Journal of Information Technology & Politics
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t792306880

Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy

Milton Mueller[ab]; Mawaki Chango[a]
[a] Syracuse University School of Information Studies, USA [b] Delft University of Technology, Netherlands

To cite this Article Mueller, Milton and Chango, Mawaki(2008) 'Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy', Journal of Information Technology & Politics, 5: 3, 303 — 325
To link to this Article: DOI: 10.1080/19331680802425503
URL: http://dx.doi.org/10.1080/19331680802425503

Disrupting Global Governance: The Internet Whois Service, ICANN, and Privacy

Milton Mueller
Mawaki Chango

ABSTRACT. The Internet's Whois service allows anyone to type a domain name into a Web interface and then receive the name and contact details of whoever has registered it. Internet Corporation for Assigned Names and Numbers (ICANN) contracts make it mandatory to provide indiscriminate public access to this information. Data protection laws in Europe and other countries conflict with this ICANN policy, yet Whois has remained in place for a decade. This article offers an explanation for this puzzling contradiction. We use the concept of a *default value* to explain how the development of a technological system can change the institutional conditions under which rights claims can be realized. We also note that the Whois story poses problems for Daniel Drezner's theory of global governance. Despite disagreement between the two great powers, the ICANN regime provides effective global governance; Drezner's theory cannot explain how the rise of a technical system could produce a global shift in privacy policy and alter the bargaining power of Great Powers.

KEYWORDS. Data protection, default value, domain name, global governance, great powers, ICANN, identity, Internet governance, jurisdiction, path dependency, personal data, policy, privacy, Whois

THE PUZZLING PERSISTENCE OF WHOIS

It has often been observed that one of the main problems with Internet protocols is that there is no identity layer (Cameron, 2006; Clark, Wroclawski, Sollins, & Braden, 2002). TCP/IP does not contain sufficient assurances about who the communicating parties are, nor does it authenticate the source, status, or

Milton Mueller is Professor at Syracuse University School of Information Studies, USA, and also XS4All Professor at the Delft University of Technology, the Netherlands. Mueller received the Ph.D. from the University of Pennsylvania in 1989. Dr. Mueller's research focuses on property rights, institutions, and global governance in communication and information industries. He is the author of the book *Ruling the Root: Internet Governance and the Taming of Cyberspace* (MIT Press, 2002). He is currently working on a book about Internet governance in the post–World Summit on the Information Society environment: *Networks and Nation-States: The Global Politics of Internet Governance*.

Mawaki Chango is a Ph.D. candidate at Syracuse University School of Information Studies. His research interests include digital identity, Internet governance, and information technologies and humanities. During his previous education in France, he earned two master's degrees: in philosophy at Lille-3 University (1995) and in political science at Panthéon-Sorbonne University, Paris-1 (1996). Subsequently, he worked with a number of international organizations, including UNESCO, coordinating programs of information and communication technology applications to development. He is a co-author of "Architecture, Infrastructure, and Broadband Civic Network Design: An Institutional View," published by the CSCW journal, and the author, among other pieces, of "Challenges to E-Government in Africa South of Sahara: Provisional Notes for a Research Agenda," published in the ACM International Conference Proceedings Series, both in 2007.

Address correspondence to: Milton Mueller, 307 Hinds Hall, Syracuse University School of Information Studies, Syracuse, NY 13244 (E-mail: mueller@syr.edu).

Journal of Information Technology & Politics, Vol. 5(3) 2008
Available online at http://www.haworthpress.com

doi:10.1080/19331680802425503

attributes of documents and other resources exchanged on the Internet. Insofar as authenticated identity is supplied by Internet technology, it comes from applications supplied at the edges, which means that they lack universality and, often, compatibility across domains. The absence of identity and identification are important concerns not only to the people directly involved in a communication; a number of third parties, from governments to copyright holders, also have an interest in monitoring or surveillance of Internet users. For various purposes—some legitimate and some abusive, some public and some private—there is widespread demand for the ability to identify who is who on the Internet.

This article examines how the Internet's Whois service has evolved into a surrogate identity system. The Whois service allows any Internet user to type a domain name into a Web interface and be immediately returned the name and contact details of whoever has registered the domain. It is used by police to bring down Web sites committing crimes; its information is harvested by spammers and marketers seeking to send their solicitations; it is used by people curious to know who is behind a Web site or e-mail address; above all, it is used by trademark and copyright attorneys to keep an eye on their brands in cyberspace.

The Whois service is defined through contracts and policies as much as by technical protocols. Its existence is based on an international regime known as the Internet Corporation for Assigned Names and Numbers (ICANN). The businesses that provide domain name registration services are required to offer a free public Whois service by the ICANN contracts that authorize them to do business.

We recount the story of Whois because it forces us to re-examine our understanding of the relationship between technological systems and global governance institutions. To understand the importance of the Whois service, one need only think of the license plate of an automobile on the road, and imagine that anyone who saw the license plate would be able to type it into a computer and be returned the name of the car owner and his or her street address, telephone number, and e-mail address. That is, what Whois does to domain name registrants. It links the vehicle for navigating the complex arena of cyberspace (domains) to a responsible individual, a location, or a jurisdiction.

Of course in the real world, access to drivers' license databases is restricted to law enforcement authorities and motor vehicle departments. It is not difficult to imagine both the benefits—and the trouble—that might be caused by free, anonymous, unrestricted public access to drivers' license databases. No doubt some additional crimes would be solved and perhaps some amazing new information services could be developed by a Google of the future. No doubt, also, incidents of road rage and stalking would be taken to new heights. The same concerns apply to Whois. In addition to facilitating accountability on the Internet, open access to registrant contact data raises privacy issues and concerns about abuse of sensitive personal data by spammers, stalkers, and identity thieves.

In Europe and other countries such as Australia and Canada, data protection laws are in obvious conflict with the Whois publication requirements of ICANN. At least since May 2000, data protection authorities outside the United States have made this conflict known to ICANN.[1] Thus, the Whois service pits the global, contractual governance model of ICANN against the territorial jurisdiction of nation-states. It has also pushed the U.S., with its emphasis on supporting intellectual property interests and its weaker norms regarding privacy protection, into an ongoing, low-level conflict with the European Union. But despite numerous ICANN task forces, Congressional hearings, and letters from data protection authorities, no major changes in access to Whois data have been made since the formulation of ICANN's first registrar accreditation contract in 1999. Indeed, within the ICANN regime, the Whois privacy issue has become synonymous with endless policy deadlock. Why, despite the numerous national and international laws that protect citizens and consumers against indiscriminate access to their personal data without their consent, has ICANN's global Whois policy remained in place?

This article focuses on the puzzling persistence of open access Whois. We believe that

solving this puzzle has important implications for understanding the global governance of the Internet, and perhaps other large-scale technological systems. At its simplest, it is a story of how the Internet governance regime of ICANN has created a new, global jurisdiction, wherein traditional rights to privacy are redefined, almost from scratch. In making this explanation, we draw upon the concept of a "default value," which we believe is a useful way to capture a specific way that technological systems can generate institutional change.

It is also a story of how technological systems are shaped by interest groups: We recount in detail how the specific policies and practices of Whois have been shaped by political demand for adding identification capabilities to the identity-deprived Internet. More fundamentally, we are interested in developing an explanation for the apparently counterintuitive fact that a new global governance regime can remain so impervious to well-established national laws and international norms, despite the absence of any formal treaty or agreement by the supposedly sovereign nations whose data protection guarantees have been compromised.

We believe that the solution to this puzzle has important implications for more general theories of global governance. Thus, we try to reconcile the facts about Whois and the ICANN regime with the new theory of global governance advanced by Daniel Drezner (2007). We show that the Whois privacy issue poses severe problems for Drezner and other theorists who view delegation by state actors as the sole source of an international regime's power. Traditional notions of delegation and agreement among states cannot explain the massive shift in privacy policy created by the implementation of a global Internet directory service. Moreover, the ICANN regime provides an example of effective global governance, despite the fact that there is no agreement on policy between the two "Great Powers" (the U.S. and the EU). The unilateral globalism of the ICANN regime thus conflicts with Drezner's assertion that Great Power agreement is needed if global governance is to be effective. On the other hand, there are elements of the story that support Drezner's view, notably the policy deadlock within ICANN that has emerged from U.S.–EU disagreement. What is missing from Drezner's account is an understanding of how the evolution of a technical system can shape the outcomes of global governance processes, due to network externalities and the switching costs caused by default values embedded in a technical system.

THEORY: DEFAULT VALUE, GLOBAL GOVERNANCE, AND THE INTERNET

A "default" is defined as a situation or condition that persists in the absence of active intervention. A definition grounded more in computer science, and thus appropriate in the context of the Internet, defines a default as "a particular setting or value for a variable that is assigned automatically by an operating system and remains in effect unless canceled or overridden by the operator."[2] Defaults tilt the playing field toward one option by giving the specified value the benefit of inertia. Those who prefer an alternative must exert effort to change it.

Most computer users are aware of the latent power of defaults. Default values can get a person to use software A over software B even when s/he would prefer to use B, because it is too much trouble to change it, or because the user lacks the requisite knowledge to do so. Default values can get users to start their Internet browser at one site over another, steering millions of eyeballs and potential revenue-generating "clicks" to one supplier instead of another.

