Fall 2000

The Establishment of a U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and its Impact on U.S.-China Relations: Marco Polo Where are You?

Omar Saleem
Florida A&M University College of Law, omar.saleem@famu.edu

THE ESTABLISHMENT OF A U.S. FEDERAL DATA PROTECTION AGENCY TO DEFINE AND REGULATE INTERNET PRIVACY AND ITS IMPACT ON U.S.-CHINA RELATIONS: MARCO POLO WHERE ARE YOU?

by OMAR SALEEM†

I. INTRODUCTION

The explorer Marco Polo traveled from Italy to exotic parts of Asia and the Middle East in the thirteenth century.[1] During his travels, he maintained a travelogue in which he expressed his perceptions of the peoples and places he visited. He chronicled his exploits in Asia in general, and China in particular. In his travelogue, Marco Polo described Kublai Kahn's palace and the wonders of China. Perhaps his greatest contribution was the link he created between east and west, two worlds profoundly unfamiliar with each other at the time.[2] His travelogue precipitated other European explorations and established a foundation for a global economic network sustained through commerce.

Marco Polo's desire to explore new worlds and exchange both ideas and goods should be the impetus behind the Internet. The Internet is the global economic network of the new millennium. It is a virtual silk road connecting east and west, and a mechanism to generate wealth for both. The Chinese government, for example, has indicated that the In-

† Professor of Law, St Thomas University School of Law, Miami, Florida. This article is based on remarks prepared for the Symposium, *Federal Data Protection Agency: Regulating Internet Privacy*, September 22, 2000 at the John Marshall Law School.

1. *Venetian Adventurer: The Life and Times of Marco Polo 157* (Ronald Letham, Stanford University 1982). For an excellent depiction of Marco Polo's travels through a collection of photographs and accompanying text, see Alain Cheneviere, *Travels in the Orient in Marco Polo's Footsteps* (1997).

2. Jonathan D. Spence, *The Chan's Great Continent* 3 (1998) (stating that Marco Polo described China as "a benevolently ruled dictatorship, colossal in scale, decorous in customs, rich in trade, highly urbanized, inventive in commercial dealings, weak in war.").

ternet is a vital and intricate part of its goal of modernization.[3] Since 1978, China has advocated a national goal of modernization, and the country has taken numerous steps in that direction. China's drive towards modernization presents significant concerns for the U.S. as China seeks to regulate Internet privacy. The concerns center on the fact that China has millions of people on the Internet, and that number continues to increase exponentially. Will Western theories and rules of privacy apply to the global Internet? Will the U.S. compromise other interests to gain China's cooperation in the Western idea of Internet privacy regulation? With such a tremendous population and enormous economic potential, will China adopt privacy rules promulgated by a U.S. Federal Data Protection Agency and the European Union (EU)? Will China comply with western theories of privacy to govern the Internet or will it offer substantial resistance?[4]

This Article first discusses the factors that have caused both the reevaluation of Western notions of privacy, and consideration of the establishment of a Federal Data Protections Agency. Next, the article discusses the EU's approach to regulating Internet privacy. This section is followed by a discussion of why the U.S. and EU approaches to Internet privacy regulation must be implemented from a global, or Marco-Polo-like perspective, that includes the knowledge and experiences of other cultures, such as the Islamic world and China. The article then discusses how the premature establishment of a Federal Data Protection Agency to regulate Internet privacy may hamper U.S.-China relations. In conclusion, I articulate the particular concerns of regulating Internet privacy and demonstrate how the U.S.-China dispute about the Internet Corporation for Assigned Names and Numbers ("ICANN") will resurface around online privacy if the U.S. engages in unilateral development of online privacy rules.

---

3. *See generally* Asia Rumblings, *Doom & Gloom for China's Internets. . .Surprising?* <http://asia.internet.com/Rumblings/00/0211.html> (accessed Feb. 22, 2000) (indicating a dominate mood in China from the period of Deng Xiaoping and afterwards, has been that wealth is good and that the Internet is a means to wealth); Canada China Business Forum, *In Search of Growth, China Turns to High-Tech Venture Capital Funds* (Mar.-Apr. 2000) (noting that China has vigorously sought foreign investments to develop its high-tech markets); Blaise Zerega, *What Would Mao Think?* <http://www.redherring.com/mag/issue83/mag-china-83.html> (Nov. 18, 2000) (discussing the campaign in China to get its inhabitants online).

4. *See* Todd G. Hartman, *The Marketplace vs. Ideas: The First Amendment Challenges to Internet Commerce*, 12 Harv. J. L. & Tech. 419, 440 (1999) (predicting efforts to regulate the Internet will meet with considerable resistance). The concern is whether the international community will also resist regulation of the Internet. *Id.*

II. FACTORS PRECIPITATING THE CONSIDERATION OF A U.S. FEDERAL DATA PROTECTION AGENCY

It is undeniable that privacy is a right. Privacy in the U.S. is inextricably bound to personal freedom and general well being. [5] The when, where, and how of Internet privacy regulation have become difficult because technology has outpaced law.[6] Questions have arisen regarding how to define, regulate and enforce Internet privacy, and whether it is feasible to establish a U.S. Federal Data Protection Agency? The assumption that there is an urgent need to regulate Internet privacy and establish a Federal Data Protection Agency is the product of numerous factors.

One factor is the proliferation of insightful scholarship about the Internet. The pertinent scholarship has deconstructed prevailing views in the U.S. about Internet privacy regulation and other Internet-related concerns. Writers such as John Perry Barlow, in his *Declaration of Independence for Cyberspace*, have provocatively asserted that cyberspace has no sovereignty and should be free from government regulation.[7] Another probing question is whether existing privacy laws and organizations are sufficient to protect online privacy. David G. Post provided an insightful discussion on this point in his article, *Of Horses, Black Holes, and Decentralized Law-Making in Cyberspace*, in which he critiqued

5. The White House, *A Framework for Global Electronic Commerce* <http://www.ecommerce.gov/framewrk.htm> (accessed Feb. 22, 2000); *see e.g. Malloy v. Hogan*, 378 U.S. 1, 8 (1964) (noting that in the U.S. the right to privacy is a means to acknowledge a correlation between privacy, conscience, and the soul). U.S. Const. Amend. V. The Fifth Amendment to the U.S. Constitution specifies, "No person . . . shall be compelled in any criminal case to be a witness against himself." The *Malloy* Court indicated that this clause protects the right of a person to remain silent unless that person chooses to speak in the unfettered exercise of free will. *Malloy, 378 U.S. at 8. See also Schmerber v. California*, 384 U.S. 757, 759 (1966) (explaining that the admissibility of blood withdrawn from a person suspected of driving while intoxicated did not violate the Fifth Amendment protection against self-incrimination because the blood sample was neither testimonial nor communicative in nature). In other decisions, the Court held that neither voice demonstrations nor field sobriety tests were testimonial for purposes of the Fifth Amendment. See *United States v. Wade*, 388 U.S. 218, 261 (1967); *Pennsylvania v. Muniz*, 496 U.S. 592, 616 (1990); *United States v. Nobles*, 422 U.S. 225, 233 (1975) (stating that the Fifth Amendment protection against self-incrimination only applies to testimonial evidence because the privilege protects the "private inner sanctum of individual feeling and thought.").

6. Frederick Schauer, Symposium, *Internet Privacy and the Public-Private Distinction*, 38 Jurimetrics J. 555 (1998) (indicating that the law looks backwards, and therefore, has difficulty dealing with change). According to the author, the Internet and related technologies have altered privacy is several respects: quantatively, the Internet has made it easier to access numerous databases; qualitatively, the Internet has created new ways to invade privacy; and, conceptually, notions of privacy are dependent on technological capabilities. *Id.*

7. John Perry Barlow, *A Declaration of Independence for Cyberspace* 8 <http://www.webveranda.com/freedom/doi.html> (accessed Feb. 6, 2000).

Judge Frank Easterbrook's premise that existing theories of law are sufficient to address the factual and legal disputes that arise on the Internet.[8] Easterbrook presented the challenge—in his insightful analogy of the law of the horse—that there is really no such law as Internet law, and that existing laws are sufficient to resolve Internet-related disputes. There is also Lawrence Lessig's challenge from his seminal text, *Code and Other Laws of Cyberspace*, that societies should not rely upon an invisible hand to regulate the Internet, rather citizens should build a free and open society on the Internet because [l]eft to itself, cyberspace will become a perfect tool of control. [9] Furthermore, Michael Froomkin in his article, *It Came From Planet Clipper: The Battle Over Cryptographic Key Escrow,* discussed the necessity for secure communications via encryption and the international implications of such technology.[10] There are also the insights of Joel R. Reidenberg in his article, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, in which he noted that law and government are not the only sources of rule making and that ground rules for the Internet can also arise out of networks from a Lex Informatica. [11] These articles, and numerous others, have generated considerable discussion about the future direction of Internet regulation.

A second factor is the public fear that the relentless march of commerce [will] plow over privacy concerns. [12] In a Wall Street Journal-NBC poll, people were asked, In the new millennium, what threats do you fear most? [13] The response was not the usual, i.e., war, environmental degradation, inadequate social security, inadequate public school, illegal drugs, crime, or world hunger; instead, the response was loss of personal privacy.[14] Another poll conducted by Price Waterhouse re-

---

8. David G. Post, *Of Horses, Black Holes, and Decentralized Law-Making in Cyberspace* 3 <http://webserver.law.yale.edu/censor/post.htm> (accessed Oct. 16, 2000); *but see* generally Symposium, *Surveying Law and Borders: Law and Borders — The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367 (1996) (predicting the potential emergence of new rules to govern cyberspace).

