data. As early as 1997, the Abelson Group stated that while encryption made information secure from prying eyes, eavesdropping, interception and outright theft, it also made it impossible for law enforcement and intelligence agencies to carry out surreptitious

---

[145] *See* David Nelken, *Comparatists and Transferability*, *in* COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 437, 454 (Pierre Legrand & Roderick Munday eds. 2003) (suggesting that the "mediating role of institutions" be taken into consideration in evaluating the success of legal transfers between countries).

[146] *See* Rajiv Shah and Jay Kesan, *Manipulating the Governance Characteristics of Code*, 5 EMERALD 3-9 (2003) (suggesting that regulation through computer code rather than statute is growing in importance in the field of information technology).

[147] *See* Hal Abelson et al., The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption, *available at* http://www.cdt.org/crypto/risks98/ (last visited Aug. 17, 2005)(according to Abelson and his colleagues, the key recovery system is an encryption procedure based on the use of complex mathematical logarithms to scramble data so as to make it virtually impossible for anyone other than the authorized recipients to unscramble or decode the original "plaintext" of the message. This allows sensitive and or proprietary information to be stored on insecure computers or transmitted across insecure networks and only parties with the right decryption "keys" can recover the plaintext of the data or information).

electronic eavesdropping, wiretapping and surveillance against suspected criminals, organized crime, industrial spies, terrorists and rogue states.[148] Law enforcement and intelligence agencies then started to require the deployment of key-recovery systems designed to facilitate surreptitious third party (governmental) access to encrypted data and communication without the knowledge of the key owners.[149] The Abelson Group thinks that a centralized government-controlled key-recovery infrastructure like the one in Russia is incompatible with democratic governance: "The very notion of a pervasive government key-recovery infrastructure runs counter to the basic principles of freedom and privacy in a democracy and that alone is enough reason to avoid deploying such systems."[150]

However, the niceties of democracy, good governance, and open global trade do not carry the same weight in Russia that they do in the U.S. Russia's choice of a homegrown key-recovery infrastructure is therefore neither fortuitous nor accidental. The technology is designed to give Russian intelligence and law enforcement agencies access to the plaintext of encrypted data. This is the case because under the e-signatures law, the government is the binding root certification or certificate authority, which authenticates or "vouches for" the existence or integrity of one or both parties in a transaction involving e-signatures.[151] Russia's decision to opt for a technology-specific law goes against the grain of U.N. efforts to harmonize and unify e-commerce law at the global level. Additionally, by opting for a public key-cryptography-based digital e-signature regime, Russia parted company with the European Union and the U.S., who define e-signatures in rather generic terms and do not tie them to a specific technology.

The explanation for this is that Russia has always had a culture of centralized governmental information and telecommunications control for purposes of surveillance. Russia's governmental information control reflex is a tradition that Rafal Rohozinski calls the "communication/control pathology."[152] According to Rohozinski, the Internet has not changed Russia; Russia has changed the Internet. The country has succeeded in molding the Internet (at least that part of it within its jurisdiction) into its image. Russia is said to have colonized Internet technology and made it perform some of the social and political activities that used to be performed in the pre-Internet Soviet era.[153]

Russia's regulation of e-signatures shows a limitation of international policy transfer. Since legal or regulatory reform in the international system is often achieved through hegemony and or unequal power relations between nations,[154] the U.S. has been able to influence the U. N. and much of the international community towards adopt its free-market e-commerce policies. At the height of the so-called "dot com bubble," the U.N. and the U.S. hoped to do what David Nelken asserts is typical in cases of transnational legal transfers: use e-signature law to help Russia "jump-start the wider

[148] *Id.*
[149] *Id.*
[150] *Id.* at 11.
[151] *Id.* at 88.
[152] *See supra* note 84 at 334, 335.
[153] *Id.* at 337.
[154] *See* Allen Buchanan & David Golove, *Philosophy of International Law, in* THE OXFORD HANDBOOK OF JURISPRUDENCE AND PHILOSOPHY OF LAW 868, 886 (Jules Coleman & Scott Shapiro eds.2002).

process of social [and economic] change and leap-frog standing cultural and social obstacles [to free-market capitalism and e-commerce]."[155] The Russian Federation did not see it that way. It did not incorporate the UNCITRAL model law into its national legislation because the model law does not sit well with its political, socio-economic, and cultural realities. Russian law essentially fragments the encryption and e-commerce market, contrary to the wishes of the U.S. and the U.N.[156]

[155] *Id* at 455.

[156] For an example of American government displeasure at China's insistance on standardizing its own encryption technology, *see* Steve Lohr, *U.S. Pressing China to Yield on Wireless Technology*, NEW YORK TIMES, Mar. 4, 2004 at C7.

CONCLUSION

The general picture that emerges from this comparative study is that both the U.S. and the Russian Federation regulate e-signatures in their national interests. Both have import and export restrictions on encryption technology that is crucial in e-commerce. However, the U.S. has a broad international vision consistent with its laws, traditions, commercial culture and national interests. Though UNCITRAL model laws are ostensibly aimed at promoting the welfare of all the peoples of the world, especially those in the developing countries,[157] the harmonization, standardization and globalization of the regulation of e-commerce, as advanced by UNCITRAL and promoted actively by the American government, globalizes America's neo-mercantilist, *laissez faire*, free-trade regime.

Indeed, the UNCITRAL Model Law on Electronic Signatures, like the UNCITRAL Model Law on Electronic Commerce before it, is essentially an instrument for the global diffusion of the American, and to a lesser extent, Western European free-market economic ideology.[158] In contrast, the Russian Federation's attitude towards e-signatures is illustrated by its desire to control as much of the information and communication technology within its jurisdiction as possible.

The main contention of this article is that the U.S. and Russia have a significant divergence of ideology over the specificities of e-signature regulation because the UNCITRAL model law involves the transplantation of policies that are tailor-made for the economic, political, and social realities of the U.S. rather than those of Russia. Transfer of policy from UNCITRAL to the Russian Federation did not take place because any such transfer would amount to exportation of a culture-specific ideology.[159]

Finally, this study shows that the UNCITRAL Model Law on Electronic Signatures was perhaps overly optimistic about harmonization and unification of international e-commerce law. In hindsight, the U.N. and the "international community" may have been caught up in the euphoria over the Internet during period of the dot com bubble. The promises and benefits of harmonization were clearly overstated, given the still active rivalry between the U.S. and the Russian Federation over encryption technology.[160] The comparison of American and Russian Federation legislation of e-signatures shows that model laws are indeed what states make or fail to make of them.

---

[157] G.A. Res.2205 (XXI) UN GAOR 21ST Session, U.N.Doc A/RES/2205(XXI) (1966).

[158] *See* ROBERT BURNETT & P. DAVID MARSHALL, WEB THEORY 43 (Routledge 2003)(suggesting that the Internet facilitates the flow of information for purposes of promoting globalization).

[159] *See* David Nelken, *Comparatists and Transferability*, *in* COMPARATIVE LEGAL STUDIES: TRADITIONS AND TRANSITIONS 437, 458 (Pierre Legrand & Roderick Munday eds. 2003 (suggesting that the "mediating role of institutions" be taken into consideration in legal transfers between countries).

[160] *See* Lee Artz, *Globalization, Media Hegemony and Social Class, in* GLOBALIZATION OF CORPORATE MEDIA HEGEMONY 3 (Lee Artz & Yahya Kamalimpour eds., 2003) (suggesting that globalization and economic "reforms" have led to inequalities around the globe).