The common debate in privacy policy over requiring users to "opt in" before they receive solicitations, or forcing them to "opt out" if they don't want them, is an argument about where the default value of privacy policies should be situated. The costs of moving away from a given default can be characterized as "switching costs," which provides a link to a robust economic literature on their important effects on industries and markets (Shapiro, 1999). If the costs of changing the default are low, and the changes do not enmesh the person making the changes in any negative network

effects, the power of the default is minimized. But by the same token, if switching costs are high, the default value can take on an extraordinary power.

We show that a Whois directory originated as a feature of the Internet when it was a small-scale, closed, scientific network. As the Internet evolved into a large-scale, public, commercial system, the Whois capability remained in place by default. The presence of an open Whois directory was then exploited by interest groups with the most to gain from a global identification capability, particularly trademark and copyright holders. When the ICANN regime was created, this interest group was able to institutionalize its access to user contact data through a system of private contracts that cemented into place an open global directory service on the Internet, despite its orthogonal relationship with national and international public laws. Once the default value was institutionalized in this manner, it became very difficult, if not impossible, to change. Our argument about defaults is, therefore, fundamentally an argument about sequence and historical process. Thus, the analysis is organized around the timeline summarized in Table 1, and further detailed in the corresponding sections below.

To some historical institutionalists, this may sound as if we are making an argument about path dependency.[3] A process is path-dependent if initial moves in one direction elicit further moves in the same direction (North, 1990). The use of this term, however, does not correspond perfectly to what we mean by default value, and it also has connotations that might act as an obstacle to an in-depth understanding of the actual phenomenon. We agree with Kay (2005) when he notes that the concept of path dependency does not provide a necessary or sufficient condition to understand or explain that which it labels: "Path dependent processes, even when identified, require theorizing" (p. 554).

TABLE 1. WHOIS Timeline, 1982–2007

1982–1990	Phase 1: WHOIS established as part of Internet
1991–1998	Phase 2: WHOIS default remains in place during transition from closed to open, public network
1999–2001	Phase 3: WHOIS institutionalized by ICANN regime
2001–2007	Phase 4: Political contention over WHOIS: identification tool vs. data protection laws and norms

This article focuses on the default value embedded in the Internet's directory system; we explain both how the default got there and what political and technical forces held it in place. In so doing, we are documenting how a particular path of institutional development got established in the first place; we are not simply asserting the generic truism that the process was in some sense path-dependent.[4] Also, our argument does not rely on the concept of increasing returns, which is strongly associated with path-dependency arguments.[5] What locked a particular institutional solution into place in this case was not an incremental amplification of feedback that widened the gap between two equally feasible alternatives over time, but the vested political and economic interests that formed around the initial situation, and the high costs associated with moving away from the default once it was already in place.[6]

Some may also believe that we are making a "code is law" argument (Lessig, 1999). But here again a resort to a popular term can obscure rather than clarify the argument. The claim that code is law is not helpful until and unless one demonstrates exactly how the configuration of the code creates barriers and costs that channel human behavior in a particular direction. Also, as Lessig himself recognizes, law, norms, and markets can supersede or override code, so one must be able to explain why the code remains in place and is not changed. Also, the idea that code is law, if it is not carefully applied, can assume intentionality where none exists. The creators of the original Whois protocol in the early 1980s had no desire to undermine privacy rights and probably had little inkling of the massive scale and scope in which their service eventually would be used. The explanation for the persistence of Whois lies in the interaction of politics, economics, and historical sequence, not in code.

The argument about default value can make a significant contribution to our understanding

of socio-technical systems on its own. Adding to its relevance, however, are its implications for Daniel Drezner's seemingly persuasive and useful explanation of global governance. Drezner (2004, 2007), like a growing number of scholars interested in global governance generally and Internet governance specifically, makes the case for a state-centric view of international phenomena. Like Goldsmith and Wu (2005), he rejects the idea that the Internet has somehow altered traditional patterns of nation-state control. Private entities in global governance, such as ICANN, are subordinate to governmental authority, in his view. He argues that ultimately states (and particularly the most powerful ones, which he refers to as Great Powers) are the only actors who manage to secure their preferences in the globalization outcomes: "Powerful states will use a range of foreign policy substitutes, such as coercion, inducements, delegation, and forum shopping across different international institutions to advance their desired preferences into desired outcomes" (Drezner, 2004, p. 478). He sees the nonstate actors, be they nongovernmental or intergovernmental organizations, as "agents of state interests" (p. 479), although they might have some independent but marginal role in setting agendas. He further identifies various forms through which those states fulfill their role:

> Great-power options include delegating regime management to nonstate actors, creating international regimes with strong enforcement capabilities, generating competing regimes to protect material interests, and tolerating the absence of effective cooperation because of divergent state preferences. Because globalization scholars fail to consider the delegation strategy as a conscious state choice, they have misinterpreted the state's role in global governance. (Drezner, 2004, p. 478)

From this basic set of assumptions, Drezner has produced an appealingly simple typology of global economic governance. There are at the moment only two Great Powers, the U.S. and the EU. When U.S. and EU interests are congruent, and the rest of the world is not adamantly opposed, we will get harmonized and effective global governance. When the EU and U.S. agree, but the rest of the world will not go along, the Great Powers will avoid universal institutions and forum shop, and we will get "club" standards. When the EU and U.S. disagree, and there is wide divergence of interest among the rest of the world, we will get "sham" standards, putative global governance principles that do not mean anything and can not be enforced. And when the EU and U.S. disagree and have clusters of allies around the world, we will get rival governance standards, as in the case of genetically modified foods.

We will show that the Whois story acts as a major anomaly for this otherwise elegant theory. Drezner's theory is useful enough that one would not want to approach this set of facts without something like it, but it clearly does not and cannot explain the facts about the Whois situation and ICANN's unique status as a global governance institution, nor does it do justice to the ability of technological systems to alter institutional arrangements. It is an empirical situation that tests the theory in the fullest sense of the word.

THE WHOIS TIMELINE

The evolution of Whois can be divided into four phases. The first phase is the origin of a directory service known as NICNAME/Whois on the small-scale, restricted, and experimental Internet of the early 1980s. In Phase 2, the Internet is opened to the public and to commerce—yet the default value, a global directory with potentially sensitive contact data, remains in place. During this phase, those with the strongest need to identify Internet users seize upon Whois for its surveillance and identification capabilities, establishing expectations about what is an appropriate level of access to user contact data and a powerful economic interest in its continued availability. Phase 3 covers the formation of the ICANN regime and the institutionalization of Whois capability in its contracts. In this phase, the Whois capability was no longer a default value, but had to be actively constructed because of the transition from a single, centralized registry to a system

with multiple, competing registrars and the addition of new top-level domain name registries. Nevertheless, the policies that were institutionalized were clearly a function of the expectations and interests established in the default stage, and could not have been successfully institutionalized had they not been established for years as a default. The last phase, running from 2001 to the present, involves ongoing political contention between forces who want to maintain and strengthen the use of Whois as an identification/surveillance tool and those who want to reform it to conform to data protection and privacy norms. Despite some change around the margins, we see that massive investments of political energy on both sides have been unable to move decisively in either direction.

Phase 1: Early Manifestation and Purpose of Whois

The Whois service was first defined in 1982 through an Internet Engineering Task Force standards document, Request for Comment (RFC) 812, superseded a few years later by RFC 954 (1985). See Table 2. Both RFCs describe the underlying query/response protocol, which can be consulted by any host computer on the network by sending a query from a client to a server. The introduction to RFC 954 (1985, p. 1) reads:

> The NICNAME/Whois Server . . . provides netwide directory service to Internet users. It is one of a series of Internet name services maintained by the DDN[7] Network Information Center (NIC) at SRI International on behalf of the Defense Communications Agency (DCA). The server is accessible across the Internet from user programs running on local hosts, and it delivers the full name, U.S. mailing address, telephone number, and network mailbox for DDN users who are registered in the NIC database.

The first RFCs make it clear that the Whois protocol was intended to make available to users a general directory of other ARPANET/Internet users. At the time, ARPANET was what we would now call an intranet that linked a few hundred computer scientists and researchers at less than a hundred geographically distributed sites. A critical fact about this directory, then, is that it was intended to serve a closed, relatively homogeneous, and—compared to today's Internet—very small group of networked computer users.[8] The early standards documents do not specify exactly what the purpose of this directory was. One can infer from context that it served a variety of purposes, and was seen as a convenience to the community of defense contractors involved in building the early Internet. Another critical fact is that for most users, participation in the directory was encouraged, but was not operationally, legally, or contractually required.[9] It may be that the request to register in the centralized Whois database was made to facilitate technical coordination, but this is not documented in the RFC, and evidence supporting this has not been found anywhere else. The RFC states only that the purpose is to provide "a directory service" (RFC 954, 1985, p. 1) to the network users.