9. Lawrence Lessig, *Code and Other Laws of Cyberspace* 5-6 (Basic Books 1999).

10. A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow,"* 15 U. Chi. L. Forum (1996) (reprinted in <http://www.law.miami.edu/~froomkin/ articles/planet_clipper.htm>.

11. Joel R. Reidenberg, *Informatica Lex: The Formation of Information Policy Rules Through Technology*, 76 Tex. L. Rev. 553, 554-55 (1998).

12. Theodore Y. Blumoff, *Introduction: 1999-2000 Oliver Wendell Holmes Symposium and Lectureship: The Marketplace of Ideas in Cyberspace*, 51 Mercer L. Rev. 817, 891 (2000).

13. *Id.* at 890. (providing the observations of offered by panelist Daniel Jaffe, Executive Vice President, Government Relations, of the Association of National Advertisers).

14. *Id.*; *see* Stanton McCandlish, *The Electronic Frontier Foundation, EFF's Top 12 Ways to Protect Online Privacy* <http://www.eff.org/pub/Privacy/eff_privacy_top_12.html> (accessed Oct. 16, 2000). Privacy concerns have precipitated self-help methods to protect

vealed that 86 percent of Americans were concerned about an invasion of their privacy on the Internet.[15] Additionally, a Georgetown University survey revealed that 92.8 [%] of . . . [Web] sites . . . [surveyed] collected at least one type of personal identifying information. [16] The commercial interests associated with the Internet realize that e-commerce will whither and die unless consumer fears about a lack of privacy are alleviated.[17] This has ushered forth a demand from commercial interests for self regulation of the Internet.[18] In response, some suggest that government regulation is preferable, perhaps through a newly established Federal Data Protection Agency.

A third factor is the sheer volume of subject matter on the Internet. The Internet is used for educational, commercial and entertainment purposes. Its users include individuals, organizations, institutions and businesses. The Federal Trade Commission (FTC) has been charged with the task of protecting consumers on the Internet under the Federal Trade Commission Act, which mandates that the FTC protect consumers from unfair methods of competition and deceptive acts or practices.[19] This has been a formidable task for the FTC because it has the additional task of enforcing 40 additional statutes and 30 separate rules.[20] For example,

---

privacy. Id. In an attempt to demonstrate how your privacy is affected by using the Internet, one site provides immediate information about your configuration and the URL previously visited. *See* e.g. CNIL, <http://www.cnil.fr/uk/traces/demonst/uk_config.htm> (accessed Oct. 16, 2000) (displaying an Internet user's remote host, remote ADDR, http User agent, http referer, DNS address, IP address, operating system, browser, last site visited).

15. Charles F. Luce, Jr., *Internet Privacy: SPAM and Cookies: How to Avoid Indigestion While Binging at the World Wide Automat*, 27 Colo. Law. 27 (1998).

16. Mary J. Culnan, *Georgetown Internet Privacy Policy Survey: A Report to the Federal Trade Commission* <http://www.msb.edu/faculty/culnanm/gippshome.html> (accessed Oct. 16, 2000).

17. Dennis C. Vacco, *Internet Privacy 1997: The Year in Review,* National Association of Attorneys General: Consumer Protection Committee (available in LEXIS, 1997-DEC NAAGCPR 1 (Dec. 1997)). *See* Culnan, *supra* n. 16, at 3 (stating online sales in the U.S. alone reached 7 billion in 1998 and commercial interests are concerned about consumer fears and the risk to e-business).

18. Nancy Lazar, *Consumer Online: Your Right to Privacy in Cyberspace*, 10 Loy. Consumer L. Rev. 117, 118 (1998). In response to possible government regulation of the Internet, several U.S. high-tech companies formed a coalition to facilitate e-commerce. *Id.* They formulated a position paper in which they stressed self regulation. *Id.* The companies included: Apple Computer, Compaq Computer, Data General, Hewlett-Packard, IBM, NCR, Silicon Graphics, Sun Microsystems, Stratus Computer, and Unisys. *Id.*; *see also* Oscar H. Gandy, Jr., *Legitimate Business Interest: No End in Sight? An Inquiry Into the Status of Privacy in Cyberspace*, 1996 U. Chi. Leg. Forum 77, 80 (1996) (noting the corporate sector's interests in enhancing business relations with their customers through information about consumers, citizens, and employees poses a threat to individual privacy).

19. John Graubert & Jill Coleman, *Consumer Protection and Antitrust Enforcement at the Speed of Light: The FTC Meets the Internet*, 25 Can.-U.S. L.J. 275, 276 (1999).

20. *Id.*

a grossly understaffed FTC has been bombarded with unprecedented mega-mergers, which exceeded $1.8 trillion in 1999.[21] The massive volume and complexity of tasks demanded of the FTC has generated concerns about whether the FTC should handle Internet-related consumer concerns or whether a newly established Federal Data Protection Agency is a viable alternative.

A fourth factor is the ongoing debate over the government's role in regulating the Internet in general and online privacy in particular. Some critics either have a distrust of government or they simply perceive industry self regulation as a more efficient method to regulate the Internet.[22] Perhaps this trepidation about government regulation is legitimate in light of numerous U.S. federal agencies' failure to protect consumers' privacy on the Internet. In an effort to promote the efficiency of the marketplace, the FTC has identified potential consumer protection issues, held public forums, and strongly encouraged self regulation.[23] Furthermore, the FTC has established four fair information principles for the protection of consumer privacy on the Internet. The four principles are notice (notification of a Web site's data collection practices), choice (the right to opt out), access (to one's personal data) and security (assurance that the data provided is secure).[24] In the past, these principles have been used to evaluate the conduct of commercial sites on the Internet. Recently, the Government Accounting Office (GAO) studied how federal government agencies fared when measured against the FTC's fair information principles for commercial Web sites. The GAO results demonstrate that government agencies are failing to comply with the FTC principles for online privacy protection.

> As of July 2000, all of the 65 web sites in our survey collected personal identifying information from their visitors, and 85 percent of the sites posted a privacy notice.The majority of these federal sites (69 percent) also met FTC's criteria for Notice. However, a much smaller number of sites implemented the three remaining principles —Choice (45 percent), Access (17 percent), and Security (23 percent). Few of the federal sites — 3 percent— implemented elements of all four of FTC's fair information principles. Finally, a small number of sites (22 percent) disclosed that they may allow third-party cookies; 14 percent actually allowed

21. Jeanna Greene, *FTC Affected by Deluge of Mergers*, Natl. L.J. B5 (Sept. 18, 2000).

22. Fred H. Cate, *Principles of Internet Privacy*, 32 Conn. L. Rev. 877, 890 (2000) (asserting that "when it comes to privacy, Americans generally do not assume that the government necessarily has citizens' best interests at heart.").

23. David Medine, *Regulatory Issues in Internet Privacy: The FTC's Role* ¶ 5 (May 1998) (available in WL, 3 No. 1 GLEBLCR 7).

24. Steve Lohr, *Online Industry Seizes the Initiative on Privacy*, N.Y. Times ¶ 22 <http://www.nytimes.com/library/tech/99/10/biztech/articles/11priv.html> (accessed Oct. 24, 2000).

their placement.[25]

One commentator amply articulated consumer fears of Big Brother in stating, Nobody is going to be out there protecting me. I don't think the EU and the data czar will protect me. I very much doubt that the federal government will protect me. In fact, they are the most frightening aspect of the whole thing. [26] In effect, consumers are concerned about whether the Federal Government is a protector of privacy or the primary predator that devours privacy rights.[27]

A fifth factor that has generated thought about the feasibility of a Federal Data Protection Agency is the tremendous array of privacy laws within the U.S. Privacy within the U.S. is broadly categorized into two spheres, transactional and informational.[28] The former encompasses the right to prohibit other people or the Government from knowing what a person engages in at a given moment. The later, encompasses the right to prohibit other people or the Government from obtaining information about a person's past. These broad generalized conceptions of privacy provide categories, but fail to depict the depth of sources for privacy concerns in the U.S.

Professor Dorothy Glancy has provided a comprehensive discussion on how the application of privacy laws to the Internet leads to considerable complexity and uncertainty.[29] Glancy explains that U.S. privacy law is diverse, decentralized and dynamic.[30] Privacy laws are diverse because different types of privacy law arise from constitutional law, common law, statutory law, regulatory law, and self-regulatory measures.[31]

---

25. Letter from Honorable Dick Armey, Majority Leader, House of Rep., to Honorable W.J. "Billy" Tauzin, Chairman, Subcomm. on Telecomm., Trade and Consumer Protection Comm. On Commerce, *Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles* (Sept. 11, 2000) (copy on file with the author).

26. Symposium, *Privacy in Cyberspace Transcripts from the 1999 Judge James R. Browning Symposium*, 61 Mont. L. Rev. 43, 49 (2000) [hereinafter *Privacy in Cyberspace*].

27. David Stout, *Major University to be Asked to Review F.B.I.'s 'Carnivore,'* N.Y. Times ¶ 5 <http://www.nytimes.com/library/tech/00/08/biztech/articles/11cnd-carnivore.html> (accessed Aug. 15, 2000). Public fears about the Federal Government's cyber-surveillance through a program called Carnivore has prompted the U.S. Justice Department and a major university to review the FBI's e-mail surveillance program to determine how and when the Federal Government has invaded individual privacy. *Id.* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness,* 11 Berkeley Tech. L.J. 1, 48-56 (1996) (discussing the U.S. Government's interest in collecting data about individuals).

28. *Privacy in Cyberspace*, *supra* n. 26, at 43.

29. Dorothy Glancy, Symposium, *At The Intersection of Visible and Invisible Worlds: United States Privacy and The Internet*, 16 Santa Clara Computer & High Tech. L.J. 357, 358 (2000).