TABLE 2. Phase 1, 1982–1990: Whois Etablished as Part of the Internet

Date/Period	Event or released material (link)	Source/Author
March 1, 1982	First specification of a standard for Whois (NICNAME) RFC 812: http://www.ietf.org/rfc/rfc0812.txt?number=812	IETF, Ken Harrenstien Vic White (NIC; SRI International)
August 1982	First specification of the Domain Name System (DNS) in RFC 819, http://www.ietf.org/rfc/rfc0819.txt?number=819	IETF, Network Working Group Zaw-Sing Su (SRI) Jon Postel (ISI)
October 1985	RFC 954 updating the Whois standard, http://www.ietf.org/rfc/rfc0954.txt?number=954	IETF, Network Working Group; K. Harrenstien, M. Stahl, and E. Feinler (SRI)

Phase 2: Internet Opened to the Public and to Commerce

While the number of host computers connected to it grew rapidly, the Internet was still a closed community of specialized users throughout the 1980s. From 1991 to 1995, a critical change occurred: The Internet was opened to commercial users and to the general public. This change was accelerated by the creation and deployment of the World Wide Web (WWW) and user-friendly Web browsers, which made the Internet usable and interesting to ordinary members of the public. The number of computers connected to the Internet exceeded 1.3 million before the end of 1992, and was somewhere between 6 and 8 million by the middle of 1995.[10] This was no longer a "community" of computer scientists and researchers, but a mass, heterogeneous public engaged in commerce and in public and personal communication. It was also an increasingly contentious and litigious public. As documented by Mueller (2002), the emergence of the WWW gave domain names economic value as locators of Web sites. Domains were now commonly registered for speculative and sometimes fraudulent activity. The economic value of domains made them a site of conflict over legal rights to names, as trademark owners and registrants negotiated new property rights boundaries around the use of domains. See Table 3.

During this tornado of change, the Whois service that was implemented between 1982 and 1985 remained in place. The user base of the Internet was no longer closed, no longer homogeneous, no longer situated within a noncommercial community, and no longer relatively small and manageable. But the technical protocol and the practices supporting a directory of Internet users remained the same. The only significant change was that the burden of supplying the Whois service shifted from defense contractor Stanford Research Institute to civilian National Science Foundation contractor Network Solutions, Inc. As the Internet moved from the small, noncommercial, and closed world of the 1980s to the open, public, and commercial world of the mid-1990s, no one made a conscious decision to retain the open-access Whois service of RFC 954; Whois was an unnoticed default value.

In this constancy in the midst of radical transformation, we find an important trigger of change in global governance arrangements. Establishing open access to user contact information as the default gave an opening to those looking to compensate for the anonymity of Internet use. In particular, trademark lawyers viewed domain names that incorporated or resembled the marks of their clients as threats to the exclusivity and value of their brand

TABLE 3. Phase 2, 1991–1998: Whois Default Remains in Place During Transition

Date/Period	Event or released material (link)	Source/Author
1991–1992	Internet opened to public; Commercial Internet eXchange founded in 1991; legislation passed in 1992 revising NSF's Acceptable Use Policy to permit public use of NSF supported networks	CIX, NSF
1992 –1993	Public release of graphical World Wide Web browsers	Mosaic, Netscape
1994	First lawsuits related to domain name—trademark conflicts*	US Courts
July 1995	Charging for domain registrations instituted by Network Solutions, Inc. NSI "Domain Dispute Resolution Policy" gives trademark owners special rights to domain names	Network Solutions, Inc. (NSI)
1996–1999	Growth of automated processes to collect zone file / Whois data from centralized NSI database	
November 1998	U.S. Commerce Department recognizes ICANN as the "NewCo" called for by the June 1998 White Paper http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm	US Commerce Department
January 1999	U.S. Commerce Department, NSI agree on usage restrictions for zone file data for .com, .net and .org	US Commerce Department, NSI

*An online academic study conducted in 1998 provides a list of the early domain name v. trademark conflicts.

names. These industrial interests created a strong demand for Internet capabilities that permitted them to monitor domain name registrations and identify the registrant. Whois records were perfectly suited to this purpose: They combined information about registered domains with the date of the registration and extensive contact information for the registrant and technical administrators. That combination enabled mark holders not only to identify what they considered infringements, but also to quickly serve legal process on the registrant. The data in the Whois record was as close as the Internet got to an identity card. Well before the creation of ICANN's contractual regime in 1999, suppliers of trademark monitoring services, such as Thomson, Inc., were systematically incorporating Whois information into their products.

The practice of using Whois information for private policing functions quickly spread to include copyright holders who wanted to be able to identify and prosecute Web sites that were distributing infringing content, and then to public law enforcement agencies tracking online fraud. Law enforcement agencies found the instant access to identification information, without any need for due process, temptingly convenient. Social science researchers interested in objective data about aspects of the Internet also joined the game.[11] With domain name registration and Web site hosting evolving into a multibillion-dollar industry, access to registration records and zone files were also being used to gain marketing data. Thus within a few years of the Internet's commercialization, the process of using Whois as a form of identification, surveillance, and data mining, often using automated scripts to gather data, had become common practice.

In its original default, Whois data and the DNS zone files were pure data "commons," accessible to anyone on the Internet. Network Solutions, Inc., the central registry that held the exclusive contract to operate the .com, .net, and .org domains, was required to make its central list of registered domains and Whois record (also known as zone file) available for legitimate use. In January 1999, however, only a few months after the U.S. government recognized ICANN, the potential for abuse of open access to this data became evident. The emergence of automated query processes directed against Network Solutions' registration and Whois systems prompted it to press the Commerce Department to tighten restrictions on the use of the data, through a Zone File Access Agreement.[12]

Phase 3: ICANN Institutionalizes Whois

From 1997–1999, the U.S. government created a new global governance regime for the Internet's domain name system (DNS). The regime was centered in a nonprofit California public benefit corporation, the Internet Corporation for Assigned Names and Numbers (ICANN). See Table 4.

The ICANN regime had three main purposes. One was to provide a formal institutional home for the coordination of the Internet's identifier system; the second was to develop a mechanism for handling domain-name–trademark conflicts; the third was to introduce competition in the supply of domain names. The latter goal, which required separating registries from registrars and thus decentralizing the maintenance of customer account records, was incompatible with the original design of Whois. Put bluntly, registrar competition broke the old, centralized Whois service. ICANN could, therefore, no longer rely on the default. In order to institutionalize the legacy capability of Whois, it had to define new contractual relationships among the parties. As ICANN's general counsel Louis Touton stated at the time, "An overall goal of the Whois provisions of the Registrar Accreditation Agreements was to help restore the InterNIC Whois service that existed in .com, .net, and .org prior to the introduction of multiple registrars."[13]

As Touton's statement indicates, the central component in the evolution of Whois policy is the Registrar Accreditation Agreement (RAA). Registrars are artifacts of ICANN's regulatory regime for the supply of domain names. They are the retail side of a contractually imposed vertical separation between wholesale registries that exclusively operate top-level domains (such as .com or .info), and multiple registrars who compete at the retail level to sell second-level

TABLE 4. Phase 3, 1999–2001: New Whois Institutionalized by ICANN Regime

Date/Period	Event or released material (link)	Source/Author
March 1999–November 1999	First ICANN Registrar Accreditation Agreement (RAA) developed http://www.icann.org/registrars/policy_statement.html http://www.icann.org/registrars/ra-agreement-12may99.htm http://www.icann.org/nsi/icann-raa-04nov99.htm	ICANN
April 30, 1999	Final Report of WIPO Internet Domain Name Process recommends that "contact details of all domain name holders should be made publicly available" http://www.wipo.int/amc/en/processes/process1/report/finalreport.html	WIPO
August 3, 2000–February 2001	Litigation related to Verio's use of automated collection of Whois and zone file data for marketing purposes, http://www.icann.org/announcements/advisory-02feb01.htm http://www.dnso.org/dnso/notes/20020122.rc01.4.html Injunction granted http://www.icann.org/registrars/register.com-verio/order-08dec00.htm	Register.com v. Verio, Inc.
May 2000	International Working Group on Data Protection in Telecommunications warns ICANN that "publication of personal data of domain name holders gives rise to data protection and privacy issues." http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm	Internationaler Datenschutz, Berlin, Germany
December 1. 2000	Whois Committee convened by ICANN to address implementation questions caused by registrar competition http://www.icann.org/committees/whois/	ICANN (VP & General Counsel)
March 6, 2001	ICANN Whois Committee recommends standardizing Whois output across registrars http://www.icann.org/committees/whois/committee-recommendations-06mar01.htm	ICANN Whois Committee
May 2001	2nd (Current) Iteration of ICANN Registrar Accreditation Agreement http://www.icann.org/registrars/ra-agreement-17may01.htm	ICANN

domain name registrations (such as aol.com or igp.info) in the top-level domains to end users. Before any company could become a registrar, it had to sign an accreditation contract with ICANN. This contract was used to impose regulations pertaining to the supply of Whois services, among many other things. Development of the RAA contract started in February 1999; the first published version of it is dated May 12, 1999, and it reached something close to its current form with the November 1999 version.[14]

In preparing the RAA, the architects of the ICANN regime openly catered to the needs of the intellectual property interests. The U.S. Commerce White Paper that set in motion the process of creating ICANN called upon the World Intellectual Property Organization (WIPO) to convene a process for making policy recommendations regarding domain names (U.S. Department of Commerce NTIA, 1998). In its Interim and Final Reports, WIPO recommended that "contact details of all domain name holders should be made publicly available" (WIPO, 1999, ¶ 74).