30. *Id.*

31. *Id.* at 364; *see also* F. Lawrence Street & Mark P. Grant, *Law of The Internet*, 109-220 (Lexis Law 2000) (listing common law privacy rights, constitutional privacy rights,

Each source of law generates volumes of jurisprudence and questions about the definition, scope, regulation and enforcement of privacy in both the real world and the cyberworld.

Professors Paul Schwartz and Pamela Samuelson have also discussed the flaws in U.S. privacy laws. Schwartz states that it is time to consider a new definition of privacy, which defines privacy norms as shifting and multidimensional.[32] According to Schwartz, privacy laws are cloaked in uncertainty, and this has a negative impact on individual self-determination and is unhealthy in a deliberative democracy.[33] Schwartz proposes, "In place of the existing privacy horror show, we need . . . fair information practices."[34] Samuelson has explained, ". . . a serious impediment to a comprehensive approach [to the challenge of information privacy] in the U.S. is the lack of clarity in this country about the nature of the interest that individuals have in information about themselves: Is it a commodity interest, a consumer protection interest, a personal dignity interest, a civil right interest, all of the above, or no interest at all?"[35]

The above factors of increased scholarship, public rage, the volume of subject matter on the Internet, the debate about the role of government, and the proliferation of privacy laws have created a vacuum. This vacuum, has in turn, presented a dilemma of how to place the Internet under increased surveillance while protecting both commercial interests and individual privacy. Because the Internet is unlike any other medium it raises questions about whether the traditional theories of property, speech and privacy apply. Due to the Internet, these theories are in a state of flux, and the resulting disorder seemingly demands an urgent solution. One reference point is the approach adopted by the EU, which has established a privacy commission or agency. Although an appealing model, the U.S. should proceed with caution when considering the adoption of the EU's approach for regulating Internet privacy.

---

statutory privacy protections, and privacy legislation in the U.S.); *see generally* Jonathan Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 Cath. U. L. Rev. 1183, 1192-1206 (1999); Elizabeth deGrazia Blumenfeld, *Privacy Please: Will the Internet Industry Act to Protect Consumer Privacy Before Government Steps In?*, 54 Bus. Lawyer 349, 357 (1998) (available in WL, 54 BUSLAW 349).

32. Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn. L. Rev. 815, 834 (2000).

33. *Id.* at 833; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1607 (Nov. 1999).

34. *Id.* at 1607 (defining fair information practices as obligations, transparent processing systems, limited procedural and substantive rights, and external oversight).

35. Pamela Samuelson, Symposium, *Privacy as Intellectual Property?*, 52 Stan. L. Rev. 1125, 1170 (May 2000).

III. EUROPEAN UNION & THE UNITED STATES NOTIONS OF PRIVACY

On October 24, 1995, the European Parliament and the Council of the European Union adopted Directive 95/46/EC [hereinafter "EU Directive"].[36] The objective of the EU Directive was to facilitate among states the adoption of laws to protect an individual's fundamental right to privacy with respect to the processing of personal data and the flow of data between states.[37] The EU Directive recognizes privacy as a fundamental human right.[38] The EU Directive's guidelines for information privacy are: personal data is collected for specific legitimate purposes; the data must be relevant, accurate, current, not excessive and kept no longer than necessary; personal data may be processed only if the Internet user has unambiguously given consent (or under specified exceptions); member states must establish supervisory bodies, (e.g., commissions, regulatory agencies) and remedies for a breach of privacy rights; and, transfer of data to a third country is restricted unless the third country has an adequate level of protection for data privacy.[39] The EU Directive is deemed to be more protective of privacy rights than the privacy protections within the U.S. because the former recognizes privacy as a fundamental right and requires member states to appoint a privacy regulator or commissioner and establish national privacy laws, while the latter has failed to develop a coherent definition for privacy.[40]

The EU Directive places considerable pressure on the U.S. to regu-

36. *Directive 95/46/EC of the European Parliament and of the Council of Oct. 24 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,* 1995 O.J. (L 281/33) ¶¶ 75-93 <http://europa.eu.int/eur-lex/en/lif/dat/1995/ en_395L0046.html> (accessed Aug. 30, 2000) (commenting on the protection of individuals with regard to the processing of personal data and the free movement of such data).

37. *Id.* at ¶ 76 The object of the Directive provides: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1." *Id.*

38. *Id.* at ¶¶ 1, 10, 37; *see also* Al Gidari & Marie Aglion, *EU Directive on Privacy May Hinder E-Commerce*, IP Magazine ¶ 1 <http://www.ipmag.com/dailies/ 980629.html> (June 29, 1998).

39. Donna N. Lampert, *Internet Privacy: An Overview of Domestic and International Issues and Policy Responses* 372 (Mar. 2000) (available in WL, 597 PLI/Pat 357); *see also* Kurt Wimmer, *Internet Privacy and Free Expression: New Media for the New Millennium* 18 (Spring 2000) (available in WL, 18-Spg. ComLaw 1); Eric J. Sinrod, Jeffrey W. Reyna & Barak D. Jolish, *The New Wave of Speech and Privacy Developments in Cyberspace,* 21 Hastings Commun. & Ent. L.J. 583, 595 (1999).

40. Karl D. Belgum, *Who Leads at Half-Time?: Three Conflicting Visions of Internet Privacy policy,* 6 Rich. J. L. & Tech. 1, 66 (1999).

late Internet privacy and provide adequate protections. [41] The EU Directive's requirement of adequate protection and government regulation caused grave concerns for U.S. businesses with a preference for self regulation. Although the U.S. did not join as one of the member states that adopted the EU Directive, the U.S. later reached a safe harbor agreement with the EU.[42] This agreement was reached through the U.S. Department of Commerce to encourage the implementation of effective protections for consumer privacy on the Internet.[43] The approach taken in the safe harbor agreement is a departure from the EU Directive. While the EU Directive seeks to promote the creation of privacy laws by member states, the safe harbor agreement seeks to encourage self-regulatory efforts in the private sector for data collection and dissemination. Under the safe harbor Agreement, a U.S. company must register with the FTC, commit itself to comply with the EU Directive, notify customers when data is collected, provide for an opt-out opportunity, and allow Internet users to obtain and modify information held by the company.[44] Adherence to the principles of the safe harbor Agreement is entirely voluntary.[45]

The cultural and jurisprudential differences between the EU and the U.S. are depicted in their different policies and practices to governing Internet privacy. Privacy protections under the EU Directive are stricter than in the U.S. Under the EU Directive, privacy is a fundamental right, whereas, in the U.S., privacy has developed more piecemeal and state-by-state. In the U.S., for example, most state legislatures discussed, debated or passed privacy legislation during their respective 2000 legislative sessions.[46] In addition, the U.S. Supreme Court, unlike the EU, has not recognized a fundamental right to privacy. Rather, the Court has addressed various issues related to privacy and found privacy rights implicit in the Bill of Rights.[47]

---

41. Thomas J. D'Amico & June E. Cohan, *Eye On Washington* 22 (Mar. 1999) (available in WL, 1 No. 5 E-Commerce L. Rep. 22).

42. *See* U.S. Dept. of Commerce, *International Safe Harbor Privacy Principles* ¶ 1 <http://www.epic.org/privacy/intl/doc-safeharbor-1198.html> (DOC Nov. 4, 1998).

43. *Id.*

44. Wimmer, *supra* n. 39, at 18; *see also* Sinrod, *supra* n. 39, at 595.

45. U.S. Depart. of Commerce, *supra* n. 42, at 1.

46. *See e.g.* Government Relations, *State Privacy Legislation* <http://www.sia.com/state_affairs/html/state_privacy_issues.html> (accessed Nov. 22, 2000).

47. *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) (stating that although a right to privacy is not expressly stated in the U.S. Constitution, it is implicit in the Bill of Rights); Katz v. United States, 389 U.S. 347 (1967) (recognizing that the Fourth Amendment protects individuals' reasonable expectations of privacy against certain government intrusions); *Paul v. Davis*, 424 U.S. 643, 713 (1976) (recognizing a right to privacy for marriage and child rearing); *Roe v. Wade*, 410 U.S. 113, 153 (1973) (recognizing that a woman's decision whether to terminate her pregnancy is a privacy right).

Furthermore, unlike the EU, data privacy in the U.S. has been construed as a matter of commerce rather than a fundamental right because the power to regulate Internet privacy is within the jurisdiction of the FTC. In a report to Congress, the FTC suggested legislation to establish standards for the collection and use of information online for profiling and the creation of an agency to enforce those standards.[48] The FTC also emphasized that self regulation by the private sector was the most effective and least intrusive method to ensure fair trade, access, choice, security, enforcement and other consumer protections on the Internet.[49] Despite the different approaches adopted by the U.S. and the EU to regulating Internet privacy, both have begun serious consideration of the issue. Notwithstanding these efforts, the global nature of the Internet makes its regulation a matter beyond the geographical boundaries of the U.S. and Europe.

IV. WESTERN THEORIES OF PRIVACY FOR THE GLOBAL COMMUNITY?

The Internet connects the world unlike any other medium and has made geographical distances less relevant.[50] It is impractical to define privacy on the Internet from a Western perspective without the input of nations throughout the world. While the U.S. enters the new millennium and considers the establishment of a Federal Data Protection Agency, caution should be exercised lest privacy rules are established and it is later discovered that the rules are one-dimensional and obsolete. Technology is moving rapidly, and all societies throughout the world have concepts of privacy.[51] It may behoove the West to consider privacy concepts offered by moral philosophy and anthropology to determine whether privacy is a universal or local concept, or both.[52] In the

48. Federal Trade Commission Rpt., *Online Profiling: A Report to Congress, Part 2 Recommendations* (July 2000) ¶ 9 <http://www.ftc.gov/os/2000/07/onlineprofiling.htm>.

49. Federal Trade Commission Rpt., *Self-Regulation and Privacy Online* ¶ 5 <http://www.ftc.gov/os/1999/9907/pt071399.htm> (accessed Oct. 24, 2000).

50. David R. Johnson & David Post, Symposium, *Law and Borders – The Rise of Law in Cyberspace,* 48 Stan. L. Rev. 1367, 1370-76 (May 1996). *See also* Walter Gary Sharp, Sr., *Cyberspace and The Use of Force* 18-25 (Aegis Research 1999) (suggesting that war in the 21st century will take a new form and include computer espionage and computer network attacks because of the world's interconnectedness). The targets of war will include critical infrastructures such as: telecommunications, electrical and power systems, gas and oil storage, transportation, banking and finance, water supply system, emergency services and the continuity of government.

51. Jerry Kang, *Information Privacy in Cyberspace Transactions,* 50 Stan. L. Rev. 1193, 1212 (Apr. 1998) (indicating that there are zones of privacy in each culture, even if culturally, we react differently to certain disclosures).

52. Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment,* 24 Rutgers Computer & Tech. L.J. 1, 10-12

quest to define and regulate Internet privacy, the U.S. and the EU must adopt a "Marco-Polo-like" approach and seek the cultural and intellectual perspectives of other nations. A contemporary definition of privacy must include a global perspective[53] and extend beyond a pre-Marco Polo perspective that the West comprises the entire world.[54] The U.S. and EU must acknowledge that the world is more interconnected than in the past and that the Internet is a global mechanism or virtual silk road of information and commerce.[55] This acknowledgment is critical for governing privacy on the global Internet, which in 1995 reached 100 countries,[56] and by 2004 will reach 1.4 billion people worldwide.[57]

In an effort to establish a global consensus on privacy, a group called Privacy International published a report titled, *Privacy & Human Rights 1999*.[58] The report outlines the threats to privacy, provides a definition of privacy, and explains the right to privacy and the technologies that threaten and invade privacy.[59] According to the report approximately 40

(1998) (discussing the works of Alan Westin who surveyed privacy concepts, including the theories of renowned anthropologist Margaret Mead).

53. Gillian Triggs, *Confucius and Consensus: International Law in the Asian Pacific*, 21 Melb. U. L. Rev. 650, 652-53 (Dec. 1997) (noting in 1945 when the Charter of the United Nations was signed, there were only 50 nations, and they shared a similar cultural background). However, since 1945, 89 countries have undergone decolonization and have demonstrated belief systems at variance with Western values. *Id.*

54. 2000 I.C.J. Acts & Docs., *Statute of the International Court of Justice* <http://www.icj-cij.org/icjwww/ibasicdocuments/ibasictext/ibasicstatute.htm> (accessed Nov. 22, 2000). The perception that the West comprised the entire world and other people were insignificant or uncivilized existed as late as the 20th century. *Id.* For example, when nations decided to establish the International Court of Justice it was agreed that disputes would be settled through the application of, *inter alia*, "the general principles of law recognized by *civilized nations.*" *Id.* The term *"civilized"* is from article 38 of the Statute of the International Court of Justice. *Id.*

55. *See* Henry Kissinger, *Diplomacy* 23-28 (1994) (noting the world has become more interdependent and that the former USSR and the United States can no longer maintain global bipolar dominance). *See also* Jane Perlez, *With Time Short, Albright Stays Aloft*, N.Y. Times, A7 (July 3, 2000) (indicating that Madeleine Albright, Secretary of State for the Clinton Administration, advocated a global community with emphasis on Internet literacy in nations under dictatorships).

56. Karen S. Frank, *Potential Liability on the Internet*, 437 PLI 417, 421 (1996) (citing statistics from the International Internet Association).

57. The ARC Group, *Wireless Internet: Applications; Technology & Player Strategies* <http://www.the-arc-group.com/reports/wireless_2000/titlepage_wi2k.htm> (accessed Oct. 24, 2000).

58. Privacy International, *Privacy & Human Rights 1999* <http://www.privacyinternational.org/survey/summary.html> (accessed Oct. 24, 2000) (indicating that privacy is a fundamental right recognized by all major international treaties and agreements on human rights).

59. *Id.* Such technologies include identity cards, biometrics, communications surveillance, interception of e-mail and Internet communications, national security and the echelon system, video surveillance, and workplace surveillance. *Id.*

nations have enacted privacy and data protection laws to protect Internet privacy.[60]

The fact that approximately 40 nations have enacted privacy laws for the Internet appears impressive; however, that number represents a small percentage of the 190 independent states[61] and approximately 50 dependencies and areas of special sovereignty.[62] Notably, two "major parts of the world" are not present in this global effort to define privacy on the Internet. These are the Islamic cultures and China. Both are characterized as "major parts of the world" because they constitute a significant percentage of the world's population.[63] World population has reached 5.9 billion,[64] with the total number of Muslims estimated at 1 billion,[65] and the population of China estimated at 1.243 billion.[66] Approximately, one out of five people in the world live in China. Furthermore, China has a large Muslim population with 40,000 imams, 26,000 mosques[67] and millions of Chinese Muslims on Mainland China.[68] Con-

60. *Id.* (listing privacy measures adopted by such countries as Argentina, Australia, Belgium, Brazil, Bulgaria, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, Iceland, India, Ireland, Israel, Italy, Japan, South Korea, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, Poland, Portugal, Russia, San Marino, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, and Taiwan).

61. U.S. State Dept., *Independent States of the World* <http://www.state.gov/www/regions/independent_states.html> (accessed Oct. 24, 2000) (listing 190 independent states).

62. U.S. State Dept., *Dependencies & Areas of Special Sovereignty* <http://www.stategov/www.regions/dependencies.html#> (accessed Oct. 24, 2000).

63. For information about China's population *see*, United Nations, *1998 Revision of World Population Estimates and Projections* <http://www.popin.org/pop1998/1.htm> (accessed Oct. 25, 2000) (indicating that 2 out of 5 people in the world live in either China or India). Although beyond the scope of this article, data indicates that India has also emerged as a technologically orientated society. *Id.*; *See* Standard.com, *India Eyes Steps to Bring Info Tech to the Masses* (available at <http://www.thestandard.net/article/display/0,1151,17689,00.html>) (accessed Oct. 25, 2000) (explaining India has made tremendous efforts to use the Internet and related technologies for economic development); *Cyber Law To Come Into Effect in a Month*, Arab News 8 (Aug. 16, 2000) (noting despite a lack of an expressed right to privacy in its constitution, India has passed laws for commercial transactions covering digital records, signatures, and transactions all of which were illegal until India passed a *Information Technology Act* in mid-2000); Privacy and Human Rights Overview, *An International Survey of Privacy Laws and Practice*, <http://www,gilc.org/privacy/survey/intro.html> (noting that along with the U.S. and Ireland, India does not have an expressed right to privacy in its constitution, but it has recognized a right to privacy).

64. United Nations, *supra* n. 63.

65. *The World Almanac and In-Depth Book of Facts* 727 (Robert Famighetti et al. eds., 1994).

66. *People's Republic of China Yearbook* 1998/99 vol. 18, 362 (1998/99).

67. *Id.* at 370. (noting the other main religions in China are Buddhism, Taoism, and Christianity).

68. *See generally* Dru C. Gladney, *Muslim Chinese: Ethnic Nationalism in the People's Republic* (1991) (discussing the history of Islam in China); Marco Restelli, *China's Secret Holy War*, World Press Rev., 43 (May 1994) (explaining that statistics about the number of

sequently, one-fifth of the world's population resides in China, one-fifth are Muslims, and a significant number are both Chinese and Muslim.

Eventually, both the Islamic world and China will adopt the Internet as an integral part of their economies.[69] Interestingly, both have domestic legal systems or customs at variance with Western jurisprudence.[70] Along with these cultures, there are other cultures with tremendous populations of peoples who have different legal systems, cultures, and perceptions of what is private and protected.[71] The increasing popularity of the Internet in these cultures raises concerns about whether the definition and regulation of privacy promulgated by a U.S. Federal Data Protection Agency will prove adequate for the global Internet? At a minimum, any Western attempt to regulate Internet privacy must assimilate the knowledge and cultures of Asia and the Middle East, similar to Marco Polo in the 13th century, in order to facilitate the global Internet virtual silk road of e-commerce.

The difference between culture and law in the West and in an Islamic culture is depicted in Saudi Arabia's strong interest in regulating the Internet.[72] The Saudi government deliberately limits access to the Internet. It costs more to access the Internet in Saudi Arabia than any

---

Muslims in China vary, but estimates a total of 50 million). *See also* Bureau of East Asian & Pacific Affairs, *Background Notes: China, August 1998* <http://www.state.gov/www/background_notes/ china_1098_bgn.htm> (accessed Oct. 25, 2000) (stating the Chinese government places the number at 18 million).

69. This assertion is based on the general view that the Internet is a means to generate wealth. *See e.g.* Thomas S. Valovic, *Digital Mythologies* 27-28 (Rutgers U. Press 2000) (stating there is a general perception that computer networks generate wealth through new economic orders and the elimination of "multilayered inefficiencies that have become characteristic of the institutions of modern corporate and government life."). The Chinese government has specifically stated that it expects the Internet to invigorate Chinese businesses so they can compete with the West. *Id.; See* Peter Ferdinand, *The Internet*, Democracy and Democratization 4 (2000).

70. *Contra* Anastasia Stanmeyer & Paul Mooney, AsiaWeek.com, *An Identity Crisis The Collapse of Ideology Leaves Generations Adrift in a Moral Vacuum* <http://www.cnn.com/ASIANOW/asiaweek/magazine/99/0924/cn_society.html> (accessed July 17, 2000) (arguing that China has lost it cultural focus which it had under Maoism, and that today's China has become culturally and morally adrift because it is swayed by the free-market economy and pop culture).