In the RAA and in its contracts with registries, ICANN transformed the community directory of RFC 954 into a contractual obligation. As a condition of entering the market for domain name registrations, Section F of the 1999 RAA requires all registrars to provide a free (i.e., subsidized at registrant expense) Whois service that could be queried an unlimited number of times by any Internet user.[15] The policy requires registrars to include the name and postal address as the domain name holder's personal data; the technical and administrative contacts for the SLD must provide "the name, postal address, e-mail address, voice telephone number, and (where available) fax number" (RAA, 1999, Section F, ¶ 1.h). In practice, registrants are presented with a form containing all the same contact data for the registrant, the technical contact, and the administrative contact. They are not informed that the registrant is not legally required to provide anything more than the name and postal address. A registrant who is an individual or "natural person" in legal parlance (as opposed to legal persons such as

corporations) may not have separate administrative and technical contacts, and thus must provide personal telephone and e-mail addresses. The registrar must allow any lawful uses of the registration data provided through the query-based public access. The only exception is "mass unsolicited, commercial advertising or solicitations via e-mail (spam); or . . . high volume, automated, electronic processes that apply to Registrar (or its systems)."[16]

The RAA also obligates the registrar to provide "bulk access" to Whois data. Upon payment of an annual fee capped at $10,000, registrars must make available "a complete electronic copy of the data available at least one time per week for download by third parties" (RAA 1999, Section F, ¶ 6.a). Such deals are subject to the above-mentioned restrictions on marketing uses. This part of the RAA was meant to accommodate the political demands of a growing number of trademark monitoring service providers who systematically collected Whois data and compiled it into analyses that were sold to trademark holders.

The RAA contract contains several boilerplate allusions to standard data protection principles, such as a requirement to notify end-users of what data was required and what the data would be used for,[17] and grants individual domain name registrants a nominal right to opt out of any deals for bulk access related to marketing. But the effect of these provisions is completely nullified by the basic purpose of securing a "Whois service providing free public query-based access" (RAA 1999, Section F, ¶ 1). Notifying users what purpose their data is used for becomes meaningless in the context of open, public, query-based access, which makes it possible for the data to be used by anyone for any purpose. In sum, the RAA was crafted to walk a fine line between making possible identification and surveillance for the various interest groups that relied on it, including those wanting bulk access to domain name records, while preventing the kind of wholesale and uncontrolled exploitation of a data commons that was beginning to emerge through automated processes.

In this stage, ICANN moved Whois from being a default value to an actively constructed legal obligation. Nevertheless, our argument is that ICANN's contractual regime attempted to maintain the classical Whois capability in the new situation. The institutionalization of Whois along these lines never would have been possible had it not been preceded by nearly five years of the default Whois, which created and legitimated expectations about appropriate levels of access to contact information about individuals, and also created vested interests in exploiting that access.

To fully comprehend the power and importance of the default value, we need to rely here on a counterfactual scenario. One might want to argue, in contradiction to our point, that the trademark and copyright interests are very powerful and would have succeeded in gaining access to user contact data during the institutionalization phase regardless of the prior existence of Whois and the persistence of any default value. To refute this argument, we point to the absence of any similar lookup capability outside of the domain name system. A large portion of Internet users do not have their own domain name registrations; most rely on digital identities supplied by Internet service providers or e-mail services (e.g., they navigate the Internet as goodperson@xs4all.nl or badperson@gmail.com). Most Internet users only possess usernames under domains registered by someone else, and these kinds of accounts are just as likely to be the basis of malicious use as directly registered domains.

Suppose, then, that in response to all the problems of fraud and "cybersquatting" in the early years of the Internet's existence, trademark and copyright holders and law enforcement agencies had demanded that the world's ISPs should be required to set up a globally interoperable, uniformly formatted database that allowed anyone in the world to type an ISP username such as goodperson@xs4all.nl or badperson@gmail.com into a Web interface and be returned the name and street address of the account holder.[18] What would have happened if, in the absence of a pre-existing default directory, those interested in surveillance and identification on the Internet had demanded the equivalent of a Whois capability for ISP accounts?

The strongest answer to this question is simply the absence of such a capability or anything

close to it, anywhere in the world, much less on a global basis. Yet the justification for such a capability is just as strong as, if not stronger than, the case for domain name Whois. The wider scope of such a system would allow it to access the records of the many spammers and fraudsters who use third-party ISP accounts as well as those using their own domains. It seems clear that trademark and copyright holders would not succeed in getting such a system implemented globally, or even within the U.S., no matter how strongly they wanted it. The affected businesses, the ISPs, would strenuously resist supplying unrestricted, anonymous public access to their customer lists. They would also emphasize the cost burden of creating such a globally interoperable capability, and maintain that the costs would harm the growth of the industry. ISPs would almost certainly invoke the privacy rights of their account holders, partly out of sincere concern for them and partly as a cover for their economic interest in avoiding such a scenario.[19] They would insist upon the importance of due process of law in obtaining access to the contact data, noting that only customers seriously suspected of wrongdoing should be subjected to such surveillance.

Even if the advocates of such a broader lookup scheme succeeded in overcoming the resistance of the ISPs, they would then be confronted with the incompatibility of national laws throughout the world, and the differing norms that exist in different regions. Privacy advocates and data protection authorities would subject such a proposal to intense scrutiny and oppose its implementation. Cooperation with such a system by national sovereigns would be voluntary, making it extremely unlikely that a global implementation would achieve critical mass. In short, the costs, political obstacles, and technical barriers associated with creating a Whois-like capability from scratch and across borders highlight the critical role played by the default value in shaping the approach to identity policy and data access in the ICANN regime.

Phase 4: Endless Contention

After the basic institutional framework of ICANN was put into place, the politics of Whois entered a new phase, one which we call "endless contention." The contradiction between Whois and data protection laws and norms became evident, leading to efforts to reform or alter Whois. At the same time, the interest groups that wanted Whois to become the Internet DNS's identity card became frustrated at its imperfections and pushed in the opposite direction for changes to make it more comprehensive and accurate. For the first two or three years, the advocates of strengthening Whois had the political upper hand. Sometime in late 2003, the tables turned and privacy-oriented Whois reformers gained the initiative. Nevertheless, neither side proved able to make comprehensive changes. For the next seven years, the issue would remain stuck in the default-driven equilibrium. See Table 5.

Strengthening Whois

By 2001, it was clear that DNS Whois was very useful as an identity verification mechanism on the Internet, but also that it had major limitations. The information entered into it was not authenticated or verified at the point of entry. Hence, Whois contained many inaccurate, obsolete, or deliberately misleading records. Also, the fragmentation of the supply of Whois services across competing registrars made it more difficult and costly to conduct comprehensive searches.

Another form of fragmentation was also becoming important: As the Internet spread globally, a growing number of Internet users were registering under country code top level domains (ccTLDs). ccTLD registries were not yet subject to ICANN contracts and thus could not be required to implement the Whois service. Efforts by the U.S. to rope ccTLDs into the global ICANN regime by signing contracts that reduced them to the same status as generic top level domain (gTLD) licensees were not working. Thus, nothing obligated the ccTLD operators to display the information policing agencies wanted or to integrate their Whois services with those of the generic top level domains governed by the ICANN regime.

From 2000 to 2003, the economic and political interests who supported surveillance and

TABLE 5. Phase 4, 2001–2007: Political Contention over Whois: Identification Tool vs. Data Protection Laws and Norms