71. Rene David, Les Grands Systems De Droit Contemporaines 22-32 (5th ed. 1973), *cited in* Lakshman D. Guruswamy et al., *International Environmental Law And World Order: A Problem Orientated Course Book* 136 n.4 (1999) (explaining there are five dominant legal systems throughout the world: the Romanist-German-Civilist legal system, the Common law legal system, the Marxist-Socialist legal system, the Islamic legal system, and, the Asian legal system).

72. Douglas Jehl, *The Internet's 'Open Sesame' Is Answered Warily* <http://www. nytimes.com/library/tech/99/03/biztech/articles/18riyadh.html> (accessed Aug. 19, 2000) (stating that besides Saudi Arabia, other Islamic countries also have conservative approaches toward the Internet due to religious, cultural, and state security concerns).

other place in the world.[73] Exorbitant costs allow the Saudi government to control the who, what, when, where, and how behind Internet access. There are also filters on the Internet in Saudi Arabia, and these filters slow down access and further discourage Internet use in Saudi Arabia.[74] The filters are a product of Saudi Arabia's efforts to impose strict censorship policies on Internet users. The Saudi government, for example, blocks America Online, and the 30 Internet service providers operating in Saudi Arabia are prohibited from connecting to the Internet via satellite.[75] Such government conduct raises a concern about how the Saudi government will define and regulate the privacy rights of Saudi citizens on the Internet as it balances privacy rights against the need to control the flow of information.[76]

Along with culture, the laws in Islamic countries may impact whether the U.S. can effectively provide a global framework to define, regulate, and protect Internet privacy. The Islamic legal system is a viable legal system with laws governing Internet-related topics such as banking, torts, and contracts.[77] Islamic jurisprudence has a distinct banking system that forbids interest, and characterizes interest as usury.[78] The Islamic system of commercial law challenges Western com-

73. *See generally* NEWS, *Cyber Rebels,* Star-Tribune Newspaper of the Twin Cities Mpls.-St. Paul (Aug. 1, 1999) (available in 1999 WL 7506258).

74. *Id.*

75. Andy Serwer, *Tech is King; Now Meet the Prince*, Fortune, 105-06, 117 (Dec. 6, 1999) (noting that the standard for Internet access in Saudi Arabia is different for the royal family, which has access to satellite connections).

76. Shafaq Al-Otaibi, *3,000 Porno Films Seized in Abqaiq; Three Indians Held*, Arab News, 2 (July 22, 2000). The Saudi government seems particularly concerned about controlling the flow of pornographic materials on the Internet and through any other means. *Id.* Between April 2000 and July 2000, the Saudi government arrested numerous persons who sold or rented pornographic videos and confiscated 13,000 pornographic videos. *Id.*

77. John Makdisi & Marianne Makdisi, *Islamic Law Bibliography: Revised and Updated List of Secondary Sources,* 87 L. Lib. J. 69 (1995); *see also*, John Makdisi, *The Islamic Origins of the Common Law,* 77 N. Car. L. Rev. 1635 (1999); Abdulmunin Shakir, *Constitutions of the Countries of the World* (Albert P. Blaustein & Gisbert M. Flanz eds., 1976). The Saudi government has indicated that the Quran is its constitution. *Id.* Along with the Quran, the other sources of Islamic law are: Sunnah (traditions of Prophet Muhammad); Quas (reasoning on issues and problems that have an analogy in the Qur'an or Sunnah); Idjtihad (reasoning on issues and problems that do not have an analogy in the Qur'an or Sunnah); and, Idjma (consensus of learned Islamic scholars). *Id. See also* Omar Saleem, *Be Fruitful and Multiply, and Replenish the Earth and Subdue It: Third World Population Growth and Global Warming*, 8 Geo. Int'l. Envtl. L. Rev. 1, 14 (1995). Due to globalization, Islamic scholars have begun to grapple with the Islamic perspective for interest-based banking, credit accounts, import contracts, and investments. *See Islamic Scholars to Meet in Riyadh to Debate Modern Topics*, Arab News 2 (Sept. 22, 2000); Javid Massan & Mabib Badr, *Islamic Jurists debate Key Questions* Arab News 2 (Sept. 25, 2000) (discussing the impermissibility of using Internet-based credit cards).

78. The Qur'an provides: "O you who believe! Do not live on usury, multiplying your wealth many times over (as compound interests)." *Id.* Abdullah Yusuf 'Ali, *The Meaning of*

mercial concepts in two significant ways.[79] It challenges the general belief that Western concepts of commerce are more efficient and superior, and it challenges the belief that commerce should be separate from religion.[80] Will either of these challenges present a threat to a global definition of privacy propounded by the West in its efforts to regulate online commercial transactions? If so, how will such threats impact e-commerce? The popularity of Internet use in Islamic cultures simultaneously raises concerns about Internet regulation. How will the Saudi government allow surfing of the Internet for e-commerce purposes and simultaneously perpetuate its need to monitor the conduct of its citizens? How will such a government define and regulate Internet privacy? The Saudi Arabian combination of a monarchal government, religion, and commercial interests, may generate a privacy policy significantly different from the Western views of privacy.

Although the Islamic world could possibly impact Internet privacy, it is unlikely to do so in the immediate future. This assertion is based on the number of Internet users in Islamic countries,[81] and the fact that the Islamic world is fragmented,[82] and has few Islamic states that are governed by "pure" Islamic law without secular based law in their legal system.[83] Centralized government has stifled Internet growth in Islamic countries. Conversely, China, even with a centralized government, has seen its total number of Internet users grow exponentially every 6 months. It is, therefore, probable that China will have the greatest immediate impact on shaping a global definition for Internet privacy.

---

the Holy Qur'an, 3:130 (Amana Pub. 1997). From the Islamic point of view, credit cards are permissible if the cardholder pays the bill on time and is not charged interest. *See Credit Cards and Late Payment*, Arab News 19 (Sept. 29, 2000).

79. Frank Vogel & Samuel L. Hayes, III, *Islamic Law and Finance Religion, Risk and Return* 19 (Kluwer L. Intl. 1998).

80. *Id.*

81. *See Kingdom's Banks Embark on Internet Race*, Arab News, 14 (Aug. 23, 2000) (stating that the Internet arrived late in Saudi Arabia, where Internet services were available for the first time in 1999).

82. Saleem, *supra* n. 78, at 1 (1995) (noting the inaccurateness of the popular impression that Muslims are a homogeneous population from the Middle East). Over four-fifths of the world's 1 billion Muslims live in Asia and Southeast Asia. *Id.* The country with the largest Muslim population is Indonesia, followed by Pakistan, Bangladesh, and India. *Id.* Each country with a Muslim population brings their own cultural differences and experiences to the religion. *Id.* Dr. Atta-ur-Rahman, Pakistani minister for science and technology commented on the reasons behind the lack of scientific and technology in the Muslim world, "We [Muslims] have divided ourselves into little states with very poor facilities and infrastructure." *Id. See also Feature: Science and Technology Key Options for the Muslim World*, Arab News, 11 (July 19, 2000).

83. Rodolphe J.A. De Seife, *The Shar'ia: An Introduction To the Law of Islam* 2 (Austin & Winfield 1994) (noting at the turn of the new millennium the only "pure" Islamic states, i.e., those that claim the Shariah as the rule of law, are Saudi Arabia, Afghanistan, Pakistan, Iran, and Sudan).

V. CHINA AND THE INTERNET

The exponential growth of the Internet in China is staggering with the total number of users doubling every 6 months. In January 1999, China had 2,100,000 Internet users.[84] In July 1999, that figure nearly doubled to 4,000,000.[85] From July 1999 to January 2000, the number of Internet users in China doubled from 4,000,000 to 8,900,000.[86] In July 2000, the 8,900,000 doubled to 16,900,000.[87] The most popular Web site for Chinese-language users is Sina.com, which attracts 102 million hits per month.[88] Among the 46 high-tech hubs deemed most significant in the new global high-tech network, Wired Magazine listed the Chinese territories of Hong Kong and Taiwan.[89] ChinaOnline provided the following facts about China-related Internet activities:

> (1) China is MasterCard's second biggest market (2) China will have 300 million Internet users by 2005. By then, the U.S. will have just 200 million. (3) One in four tech companies started in Silicon Valley since 1980 are run by ethnic Chinese and Indian immigrants. (4) The Chinese Web will be larger than the English Web by 2010. (5) American high tech exports to China grew 500 percent between 1990 and 1998 alone. (6) Over 64% of Chinese Internet users reported they spent less time watching TV and 67% reported sleeping less since getting the opportunity to use the Internet. (7) E-commerce will grow from 1999's US$42 million to $US3.8 billion by 2003. (8) Fully 28% – and growing – of Silicon Valley's entrepreneurs are of Chinese origin. (9) China attracts more direct foreign investment than any country except the United States. (10) China will have more Internet users than any other Asia-Pacific nation by 2001, with 40 million people online. *By 2005, China will have the most Internet users in the world (Emphasis*

84. China Internet Network Info. Center, *Statistical Report of the Development of China Internet (1999.1)* <http://www.cnnic.net.cn/develst/e-9901.shtml> (accessed Oct. 24, 2000).

85. China Internet Network Info. Center, *Semi-Annual Survey Report on Internet Development in China (1999.7)* <http://www.cnnic.net.cn/develst/e-9907.shtml> (accessed Oct. 24, 2000).

86. China Internet Network Info. Center, *supra* n. 85.

87. China Internet Network Info. Center, *supra* n. 85. (noting that there are 16.9 million Internet users in China); Inside China Today Daily News, *China Vows to Battle "Enemy Forces" on Internet* <http://www.insidechina.com/news. php3?id=187292> (accessed Oct. 24, 2000) [hereinafter *Enemy Forces*].