Date/Period	Event or released material (link)	Source/Author
July 2001	Congressional Hearing before the Committee on the Judiciary, Subcommittee on Courts, the Internet, and Intellectual Property, on "The Whois Database: 'Privacy and Intellectual Property Issues.'" http://judiciary.house.gov/media/pdfs/printers/107th/73612.pdf	U.S. House of Representatives
Feb 2001–February 2003	First ICANN Whois Task Force (Whois TF 1) established, focusing on accuracy, postponing privacy http://www.dnso.org/clubpublic/nc-whois/Arc00/ (List archives) http://www.icann.org/gnso/whois-tf/report-19feb03.htm (Final report) http://www.icann.org/correspondence/touton-message-to-cade-30jan03.htm	ICANN/DNSO
May 2002	Congressional Hearing on "The Accuracy and Integrity of the Whois Database." http://judiciary.house.gov/media/pdfs/printers/107th/79752.pdf	U.S. House, Committee on the Judiciary, Subcommittee on Courts, the Internet, and Intellectual Property
September 2002	ICANN Whois Data Problem Reports system established http://wdprs.internic.net/	ICANN
September 2003	Congressional Hearing on "Internet Domain Name Fraud – The U.S. Government's Role in Ensuring Public Access to Accurate Whois Data." http://judiciary.house.gov/media/pdfs/printers/108th/89199.pdf	U.S. House, Committee on the Judiciary, Subcommittee on Courts, the Internet, and Intellectual Property
September 18, 2003	Second ICANN Whois Task Force (Whois TF 2), focusing on Whois-privacy issues, http://gnso.icann.org/meetings/minutes-whois-sc-18sep03.shtml	ICANN/GNSO Council
October 2003	Registrar Whois Data Reminder Policy goes into effect	ICANN
November 2005	GAO releases report Quantifying Prevalence of False Contact Information for Registered Domain Names" http://www.gao.gov/new.items/d06165.pdf	US Governmental Accountability Office
November 28, 2005	GNSO Council voted by a supermajority in favor of the 'Recommendation on a procedure for potential conflicts between Whois requirements and privacy laws' in the Final Task Force Report of the Whois Task Force	GNSO Council
March 15, 2006	Final Task Force report on the purpose of Whois and Whois contacts http://gnso.icann.org/issues/whois-privacy/tf-report-15mar06.htm	GNSO Council / Whois Task Force
April 12, 2006	GNSO Council supermajority vote for narrow, technical definition of Whois purpose "http://gnso.icann.org/meetings/minutes-gnso-12apr06.shtml	GNSO Council
May 10, 2006	ICANN Board unanimously approves GNSO Council 'Recommendation on a procedure for potential conflicts between Whois requirements and privacy laws' in the Final Task Force Report of the Whois Task Force, http://www.icann.org/minutes/minutes-10may06.htm	ICANN Board
June 22, 2006	Broad set of letters to ICANN Reacting to new purpose definition, including Article 29 Working Party http://icann.org/correspondence/	Article 29 WP, Privacy Commissioner of Canada, AIPLA, banks, etc.
July 25, 2006	Letter on the consultation on the implementation of .ca Whois look-up directory privacy policy. http://icann.org/correspondence/	CIRA
November 22, 2006	Preliminary Task Force Report on Whois Services. http://gnso.icann.org/issues/whois-privacy/prelim-tf-rpt-22nov06.htm	ICANN GNSO Council
March 12, 2007	Final task force report on Whois services, recommending OPoC proposal http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm	ICANN GNSO Council
	Letter from Article 29 Working Party reacting to the 'Draft Procedure on Potential Conflicts with Whois Requirements and National Laws' and 'Preliminary Task Force Report on Whois Services.' http://icann.org/correspondence/	Article 29 Data Protection Working Party
March 28, 2007	GAC Principles regarding gTLD Whois services http://gac.icann.org/web/home/Whois_principles.pdf	ICANN's Governmental Advisory Committee
	GNSO Council creates a new Whois Working Group to specify what Whois data elements should remain publicly available and which legitimate third parties may have access to the data that is no longer publicly available. The WG continued from April to August 2007, http://gnso.icann.org/issues/whois-privacy/whois-wg/whois-working-group-charter-16apr07.pdf	GNSO

identification initiated efforts to reform and broaden Whois to make it an even more effective identity tool. Three avenues of change were promoted. One was to create political pressure in the U.S. Congress. Another was to use bilateral free trade agreements to push other countries to upgrade their Whois to U.S. standards. A third was to push for policy changes within ICANN that would improve the accuracy of Whois and to make it more universal. In each of these cases, the fact that the ICANN regime was centered in and accountable to the U.S. government proved critical.

The U.S. Congress

Three Congressional hearings were held on the Whois issue from July 2001 to September 2003. All were sponsored by the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary in the U.S. House of Representatives. The Subcommittee—whose hearings were led, along with the chair, by ranking member Howard Berman from the Congressional District in California where the Hollywood entertainment industry is centered—is known to be dominated by trademark and copyright interests. Right from his opening statement, Berman framed the issue in terms that reflected those interests clearly:

> New [top-level] domains are now being created, and their creation will exponentially increase the number of copyright and trademark infringing, cybersquatting, and defrauding Web sites. If new problems like these are going to be created, then mechanisms for addressing those problems should also be created. One such mechanism is access to the Whois Database, and accurate information therein, so that intellectual property owners, fraud busters, and the police can track down those that are taking advantage of these newly created opportunities to break the law. Registries cannot create new problems and then not provide the means to address them. (WHOIS Database: Privacy and Intellectual Property Issues, 2001, p. 2)

Like many other policy-makers in the U.S., Berman viewed the Internet exclusively as a tool for electronic commerce and dismissed privacy concerns, comparing the Whois service with the registration system for businesses in the physical world.

Only one witness, Dr. Jason Catlett, an antispam advocate, challenged the practicality or desirability of "trying to get absolute identification from anyone who registers for a domain name" ([WHOIS Database: Privacy and Intellectual Property Issues, 2001, p. 34). He also invoked the relationship between free speech and anonymity on the Internet. In contrast, Steven Mitchell, from th Interactive Digital Software Association (IDSA), emphasized that Whois was the very tool that the U.S. Congress intended to be used to enforce the Digital Millennium Copyright Act. It was "the service that allows notice and takedown to work" (WHOIS Database, 2001, p. 5). He asserted that automated and cheap means for the registrar to detect false Whois data exist, but deplored the fact that ICANN does not require them to be deployed.

Timothy Trainer of the International Anticounterfeiting Coalition (IACC) asserted that "domain name ownership is not a right," and that "a person making a decision to have a presence on the Internet . . . should have a lowered expectation of privacy" (WHOIS Database, 2001, p. 12). Trainer's position makes unusually clear the degree to which the emergence of a new technical context invites a redefinition of basic rights. Trainer also invoked ICANN's contractual governance regime as a justification for any diminishment of privacy, noting that "with all ICANN-accredited registrars, a domain name registrant gives consent to providing public access to some information" (WHOIS Database, 2001, p. 12). Like Mitchell, Trainer asked the U.S. government to put more pressure on ICANN, and for ICANN to put more pressure on registrars to collect, maintain, and make publicly available the domain name registrant's contact information.

Privacy concerns having been largely dismissed by Congress in 2001, the 2002 hearings focused exclusively on ways to enforce an accurate and complete Whois database. This

round of testimony focused extensive criticism on the conduct of registrars, who were accused of making "the bulk of their money . . . from cybersquatters" and speculators (Accuracy and Integrity of the Whois Database, 2002, p. 21). Mr. Howard Beal, Director of the U.S. Federal Trade Commission, called upon registrars to suspend domain name registrants whose contact information is incomplete or inaccurate and to implement up-front verification procedures. The FTC Director did, however, distinguish between commercial Web sites and those that are set up "for personal or for political reasons," recognizing for the latter "legitimate privacy interests at stake" (Accuracy and Integrity of the Whois Database, 2002, p. 5).

ccTLDs and the U.S. Free Trade Agreements

If the Congressional hearings provide evidence of the strong U.S. political demand for identification via Whois and the intention to leverage the ICANN regime to deliver those goals, the Commerce Department showed that it was willing and able to take the objectives into other international forums as well. Theodore Kassinger, General Counsel of the Department of Commerce, acknowledged during the 2003 Hearings on Whois that the U.S. government started inserting into its bilateral free trade agreements (e.g., with Singapore and Chile) the adoption of an ICANN-style Whois service by the trading partner's ccTLD (Internet Domain Name Fraud—The U.S. Government's Role in Ensuring Public Access to Accurate WHOIS Data, 2003). The relevant language was crafted by the U.S. Patent and Trademark Office. It reads: "Each Party shall also ensure that its corresponding ccTLDs provide public access to a reliable and accurate Whois database of domain name registrant contact information"[20] (United States–Singapore Free Trade Agreement, Article 16.3.2). The Industry Trade Advisory Committee on Intellectual Property, commenting on the agreement with Peru which refers to "reliable and accurate" contact information for domain name registrants without specific mention of Whois, complained that this was not good enough; it preferred "that there be a direct reference to the 'Whois' database as available in the gTLDs namespace [i.e., the namespace coordinated by ICANN]. Inclusion of this direct reference would clarify the type of information this database must contain."[21]

From the standpoint of our argument, it is noteworthy that the intergovernmental trade negotiation process reflected privacy concerns more readily than the ICANN regime. In the Dominican Republic–Central American free trade agreement (DR-CAFTA), for example, the following language was added to the Whois clause: "In determining the appropriate contact information, the management of a Party's ccTLD may give due regard to the Party's laws protecting the privacy of its nationals."[22] Both ICANN and the trade negotiations were heavily influenced by U.S.-based business and intellectual property interests acting with the official support of the U.S. government. But privacy concerns fared better in the trade bilaterals because the initial negotiating positions were not burdened with the default implementation of Whois.

The 2001 Whois Task Force of ICANN

Parallel to the U.S. Congress engaging in repeated scrutiny of the Whois situation, the ICANN policy development process of the Domain Name Supporting Organization (DNSO) launched its own Task Force in February 2001 to work on the issue. The Task Force was a continuation of a committee handpicked by ICANN's management, which was formed to help define and implement the Whois provisions of the RAA in the aftermath of the *Verio v. Register.com* litigation over the harvesting of Whois information for marketing purposes.[23] ICANN and its policy-making processes were still young and lacked well-defined procedures and reporting mechanisms. The DNSO Task Force's terms of reference were broad and rather indeterminate: "To consult with the community with regard to establishing whether a review of any questions related to ICANN's Whois policy is due and if so to recommend a mechanism for such a review."[24]

Eventually AT&T's Marilyn Cade, a leader of the Business Constituency and strong advocate

of the use of Whois for surveillance and identification purposes, became the chair of the Task Force. Privacy concerns were deferred and the Task Force placed its focus on the accuracy of Whois data. The group's November 2002 Report, and the updated Final Report dated February 19, 2003, recommended that ICANN and registrars take steps to better enforce the RAA provisions requiring accurate Whois information, and included detailed instructions for processing accuracy complaints. As an outgrowth of this work, ICANN implemented its Whois data problem reports system (WDPRS), allowing inaccurate Whois data to be reported and for the domain names of persistent offenders to be discontinued.[25] Intellectual property interests remained dissatisfied with ICANN and the accuracy of Whois nevertheless, advocating that ICANN be kept on a short, one-year leash with respect to the renewal of its MoU with the Department of Commerce.[26]

In 2005, the Government Accountability Office conducted tests and found that only 5.14% of the Whois entries were patently false, and 3.65% were incomplete in one or more data fields. Only a small portion of that total, they estimated, used inaccurate data to shield illegal activity; the rest are made by registrants who try to avoid having their personal data publicly displayed for unsolicited marketing (Government Accountability Office, 2005).