88. Neel Chowdhury, The New China, *Web War, Part 2* <http://www.fortune.com/ fortune/china/wir2.html> (accessed Oct. 24, 2000).

89. *Venture Capitals*, Wired 258-59 (July 2000). Wired Magazine determined what constitutes a digital hub of international significance based on several factors: whether universities and research facilities train skilled workers or develop new technology; whether established companies and multinationals are present for expertise and economic stability; whether the population has "entrepreneurial drive" to initiate ventures; and, the availability of venture capital. *Id.*

added).[90]

If the above statistics are correct, China, with a population in excess of 1 billion, will have more Internet users than any country in the world by 2005. Additional data indicates the average Internet user in China will be a 35-year-old urban male with a college education. This user will spend less time watching television and sleeping to use the Internet several hours per week.[91] As a young capitalist, he will embrace a popular belief espoused since the leadership of Deng Xiaoping, namely, that wealth is good.[92] As an educated entrepreneur, he will have more discretionary funds, along with millions of fellow citizens, to engage in e-commerce. Estimates suggest that by 2003, online shopping in China will spread like wildfire, and Chinese consumers will engage in e-commerce to a considerable extent[93] because household incomes in China are increasing, while technology and online access costs are declining.[94]

The expansive Internet use in China has been coupled with massive foreign investment in China's economy.[95] China attracts more foreign investment than any country in the world except the U.S.[96] The U.S. has invested heavily into China's economy: AT&T invested $81 million in the early 1990s; Microsoft invested $80 million in 1998 for a research laboratory; and Motorola invested $1.5 billion between 1998 and 1998.[97] A study conducted by the American Bar Association reveals:

---

90. ChinaOnline, *Interesting Facts About China* <www.chinaonline.com> (accessed Nov. 4, 2000).

91. Marty Williams, *Survey Reports Big Interests in Internet Among Chinese*, Internet Newsbytes (Apr. 15, 1999). The notion of "getting online" is a significant part of China's news pop-culture. *See* Arif Dirlik and Xudong Zhang, Postmodernism & China (2000).

92. Brian Palmer, *The New China What the Chinese Want*, Fortune.com, <http://www.fortune.com/fortune/china/gal.html> (accessed Oct. 16, 2000) (providing a Gallup Organization survey which gauged consumer attitudes and lifestyles in China, in which among 4,000 people, one-fourth stated that they would like to start their own business).

93. Neel Chowdhury, *The New China Web War*, Fortune.com, <http://ww.fortune.com/fortune/china/wir.html> (accessed Oct. 24, 2000).

94. *Microsoft Aims to Promote Internet in China Reuter, Business Today* <http://www.bostonherald.com/bhbusiness/mschina03101999.htm> (accessed Nov. 10, 2000) (describing how the Microsoft Corporation has sought to make the Internet more widespread in China with the placement of a box atop a television, called the Venus operating system).

95. Orville Schell and David Shambaugh, *The China Reader* xvii – xviii (1999). In 1978, China had no direct foreign investments and no foreign debt. *Id.* In 1997, China had more foreign investments than all nations, except the U.S., and its debtor status changed to establish China as the largest borrower from the World Bank. *Id.* In addition, China's per capita income quadrupled between 1978 and 1995. *Id.*

96. ChinaOnline, *supra* n. 90.

97. Omar Saleem, *The Spratly Islands Dispute: China Defines the New Millennium,* 15 Am. U. Intl L. Rev. 527, 548-49 (2000) (noting other investors in China include Ford Motor Company, Time Warner, IBM, Kentucky Fried Chicken, and Boeing).

> U.S. investment in China has grown every year since 1992 and reached a total of $14.1 billion in 1997. U.S. exports to China have also risen significantly in the past few years, particularly with respect to telecommunications, power generation, oil and gas exploration, chemicals, aircraft, fertilizer, wheat/cereal products, and construction machinery. China's airport infrastructure construction is anticipated to reach an estimated sum of $8.4 billion and aircraft sales are estimated at $10 to 15 billion over the next ten years. U.S. firms are pursuing a number of untapped markets in China, including pharmaceuticals, automotive components, automotive production machinery, medical equipment and devices, and transportation.[98]

The exponential growth of the Internet in China and the massive investment in its economy facilitate the emergence of e-commerce. Questions remain about whether China will adopt the rules for Internet privacy as espoused by the EU Directive and a U.S. Federal Data Protection Agency. China, similar to most countries, will eventually enact online privacy laws. The reasons why a country enacts privacy laws may differ from one country to the next.

The view articulated in the Privacy Report, is that nations enact privacy laws for various reasons: to remedy past injustices (Central Europe, South America and South African); to promote e-commerce (Canada, U.S. and Asia); and, to comply with the EU Directive for membership in the European Union (Central and Eastern Europe).[99] China will likely accept a U.S. definition for online privacy promulgated by the EU Directive or a U.S. Federal Data Protection Agency, but with a precondition and not for above reasons articulated by the Privacy Report.

Domestically, China recognizes a substantive privacy right traced back to ancient China.[100] Contemporary China has a commercial legal system similar to France, Germany, Japan and Taiwan,[101] which suggest Chinese laws would comport with Western practices to protect on-

98. James M. Zimmerman, *China Law Deskbook* 1-2 (Am. Bar Assn. 1999). The author provides an excellent source for various areas of Chinese law such as contracts, taxation, labor and employment, financial regulations, consumer protection, customs and trade, securities regulations, environmental protection, land use, bankruptcy, dispute resolution, corporate criminal liability, and laws governing the special zones of the People's Republic of China). *See also* Pitman B. Potter, *Foreign Investment Law in the People's Republic of China: Dilemmas of State,* China's Legal Reforms 155, 162 (Stanley B. Lubman ed., Oxford U. Press 1996) (noting foreign investments in China have increased—$12 billion in 1992, $57.2 billion in 1992, and $122.7 billion for 1993).

99. *See generally* Privacy International, *supra* n. 58.

100. *See generally* Global Internet Liberty Campaign, *Privacy and Human Rights An International Survey of Privacy: Laws and Practice* <http://www.gilc.org/privacy/survey/intro. html> (accessed Aug. 18, 2000).

101. Dr. John S. Mo, *The Code of Contract Law of the People's Republic of China and the Vienna Sales Convention,* 15 Am. U. Intl. L. Rev. 209, 211 (1999).

line privacy. Furthermore, China, unlike the U.S., has a privacy provision in its constitution. Article 40 of China's constitution provides:

> Laws protect the freedom and privacy of correspondence of citizens of the Peoples' Republic of China. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence *except in cases where, to meet the needs of State security* or of investigation into criminal offenses, public security of procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law (emphasis added).[102]

In spite of China's recognition of a right to privacy dating back 5,000 years, and its contemporary commercial laws and constitutional provision, China, similar to other nations, does not regard privacy as an absolute right.[103] It is a right balanced against *"the needs of State security."*[104] The Chinese government has a strong interest in quashing

---

102. The Constitution of the Peoples' Republic of China, Ch. 2 Art. 40. <http://darkwing.uoregon.edu/~felsing/cstuff/prcconst.html> (accessed Nov. 11, 2000).

103. Seven Schwankert & Johnathan S. Landdreth, *China Tightens Control Over Web Site Publishing* <http://www.virtualchina.com/news/jan00/0128/012800-regulations2-ssjsl.html> (Nov. 11, 2000) (noting law in China was promulgated with the balancing of an individual's rights, against the interests of the state or emperor). The balancing of competing interests is not atypical in privacy disputes within the U.S. *Id.* In U.S. jurisprudence, courts often use a balancing test to determine individual rights. *Id.*; *See Terry v. Ohio*, 392 U.S. 1 (1968). For example, although the Fourth Amendment provides for "probable cause," the Supreme Court has allowed searches and seizures based on the standard of reasonable suspicion, which is a lower standard than probable cause. *Id.*; The *Terry* decision acknowledged that a stop and frisk constituted a search and seizure for Fourth Amendment purposes, but allowed the intrusion of a person's privacy interests based on reasonable suspicion rather than probable cause. The intrusion into the individual's privacy was allowed because the Court's interests in protecting the officer's safety outweighed the need to protect a suspect's privacy. *Id. See also* Omar Saleem, *The Age of Unreason: The Impact of Reasonableness, Increased Police Force, and Colorblindness on Terry "Stop and Frisk,"* 50 Okla. L. Rev. 451, 471 (1997) (discussing the balancing of officer safety and the need for effective law enforcement against the privacy rights of citizens); *US West, Inc., v. FCC*, 182 F.3d 1224 (10th cir. 1999) (noting the court balanced consumer's rights to privacy against commercial interests right to gather and distribute consumer information pursuant to rights of commercial free speech); Julie Tuan, *US West v. FCC*, 15 Berkeley Tech. L. J. 354 (2000) (critiquing the *West* decision); Joan Biskupic, *Court Limits Police Records Access* <http://www.washingtonpost.com/wp-dyn/articles/A27555-1999Dec.7html> (accessed Nov. 10, 2000) (discussing the *Los Angeles Police Dept. v. Reporting Publishing Corp.* decision where the Court weighed privacy rights against commercial interests). *Id.* The Court upheld a 1996 California law, which restricted access to police records to journalists and prohibited access of the same information to a private publishing service that sold the information to lawyers and other businesses. *Id.*

104. Frank Webster, *Theories of Information Society* 52-73 (Routledge 1995) (explaining that we live in an information-orientated world that has become more organized and global, and therefore the allegiance to statehood and self-preservation remains constant, and information and surveillance have become means of warfare to preserve the state).

dissidents, maintaining social order,[105] and screening information that is politically sensitive or harmful to the state.[106] The popular case of Huang Qi is illustrative. Huang Qi published information about the 1989 Tiananmen Square crack down on his site named www.6-4tianwang.com, and was charged with "subverting state power" and faced a sentence of life imprisonment.[107] The Chinese government has indicated that while the Internet has healthy and beneficial information, it also contains information that is reactionary, superstitious and pornographic.[108] Therefore, the government has vowed to battle the "enemies of the state" who use the Internet to undermine the state,[109] and has issued regulations restricting the "transfer of state secrets on bulletin board systems, in chat rooms or through Internet news groups."[110] The problem is that the term "state secret" is ambiguous and could include a wide range of persons and activities.[111] This inherent ambiguity is a logical result because the Chinese government propounds a "democratic" system, which dictates that a collective character ensures individual rights.[112] In other words, social control through a Communist dictatorship is the key towards a successful democracy.[113]

In conjunction with China's national security concerns, China's conception of privacy is also influenced by its culture. What is considered private in the U.S. differs from what is private in China. This is illustrated by China's current use of public showers, and how domestic disputes are handled as a public matter, rather than a private one.[114]

The Chinese government's interest in state security and the cultural components of privacy indicates that privacy is perceived as something different in China when compared with Western notions of privacy.[115] This suggests that if China were to enact privacy regulation to comply with the EU Directive or the rules promulgated by a U.S. Federal Data Protection Agency, China's would not do so to protect privacy as defined

105. *See generally* Schwankert & Landdreth, *supra* n. 103; Chih-yu Shih, *Collective Democracy Political and Legal Reform in China* 59 (The Chinese U. Press 1999).

106. *See generally* Schwankert & Landdreth, *supra* n. 103.

107. *See China Says Provinces Setting Up Internet Police,* Silicon Valley News, <http://www.mercurycenter.com/svtech/news/breaking/internet/docs/2781141.htm> (accessed Aug. 7, 2000).

108. *Enemy Forces, supra* n. 87.

109. *Id.*

110. Schwankert & Landdreth, *supra* n. 103.

111. *Id.* at ¶ 3.

112. Shih, *supra* n. 105, at 57-60.

113. *Id.*

114. Fu Hualing, *Understanding People's Mediation in Post-Mao China,* 6 J. Chinese L. 211 (1992).

115. David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,* 18 John Marshall J. Computer & Info. L. 1, 31-32 (1999).

in the West.[116] In fact, China has had a long history of tracking its citizens for record keeping purposes,[117] and an intolerance for encryption technology.[118] Therefore, if the Chinese government complies with Western theories of online privacy, its primary purposes for doing may be tangential to a policy for protection of online privacy[119]

In the past, China has manipulated issues that are "fundamental" to the industrialized nations to enable China to achieve its economic or political goals. China used this tactic with the U.S. as early as the 19th century. In 1821, a sailor aboard a U.S. merchant ship, called the Emily, dropped a ceramic bottle on the head of a Chinese fruit seller who occupied a smaller boat below the Emily.[120] The fruit seller fell overboard and drowned. The Chinese government was outraged and insisted that the sailor face trial before a Chinese court.[121] The captain of the Emily refused to release the sailor and insisted that the trial would occur aboard the Emily. The Chinese government immediately ordered the suspension of all U.S. trade in the Canton region. In response, the captain released the sailor to the Chinese authorities. He was executed the following day.[122]

In atypical fashion, the merchant ship Emily case involved a dispute in which both China and the U.S. had significant interests. China sought preservation of its territorial sovereignty and the integrity of it courts, and the U.S. wanted to protect its sovereignty and preserve its trading relationship with China. Typically, with conflicts between the U.S. and China, the U.S. has a fundamental interest involved, and China deems the issue of less significance. Nonetheless, the case illustrates how China has historically used Western trade interests against the West as a means to obtain a goal in China's interest.

In recent times, China's treatment of copyrights when contrasted with U.S. treatment of copyrights provides another example of how China manipulates U.S. interests to obtain a particular goal.[123] Histori-

116. *Id.*

117. *Id.*

118. Christina A. Cockburn, *Where the United States Goes the World Will Follow – Won't it?*, 21 Hous. J. Intl. L. 491, 527 (1999).

119. *See generally* Banisar & Davies, *supra* n. 115.

120. Jonathan D. Spence, *The Search for Modern China* 127 (1990) (explaining the treatment of aliens under Chinese law in the 18th century).

121. *Id.*

122. *Id.*

123. Copyright disputes in the U.S. have had significant impact on technological advancements. *See* Lawrence D. Graham, *Legal Battles That Shaped the Computer Industry*, 16, 87 (Quorum Books 1999) (citing cases including *United States v. LaMacchia*, 871 F. Supp. 535 (D.Mass. 1994), and *Whelan v. Jaslow Dental Labs., Inc.*, 609 F. Supp. 1307 (D.C.Pa. 1985), in the discussion of how the battle over copyright protections for software is one, which, along with other disputes, has defined the computer industry).

cally, copyright protection has been an important right in industrialized nations.[124] China, however, has failed to recognize copyright protections from a Western perspective.[125] This variance between the U.S. and China has resulted in disputes about whether China sufficiently protects U.S. artists' rights when it fails to restrict unauthorized reproductions. China had minimal interest in copyright protection but complied with U.S. demands to protect copyrights so that China could achieve U.S. support for its GATT accession.[126] The Chinese government made the U.S. interest in copyright protection a political issue and protected U.S. copyright when the U.S. agreed to give China support for GATT.[127]

China also manipulated one issue to achieve another purpose after the revolt in Tiananmen Square. Following Tiananmen Square, the international community reacted strongly against China.[128] The Chinese government freed two Chinese democratic leaders and allowed them to leave for the U.S. in exchange for the normalization of bilateral diplomatic relations.[129] In hopes of lessening the post-Tiananmen Square pressure from the U.S., the Chinese government also strengthened China's copyright and patent laws.[130] In effect, the Chinese government "recognized" human rights and intellectual property rights to achieve diplomatic credibility.[131]

---

124. U.S. Const. art. I, § 8, cl.8. The U.S. Constitution provides that "Congress shall have the power . . . [t]o promote the Progress of Science and useful Arts by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." *Id. See also* Hannibal Travis, *Pirates of the Information Infrastructure: Blackstonian Copyright and the First Amendment,* 15 Berkeley Tech. L. J. 777 (2000) (examining the history of English property rights as they evolved into U.S. copyright protections); Jessica Litman, *Free Speech and Electronic Commerce*, Private Censorship Conference Paper, <http://webserver.law.yale.edu/censor/litman. htm> (accessed Oct. 16, 2000) (discussing the tension between free "speech" — speech that does not cost anything — and the merchants' interests to own and regulate speech through copyright).

125. William P. Alford, *To Steal A Book Is an Elegant Offense Intellectual Property Law in Chinese Civilization* 1 (Stanford U. Press 1995) (discussing why intellectual property law has never taken hold in China and that prior to the mid-1980s most of East Asia had weak enforcement of intellectual property rights).

126. Amy S. Simpson, *Copyright Law and Software Regulations in the People's Republic of China: Have the Chinese Pirates Affected World Trade?*, 20 N.C. J. Intl. L. & Com. Reg. 575-76, 625 (1995).

127. *Id.* at 576.

128. David E. Christensen, *Breaking the Deadlock: Toward A Socialist-Confucian Concept of Human Rights for China*, 13 Mich. J. Intl. L. 469, 510-511 (1992); *see also*, Kaoru Okuizumi, *Implementing the ODA Charter: Prospects for Linking Japanese Economic Assistance and Human Rights*, 27 N.Y.U. J. Intl. L. & Pol. 367, 393 (1995).

129. *See* Christensen, *supra* n. 128, at 511.

130. Murray Scot Tanner, *The Politics of Lawmaking in China* 221 (Clarendon Press 1999) (indicating that some inside China welcome outside pressure because it breaks the administrative deadlocks).

131. *Id.*

Another example of how China used one issue to achieve another purpose occurred during negotiations between China, the U.S. and the EU for China's accession in the World Trade Organization ("WTO").[132] During the period expanding from the 1980s until the year 2000, the U.S. had an annual review of China's trade status, and China repeatedly sought membership in the WTO.[133] During the WTO talks at the beginning of the new millennium, the U.S. hesitated in its decision to vote for China's accession to the WTO. Subsequently, China announced a ruling that banned foreign investments in China's telecommunication/internet industry.[134] This was alarming news to U.S. businesses who had already invested millions into China's Internet and perceived China as a market for huge business potential.[135] The U.S. commercial interests encouraged the Clinton Administration to permanently normalize U.S. trade with China, by making China a member of WTO.[136] In effect, the Chinese government used U.S. interests in China's enormous business potential (consisting of over a billion potential consumers) to force the U.S. and the EU to make concession in the WTO negotiations in exchange for China's lifting of the investment ban.[137]

The U.S. government should not prematurely establish a Federal Data Protection Agency to define and regulate Internet privacy. The premature establishment of an agency to regulate Internet privacy could place the U.S. at a disadvantage in negotiations with China similar to the U.S. position during the WTO negotiations. If China needs the EU or the U.S. to compromise something unrelated to the Internet, then China could enact privacy laws with burdensome standards that would infringe upon U.S. business investments in Internet commerce.[138] For example, China could fail to develop or utilize online credit rules, distribution and delivery infrastructures, catalogue shopping, widespread credit card use, procedures to overcome language barriers, or encryption technology. Also, in an attempt to entice China to accept Internet privacy regulations established by the U.S. and EU, the U.S. may acquiesce to privacy intru-

132. Helene Cooper & David Rogers, *China Trade Bill Passes Final Test: Senate*, Wall St. J., A2 (Sept. 20, 2000).

133. *Id.*

134. Schwankert & Landdreth, *supra* n. 103.

135. Cooper & Rogers, *supra* n. 132.

136. *Id.*

137. Infoporn Raw Data, *China's Party Line*, Wired, 109 (Sept. 2000) (explaining that the parties eventually agreed that if China joined the WTO, then foreign investments in telecommunications would be capped at 49%).