A Universal Whois?

Another bold initiative to expand Whois emerged from VeriSign's 2001 agreement with the U.S. Commerce Department to divest itself of the .org top level domain and to rebid the .net top level domain. In its new contract, VeriSign agreed to allocate at least $200 million dollars for research, development, and improvements to the registry infrastructure between 2001 and 2010. ICANN specifically requested that, in terms of infrastructure improvements, priority be given to the design and development of "a Universal Whois Service that will allow public access and effective use of Whois across all Registries and all TLDs."[27] Such service would provide registrant contact information for all domain names, not just those operated by VeriSign—including country code TLDs. Work was due to commence no later than December 31, 2001, and notable progress with the implementation expected exactly a year later.

For a time, VeriSign was indeed actively involved in designing Whois-related technical proposals. Indeed, available documents show traces of a certain "uwho" service, which presumably was the company's first response to ICANN's requirements. VeriSign's work on uwho was transferred to the Internet Registry Information Service (IRIS) protocol developed by the Cross-Registry Internet Service Protocol (CRISP) Working Group inside Internet Engineering Task Force (IETF) (Newton, 2006). While IRIS was intended to supersede the "aging Nicname/Whois" protocol, the CRISP working groups have not had any impact on Whois implementation to date. Issues of technical standards are superseded by the lack of consensus on the policy issues surrounding Whois and the inertia of the current system.

To conclude, the push by trademark and copyright interests and the U.S. Commerce Department to strengthen Whois and make it a more powerful tool of identification and surveillance met with limited success during this period. Systematic measures to report inaccurate data have been implemented, and the tools to take down domains based on inaccuracy have been created. But there has been little progress on attempts to universalize Whois, and attempts to spread ICANN-type Whois policies to ccTLDs via bilateral trade agreements confronted privacy law barriers.

Privacy Gains the Upper Hand

As noted before, a European-based Working Group on Data Protection in Telecommunications issued a statement in May 2000 raising privacy concerns about the publication of individual domain name holders' information. The statement concludes with the assertion that the Whois policy implemented by ICANN-accredited registrars should be contingent upon the laws and public policies in effect in any registrar's territorial jurisdiction.

The Working Group reiterated its position in January 2003, in a letter directly addressed to

ICANN and referring back to the initial statement.[28] At this point privacy concerns had exploded among ICANN constituencies and within the Internet community, making privacy advocates a counterweight to the previous trend for an open, universal, and accurate Whois database. Another important shift occurs when the registry and registrar businesses openly broke with the intellectual property interests and began to actively support privacy-oriented reform. One reason for this was the growing abuse of registrars' and registries' Whois capability. Whois operates using an Internet "port" designed to be a vehicle for individual queries.[29] Yet by 2003, this port was being pounded by automated request programs to systematically collect a registrar's customer data. Such programs had the same effect as bulk access downloads, yet strained the registrars' infrastructure while producing no revenue. The World Summit on the Information Society, which in late 2003 concentrated world attention on ICANN and its unilateral control by the U.S. government, also contributed to the shift, as civil society activists used Whois as an example of how ICANN made global public policy.

So from early 2003 on, privacy activists inside the ICANN structure gained support and became more visible and vocal. In March 2003, the Non-Commercial User Constituency, one of the stakeholder groups that composed the ICANN's Generic Name Supporting Organization (GNSO), submitted to the GNSO Council an issues report stating that privacy concerns need to be addressed properly and that a new task force was needed to achieve this.[30] The European Article 19 Data Protection Working Party called on the ICANN community to undertake a clear definition of the purpose of Whois directories and to look for a way to achieve such purpose without making personal data public and undermining the privacy rights of individuals.[31]

Responding to these concerns, the GNSO Council reconvened a new task force on Whois and privacy. The Whois Privacy task force would continue working for four years, an astoundingly long period of time for a policy development process that, according to ICANN's bylaws, is supposed to last a few months. The Task Force's political alignments were predictable, with domain name supply industry interests (registrars and registries) and privacy advocates within the Noncommercial Users Constituency pitted against the three trademark-oriented business user constituencies. The Whois Task Force did produce three outcomes:

1. A policy that recognizes the existence of, and defines a procedure for handling, conflicts between the RAA and national privacy laws
2. A proposed definition of the purpose of Whois that is narrow and focused on technical coordination rather than law enforcement
3. A proposal for shielding some of the displayed Whois information from public access, known as the Operational Point of Contact (OPoC)

These privacy-oriented initiatives, however, produced a second surge of lobbying, pressure, and statements from what can now be called the identification party: intellectual property holders, major e-commerce multinationals, and public and private law enforcement agencies. The critical flashpoint in the debate came during a vote on the purpose of the Whois service in April 2006 by the ICANN domain name policy-making entity, the GNSO Council. The Council voted by a controlling two-thirds majority for a narrowed, technical definition of the purpose of Whois, as opposed to a broader one that defined its purpose as providing information to resolve any issues regarding domain names. The definition of purpose is important, because privacy laws and norms dictate that the collection and use of data be limited to those data elements and uses required to serve the defined purpose, and no other.[32]

The GNSO vote generated strong protest from private business associations and some prominent government representatives. Indeed, the Australian representative to the Government Advisory Committee, contradicting his country's own privacy legislation, sent a letter opposing the new definition to ICANN's GNSO Council Chair Bruce Tonkin (also an

Australian) immediately following the vote.[33] Strong behind-the-scenes pressure was placed on ICANN and the GNSO by the U.S. Commerce Department among others to reconsider its vote. Letters of protest came from entities such as the BITS Financial Service Roundtable, the International Trademark Association, the American Intellectual Property Law Association, the UK's Office for Fair Trading, the InterContinental Hotels Group, the Finance Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, the International Anti-Counterfeiting Coalition, and RSA Security.[34] While sometimes paying lip service to the need to deal with privacy concerns, these letters insisted on retaining the status quo of open access Whois. Added to this was direct pressure from the U.S. Commerce Department. In September 2006, in renewing ICANN's contractual agreement until 2009, the Department inserted a provision requiring the corporation to "enforce existing Whois policy" and maintain "timely, unrestricted and public access to accurate and complete Whois information."[35]

But the privacy party also weighed in, either to support the path taken with the GNSO's newly formulated purpose for Whois or to raise remaining issues regarding privacy. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) argued that "the automatic and mandatory publication of individual registrant contact information via the online Whois database may violate Canadian privacy law."[36] The Privacy Commissioner of Canada applauded the resolution of the GNSO Council opting for a technical, narrow definition of the purpose of Whois, and noting that the same approach had been adopted by the Canadian Internet Registration Authority (operator of the .ca top level domain).[37] In a June 2006 letter, the Article 29 Working Party pointed out that domain name registration by natural persons raises a different set of legal questions than by organizations and legal entities, and that a principle of proportionality should be observed in order to retain Whois services without mandatory publication of the personal data of nonconsenting natural individuals. The Privacy Commissioner of Belgium supported the position taken by the Article 29 Working Party as well as the position issued much earlier by the International Working Group on Data Protection in Telecommunications.

Another letter from the Article 29 Working Party (WP) commented on the OPoC proposal and the draft ICANN procedure for handling Whois conflicts with privacy law. While welcoming the proposal to take some contact information out of the public Whois service, they chided ICANN for still requiring the name of individual domain name holders to be published. Addressing the draft ICANN procedure for handling Whois conflicts with national privacy laws, the WP clarified the role of Internet registries and registrars as "data controllers" in the nomenclature of the EU Data Protection Directive. Alluding to language in the ICANN proposals referring to "potential" conflicts with national privacy laws and contemplating negotiated accommodations between registration authorities and law enforcement authorities, the WP explained that "The Article 29 WP sees, in the current situation, *actual* conflicts between current Whois practice and EU data protection and privacy laws, not just potential conflicts," and it warned ICANN that "national privacy legislation is not negotiable as such."[38]

The stalemate over Whois and privacy was further reflected in a March 2007 Statement issued by ICANN's Governmental Advisory Committee (GAC).[39] The GAC's long-awaited policy principles regarding gTLD Whois services were finalized after nearly a year of deliberations sparked by the new Whois purpose definition. These principles identified a set of legitimate activities that Whois was currently used for, which included everything from policing trademark and copyright infringement to looking up the expiry date of a domain. Due to pressure from European Union participants, however, the statement said only that the activities were legitimate and did not specifically say that open access to Whois data to pursue these activities was legitimate. The GAC statement also recognized concerns about the misuse of the public data and that ICANN policies could only be implemented within the confines of national laws. Its only recommended action was to call for further studies of the Whois issue.