138. World Trade Organization Ministerial Conference Second Session, *Declaration on Global Electronic Commerce* <http://www.ustr.gov/wto/geneva.shtml> (accessed Nov. 4, 2000) (noting the free flow of commerce on the Internet depends on nations enforcing commitments to telecommunication and financial services, duty-free arrangements, a lack of technical trade barriers, nondiscriminatory access for network and service providers).

sions. For example, China could curtail online communications and claim concerns about "state secrets," and the curtailment could significantly impact legitimate communications and e-commerce because "state secrets" is a broad term. What would the U.S. concede in order to persuade China to narrow its definition of "state secret" to facilitate e-commerce, and its counterpart privacy? Perhaps China and the West would agree that it would be an "invasion of privacy" for any U.S. corporation to ask a Chinese citizen, residing on the mainland, about anything "political." Would "political" questions justify privacy intrusions by the state and form the basis of a legal cause of action against the particular foreign corporation conducting online business in China? Will the U.S. agree to limit online speech to a narrowly defined concept of commercial activity and allow intrusions of individual rights and sanction any country that violates China's ban on "political" speech? Will cyberspace have a realm where speech is free, and another realm where speech is limited and the dominant concern is commerce? Will this in turn create tiers of cyberspace communications where privacy is protected in certain realms, to varying degrees, and so-called lesser tiers will exist for renegade nations and businesses failing to comport with a definition of privacy promulgated by a U.S. Federal Data Protection Agency?

The U.S. and the EU have tremendous stakes in e-commerce. It is estimated that in 1998, e-commerce business totaled $102 billion,[139] and worldwide business-to-business e-commerce is estimated to reach $2.7 trillion by 2004.[140] Both the U.S. and the EU have considerable expectations for profits from the Chinese market.[141] There is a strong possibility that, with billions of dollars at stake, commercial interests will trump strategic long-term foreign policy planning. Commercial interests in sustaining e-commerce should not be underestimated because market priorities are the decisive influences on computer related technologies.[142]

Predictably, both the U.S. and the EU would make concessions in some other areas in exchange for China's agreement to accept Western privacy standards. Will such commercial interest cause the U.S. to sacri-

139. *Internet Domain Name and Intellectual Property Rights: Hearings Before the Subcomm. on Courts and the Intellectual Property of the House Comm. on the Judiciary*, 106th Cong. (1999) <http://www.house.gov/judiciary/chas0728.htm> (accessed Nov. 4, 2000) (noting testimony of Anne Chasser, President of the International Trademark Association).

140. Rich Whiting, *E-data for a Price,* Info. Week 44, 45 (Aug. 25, 2000).

141. *Chinese Development Zone Draws Investors,* ChinaE News, People's Daily <http://www.chinae.com/ENEWS/131_39.HTM> (accessed Oct. 17, 2000) (explaining that one development zone in China, called the Fuzhou Economic Development Zone, — located in the Fujian Province — has investors from more than 20 countries including Britain, Canada, France, Germany, Italy and Japan). *See also* Ellen Bork, *Dot-Commies*, The Weekly Standard 16 (May 15, 2000) (stating that China's market has always had a seductive hold on America).

142. Frank Webster, *Theories of the Information Society* 71 (1995).

fice strategic or military interests? As we proceed into the new millennium, China has international concerns about its accession into the WTO, military development, the Spratly Islands, and Taiwan.[143] The U.S. must develop a policy for U.S.-China relations and engage in well-thought planning and negotiations lest U.S. businesses dictate, in a piecemeal fashion, U.S.-China policy. It is likely that a lack of strategic planning will cause the U.S. to concede Taiwan and other issues to China due to U.S. business pressures which will arise in response to China tightening its control over Internet privacy.[144]

VI. CONCLUSION

The increased scholarship, public rage, the sheer volume of subject matter on the Internet, debates about the role of government and the lack of clarity in U.S. privacy laws, have ushered forth a sense of urgency to develop a workable definition for online privacy. The EU model of a privacy regulator is an attractive option, which suggests the U.S. should consider the establishment of a Federal Data Protection Agency. Due to the global nature of the Internet, the U.S. should study the feasibility of a Federal Data Protection Agency, and also consider a more globally inclusive approach towards defining Internet privacy. The U.S. must adopt a "Marco-Polo-like" approach and go beyond the belief that the Western view is the only view. The West must consider the views of the East (and others) and seek a more global definition of privacy for online communications. In particular, the U.S. and the EU should remain cognizant of the fact that China has a population of more than a billion and that China will soon have more Internet users than any other country in the world. If the U.S. establishes a Federal Data Protection Agency and develops a policy for privacy in a haphazard and uncoordinated fashion[145] —solely from a Western perspective—to govern the global Internet, then the U.S. may become disadvantaged in its dealings with China or find itself embroiled in a dispute. Because China has a strong

143. Saleem, *supra* n. 97, at 532-536.

144. *Id.* Secretary of State Colin Powell acknowledged the need for an effective U.S-China policy when he stated, "But in the meantime[until increased freedom in China], we will treat China as she merits. *Id.* A strategic partner she is not, but neither is China our inevitable and implacable foe. *Id.* China is a competitor, a potential regional rival, but also a trading partner willing to cooperate in areas where our strategic interests overlap." *Id.*; *see* Senate Foreign Relations Committee, *Remarks at Confirmation Hearing* (Jan. 17, 2001), Secretary of State-Designate Colin L. Powell <http:www.state.gov/s/index.cfm?docid=443> (accessed Jan. 22, 2001).

145. Dan L. Burk, *Federalism in Cyberspace*, 28 Conn. L. Rev. 1095, 1107-134 (1996) (An analogous argument was made by Dan L. Burk, in his advocacy for Federal control, rather than state control, over the Internet based on the federal government's powers under the Due Process Clause and the dormant Commerce Clause of the U.S. Constitution).

economy and its Internet users double every month, it has become a country of investment opportunities and controversy. A recent controversy about domain registration provides an illustration of this point.

Through the authorization of the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN), Network Solutions Inc. ("NSI"), a U.S.-base domain-name registration provider, announced its plan to provide Chinese Internet user registration services for Chinese domain names ending in ".com," ".net," or ".org."[146] The Chinese government opposed this practice asserting that it was unreasonable to allow a foreign corporation to control the technical solutions on Chinese domain-name registration.[147] In theory, ICANN has the sole power to appoint registrars around the world to govern the use of Top Level Domain Names ("gTLDs").[148] The Chinese government refused to accept the rules established by ICANN, and the China Internet Network Information Center ("CNNIC") declared itself as the only body authorized to register Chinese language domain names.[149] CNNIC also established dispute resolution policies that differed from those established by ICANN.[150] The question is whether ICANN or CNNIC will control the registration of Chinese language domain names? Another question is whether other countries will follow China's position that ICANN is too Western focused and biased towards multi-national corporations?[151]

In the establishment of a Federal Data Protection Agency to regulate Internet Privacy, the U.S. should consider the questions the U.S. Department of Commerce posed for consumer protection in the global electronic marketplace. There are concerns about the protections which exist for consumers engaged in electronic commerce with foreign nations; the extent that existing laws, conventions, treaties or practices provide effective protection for consumers who engaged in electronic commerce with foreign businesses; the controlling law, courts or systems to govern transactions; the extent to which existing laws and modification of laws or systems are necessary; the impact of such modification on commerce, legal systems, and law enforcement; the ability to choose forums and contract with foreign nations; appropriate remedies and the enforcement of judgments and the minimum protections required.[152]

---

146. *See China: If ICANN, So Can We* <http://www.cnn.com/2000/ASIANNOW/business/11/20/ebiz.icann/index.html> (accessed Jan. 18, 2001).

147. *Id.*

148. *Id.*

149. *Id.*

150. See *Complete CNNIC Rules for Domain-Name Disputes*, <http://www.chinaonline.com/topstories/001110/1/C00110202.asp> (accessed Jan. 18, 2001).

151. ICANN, *supra* n. 147.

152. *U.S. Perspective on Consumer Protection in the Global Electronic Marketplace*, 63 Fed. Reg. 69, 289 (Dec. 6, 1998). The questions are taken, in part and paraphrased, from

There are indeed concerns about Internet privacy, but if the U.S. establishes a Federal Data Protection Agency to regulate privacy, the international scope and impact of such an agency must be thoroughly considered because China, despite U.S. law, will also issue regulations to govern the Internet.[153] Perhaps the essential question is how will the U.S. adjust when 1.23 billion mainland Chinese begin to use and regulate the Internet?[154]

---

those raised by the FTC when it examined the impact and viability of U.S. consumer protection practices in the global market place. *Id.*

153. *See* Timothy S. Wu, *Cyberspace Sovereignty? — The Internet and the International System*, 10 Harv. J.L. & Tech. 647, 654 (1997) (noting China has had a record of Internet regulation). *See also* Mo Zhang, *China Issues New Rules Strengthening Regulatory Structure Over Internet,* 19 No. 11 E. Asian Exec. Rep. 9 (1997); *Internet, Chinese Style: Rapid Growth, "Wild West" Atmosphere, But Will It Open Up Info Flows,* 20 No. 7 E. Asian Exec. Rep. 8 (1998); Caroline Mead & Phil Zender, *Asian Developments*, 3 No. 5 Cyberspace L. 22 (1998).

154. The question of the U.S. response to China's development is an offshoot of the one posed by noted China scholar Ross Terrill in 1978 when he essentially wondered: If 900 million Chinese succeed, how will we adjust? *See,* Ross Terrill, *The Future of China After Mao* 255 (Rigby Adelaide 1978).