Yet despite all this drama, in the end ICANN's policy development process remained stalemated, and no actual changes were made in Whois. The proposal to remove some identifying information from the public Whois did not succeed, as reform proposals got bogged down in conflict over who would be able to access the shielded information and how.[40] While privacy became widely recognized as an issue during the latter part of this phase, the presence of powerful trademark, law enforcement, and governmental interests on the opposing side prevented the emergence of a clear consensus within ICANN on systematic reform. Policy gridlock, of course, meant that the status quo stayed in place. ICANN's policy-making processes require rough consensus among all the affected stakeholder groups. The need for supermajority consent among groups with directly conflicting interests imposes near-insurmountable political costs and burdens on any attempt to move away from the default. Thus, nearly a decade after the first Registrar Accreditation Contract institutionalized Whois and more than 20 years after RFC 954, open access Whois remains in place.

CONCLUSION: IDENTITY, PRIVACY, AND GLOBAL INTERNET GOVERNANCE

Scholars from established disciplines have sometimes complained about the attention paid to Internet law and institutions, ridiculing it as akin to a field focused on the "law of the horse"[41] (Easterbrook, 1996). But this episode of Internet governance presents an unusually clear example of why political scientists and legal scholars do need to pay attention to the specifics of technological systems. The Whois story sharpens and magnifies our appreciation of how the emergence of new technological systems can generate lasting institutional change. It shows that technological change can alter the bargaining power of Great Powers in a particular sector. It shows that the process of translating existing legal rights into the terms of a new technological system is not straightforward, but involves reconstituting the rights and the laws themselves. In this reconstitution, rights can change radically or veer off in new directions. The problem is not simply that existing legal rights have to be reinterpreted in a new context. It was, in fact, very easy to apply standard data protection principles to Whois, as is proven by the early and repeated interventions of European and North American data protection authorities in the controversy. The change in the status of basic privacy rights was caused by something more profound and structural.

The Whois story is a case of path dependency; the path dependency is based not on increasing returns but on the contingent appropriation by first-movers of a pre-existing feature of the Internet that was designed in different conditions and for a different purpose. Open-access Whois was appropriated and institutionalized because it was the closest thing to an effective form of global identification that the identity-deprived Internet could provide. Thus, the world's convergence on a set of data communication protocols that included Whois altered the nature of privacy rights, altered the institutional conditions in which claims of rights can be realized, and shifted the relative political power of the actors involved.

To phrase it in a way deliberately designed to provoke realist political scientists, the Internet created a new political territory. The historical accident of the Internet's origin in the U.S. made it possible for U.S.-based actors to unilaterally establish an effective global governance regime for that territory, even as the rest of the world joined it, putting European standards at a fatal disadvantage. When it came to the data protection and privacy practices of this regime, the pre-existing default of an open access Whois directory put all the costs and burdens associated with changing the regime on privacy advocates, while allowing proponents of open access to reap the benefits of inertia and the lack of consensus on policy. The fact that the Internet originated in the U.S. made a major difference in this case. It privileged the role of U.S.-based interest groups, who can exert direct pressure on Congress and the Commerce Department; it allowed the Commerce Department to leverage its contractual authority over ICANN to rebuff challenges to the regime's

privacy policy; and of course it allowed the U.S. to establish the parameters of the international regime in the first place.

If, prior to having any knowledge of the facts, we were to apply Drezner's global governance model to this case, we would surely predict the emergence of rival standards. Indeed, Drezner and others have described how U.S.–EU conflict over privacy norms in other situations has led to a "rival-standards outcome" (Drezner, 2004, 2007; Farrell, 2003). When it comes to Whois, only one aspect of that prediction is true: the long history of indecisive contention and deadlock around Whois within ICANN. Drezner's model would be correct, were it not for the prior existence of Whois in the early Internet and its retention as the default value as the Internet became public. Because of its pre-existing status, the inability of the Great Powers to agree simply means that the default remains in place. And the default is the U.S. standard—a globally accessible, open access directory of domain name registrants and their contact information, regardless of whether they are natural or legal persons.

Drezner (2004, p. 490) has remarked that "when necessary, governments of every stripe have been willing to disrupt or sever Internet traffic in order to ensure that their ends are achieved." But this line of analysis fails to account for the degree to which the enormous economic benefits and network externalities associated with the global Internet constrain the possibility of rivalry among Great Powers. States may indeed be willing to censor a few selected Web sites here and there, but rival governments clearly are not willing to fragment the entire Internet technically by creating a different domain name system or trying to move to a different technical protocol.[42] Even if they did create such technical alternatives, they would be hard pressed to get enough private actors to migrate to it.

It is, therefore, inaccurate to understand Great Power authority so hierarchically. Drezner's theory is based on, and more applicable to, situations in which nation-states have traditional sovereign rights and must negotiate with other states to extend their standards and preferences beyond their borders. His discussion of U.S. and EU conflict over other issues, such as genetically modified foods, deals with techno-economic systems where there do not seem to be major global network externalities, and no Great Power has an advantage over the other at the outset; each one is fully in charge of lawmaking and enforcement within their territorial jurisdiction. But that assumption does not translate to the Internet or any other technology with strong global network externalities.

Another modification of Drezner's theory is suggested by the way in which government agencies outside of the U.S. have reacted to the opportunities created by the Whois default value. Many European or non-U.S. public law enforcement agencies have given tacit or active support to open access Whois, even while acknowledging that it would be illegal under their own national law. This phenomenon was most evident in the case of Australia, whose governmental representative to ICANN vigorously opposed any move away from open access Whois, despite court decisions in Australia that have denied law enforcement agencies indiscriminate access to Whois records in the .au domain (the country code top level domain for Australia). Similar situations held for law enforcement officials from Canada and the Netherlands.

This finding lends support to theorists of transgovernmentalism in international relations, who view the state as disaggregated rather than unitary and who afford mid-level officials in agencies and subunits of national governments an important role in making international policy (Raustiala, 2002; Slaughter, 2004). Clearly, these specialized agencies can take advantage of opportunities created by technological defaults or international institutions to pursue special interests, such as easier access to data relevant to transnational law enforcement. More importantly, in favoring the norms of the global regime over national law, we see a subtle yet deeper form of institutional change taking place. The new global institution not only acts as a kind of exception to territorial law, but can also subvert or undermine domestic norms and institutions.

A similar issue is raised by the role of WIPO in this case. Acting as the agent of international

trademark and copyright interests, WIPO was an early and influential advocate of institutionalizing Whois during the construction of the ICANN regime. Principal-agent theories of international institutions notwithstanding, WIPO showed virtually no interest in the privacy concerns of natural persons, despite being delegated its authority by European governments with strict data protection laws. Instead, WIPO acted as an advocate for sectoral interests, the trademark, copyright, and patent holders who make up the bulk of its epistemic community and the basis of its financial support.

Our study shows that the U.S. and EU can be poles apart on a critical policy issue, and yet the U.S. position can prevail globally, because in this case the international regime constitutes a global extension of the U.S. system. But it is important to keep in mind that the U.S. achieved this global hegemony not because of its superior state power or even because it intentionally set out to achieve a particular result. It happened because of the world's unanticipated convergence on the TCP/IP protocols, which happened to be coordinated and administered by U.S.-funded researchers and government contractors. Under the ICANN regime, Internet resources and policies created a global domain of competence within which all domain name registrars and registries are subjected to the same contractual agreements and the same policies regarding Whois and other issues. If rivalry there is, that remains at the level of the formal preferences.

NOTES

1. International Working Group on Data Protection in Telecommunications, Common Position on Privacy and Data Protection aspects of the Registration of Domain Names on the Internet adopted at the 27th meeting of the Working Group on 4–5 May 2000 in Rethymnon, Crete. http://www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm

2. *The American Heritage Dictionary of the English Language: Fourth Edition.* 2000. "Default" entry: Noun, 4a. http://www.bartleby.com/61/97/D0089700.html.

3. The authors are grateful to Hans Peter Schmitz for pointing out the resonance of this case with studies of path dependency, along with references on historical and political institutionalism literature.

4. In this way we also feel that we answer the critique whereby scholars working within the historical institutionalism framework tend "to investigate only the persistence of the victorious policy option instead of bringing out the complexity and uncertainty that characterize formative moments in the creation of policies" (Peters, Pierre, & King, 2005, p. 1277).

5. Increasing returns define "the tendency for that which is ahead to get farther ahead, for that which loses advantage to lose further advantage. They are mechanisms of positive feedback that operate—within markets, business, and industries—to reinforce that which gains success or aggravate that which suffers loss" (Arthur, 1996, p. 100).

6. As an example of the kind of switching costs that will become evident as we move into the empirical exposition, in a politically contentious environment there is a huge transaction cost difference between renewing an established contract and renegotiating a totally new and different one.

7. Defense Data Network.

8. In 1981, there were only 200 computers connected to the Internet; by 1985, that had grown to about 2,000. Internet Systems Consortium Domain Survey, http://www.isc.org/index.pl?/ops/ds/host-count-history.php

9. "DCA requests that each individual with a directory on an ARPANET or MILNET host, who is capable of passing traffic across the DoD Internet, be registered in the NIC Whois Database. MILNET TAC users must be registered in the database" (RFC 954, 1985, p. 1).

10. Supra, note 8.

11. See the work of Matthew Zook at http://www.zooknic.com for an example of creative use of zone file and Whois information in social science research.

12. ICANN's Amicus Curiae Memorandum, *Register.com, Inc. v. Verio Inc.* (22 September 2000, p. 3). As a result of these discussions, public access to the .com, .net, and .org zone files becomes subject to use restrictions set forth in a Zone File Access Agreement.

13. Letter from Louis Touton to the Committee Requesting Advice on Implementation(1 December 2000, ¶ 5), http://www.icann.org/committees/whois/touton-letter-01dec00.htm

14. Registrar Accreditation Agreement (RAA) November 1999. http://www.icann.org/nsi/icann-raa-04nov99.htm

15. At its expense, Registrar shall provide an interactive Web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e. updated at least daily) data concerning all active SLD [second-level domain] registrations sponsored by Registrar in the registry for the .com, .net, and .org TLDs. The data accessible shall consist of elements that are designated from time to time according to an ICANN-adopted policy. (RAA, 1999, Section F).

16. RAA, 1999 November, Section F, ¶ 5.

17. E.g., paragraphs 7.b, 7.e, and 7.f, plus the section R.

18. The basic technology of providing such an interface is not all that different from Whois, although uniformity across ISPs would require some standardization of data formats. But of course, that is no different from the standardization ICANN imposed on domain name registrars.

19. For example, in a 2004 U.S. Supreme Court case, U.S. telecommunication company Verizon actively fought attempts by the Recording Industry Association of America to gain access to its customer's names. See "Supreme Court Internet Privacy Decision," Washingtonpost.com. (2004, October 14). Available at http://www.washingtonpost.com/wp-dyn/articles/A29974-2004Oct13.html.

20. See the advisory opinion of the intellectual property industry to U.S. authorities: The US-Singapore Free Trade Agreement (FTA): The Intellectual Property Provisions. Report of the Industry Functional Advisory Committee on Intellectual Property Rights for Trade Policy Matters (IFAC-3). 2003 February 28, p. 7. http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Singapore_FTA/Reports/asset_upload_file273_3234.pdf. See also Roffe (2004, pp. 35–37) for an analysis of the Chile-USA Agreement.

21. The US-Peru Trade Promotion Agreement (TPA): The intellectual property provisions. Report of the U.S. government's Industry Trade Advisory Committee on Intellectual Property Rights (ITAC-15). 2006, February 1, ¶ 41. http://www.bilaterals.org/article.php3?id_article=4222.

22. Central American Free Trade Agreement, CAFTA-DR Final Text, Article 15.4.2. http://www.ustr.gov/Trade_Agreements/Regional/CAFTA/CAFTA-DR_Final_Texts/Section_Index.html.

23. Records of ICANN's .com/.net/.org Whois Committee of December 2000 are still posted at http://www.icann.org/committees/whois/ as of March 2008. Typically for ICANN at that time, the Committee included only representatives of commercial registration interests and intellectual property holders, and no civil society representatives or privacy advocates.

24. From the policy report "Accuracy and Bulk Access." Terms of Reference, ¶ 1. (30 November 2002) http://www.dnso.org/dnso/notes/20021130.NCWhoisTF-accuracy-and-bulkaccess.html.

25. Evidence of WDPRS implementation is provided by one of the yearly reports on the 2006 "Community Experiences with the InterNIC Whois Data Problem Reports System" (March 31, 2006): http://www.icann.org/announcements/wdprs-report-final-31mar06.pdf. Related to the same effort to improve accuracy, ICANN also releases a yearly report on the implementation of the Whois Data Reminder Policy (WDRP); http://www.icann.org/whois/wdrp-report-30nov06.pdf.

26. Letter of Smith and Berman, respectively (new) chairman and ranking member of the Subcommittee on courts, the Internet and intellectual property, addressed to Commerce Department in August 2003, and reproduced in the report of the September hearing.

27. Revised VeriSign .net and .org registry agreement: Appendix W. Additional Covenants of Registry Operator. Section 2, ¶ 2. Posted April 16, 2001. http://www.icann.org/tlds/agreements/verisign/registry-agmt-appw-net-org-16apr01.htm.

28. Letter from Hansjürgen Garstka to Stuart Lynn Regarding Whois Issues. (2003 January 15). http://www.icann.org/correspondence/garstka-to-lynn-15jan03.htm.

29. Port 43. In programming, a port is a "logical connection place," and in the Internet's protocol, refers to the way a client program specifies a particular server program on a computer in a network.

30. Privacy Issues Report. Prepared by Electronic Privacy Information Center on behalf of Noncommercial Users Constituency. (March 10, 2003) http://epic.org/privacy/whois/privacy_issues_report.pdf

31. Noncommercial Users Constituency of ICANN. (2005). International Data Protection Laws: Comments to ICANN from Commissioners and Organizations Regarding WHOIS and the Protection of Privacy. http://www.ncdnhc.org/policydocuments/whois-ncuc-backgrounder.pdf.

32. See GNSO Council minutes, 12 April 2006, Item 2. http://gnso.icann.org/meetings/minutes-gnso-12apr06.shtml. If, as the identification party preferred, the purpose of the Whois was to provide information to resolve "any issues related to the registration or use of a domain name," then current practices would be supported. If, on the other hand, the purpose of Whois was to "resolve, issues related to the configuration of the records associated with the domain name within a DNS nameserver," as the domain name industry and privacy party preferred, then restrictions on the data collected and restrictions on access to the data would be obligatory.

33. Note by Ashley Cross, Australia's GAC representative, sent to Bruce Tonkin as chair of the GNSO Council following the vote, and forwarded to the Council list on 13 April 2006.

34. See the correspondence to ICANN archived at its Web site: http://www.icann.org/correspondence/

35. Joint Project Agreement between the U.S. Department of Commerce and the Internet Corporation for Assigned Names and Numbers. Annex A, ¶ 5. (September 29, 2006) http://www.ntia.doc.gov/ntiahome/domainname/agreements/jpa/signedmou290906.pdf.

36. CIPPIC to ICANN. (2006, June 22, ¶ 7). ICANN correspondence page. http://icann.org/correspondence/lawson-to-cerf-22jun06.pdf.

37. Privacy Commissioner of Canada to ICANN, 12 July 2006, ICANN correspondence page.

38. Letter of March 12, 2007 (p. 4) in reaction to the 'Draft Procedure on Potential Conflicts with Whois Requirements and National Laws' and 'Preliminary Task Force Report on Whois Services.' http://icann.org/correspondence

39. Governmental Advisory Committee, GAC Policy Principles Regarding the Whois Service, 28 March, 2007.

Retrieved May 13, 2008, from http://gac.icann.org/web/home/WHOIS_principles.pdf.

40. The GNSO voted on October 31, 2007 to "Formally en[d] the Policy Development Process on gTLD Whois without making any recommendations for specific policy changes to ICANN's Board of Directors." http://gnso.icann.org/resolutions/

41. For a good summary of the debate among legal scholars about Easterbrook's article, see Murray (2007).

42. States or other actors would be willing to defect from the globally compatible DNS only if they were very confident that, in the ensuing network rivalry, the rest of the world would quickly converge on their standard rather than the incumbent one.

REFERENCES

Arthur, W. B. (1996). Increasing returns and the new world of business. *Harvard Business Review, 74*(4), 100–111.

Cameron, K., & Jones, B. (2006). *Design rationale behind identity metasystem architecture*. Retrieved July 21, 2006, from http://research.microsoft.com/~mbj/papers/Identity_Metasystem_Design_Rationale.pdf.

Clark, D., Wroclawski, J., Sollins, K., & Braden, R. (2002). Tussle in cyberspace: Defining tomorrow's Internet. *Proceedings of the 2002 SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Pittsburgh, PA, pp. 347–356.

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly, 119*(3), 477–498.

Drezner, D. W. (2007). *All politics is global: Explaining international regulatory regimes*. New Jersey: Princeton University Press.

Easterbrook, F. (1996). *Cyberspace and the law of the horse*. Retrieved February 21, 2008, from www.law.upenn.edu/fac/pwagner/law619/f2001/week15/easterbrook.pdf.

Farrell, H. (2003). Constructing the international foundations of e-commerce: The EU-US safe harbor arrangement. *International Organization, 57*(2), 277–306.

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. New York: Oxford University Press.

Government Accountability Office. (2005, November). *Internet management: Prevalence of false contact information for registered domain names.* (GAO-06–165). Washington, DC: U.S. GAO. Retrieved July 12, 2006, from http://www.gao.gov/new.items/d06165.pdf.

Kay, A. (2005). A critique of the use of path dependency in policy studies. *Public Administration, 83*(3), 553–571.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Mueller, M. (1999). Trademarks and domain names: Property rights and institutional evolution in cyberspace. In S. E. Gillett & I. Vogelsang (Eds.), *Competition, regulation and convergence: Current trends in telecommunications policy research* (pp. 51–69). Mahwah, NJ: Lawrence Erlbaum Associates.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge: MIT Press.

Murray, A. (2007). *The regulation of cyberspace: Control in the online environment*. London: Routledge-Cavendish.

National Telecommunications and Information Administration. (1998). *Management of Internet names and addresses: Statement of policy* (Federal Register, Vol. 63, No. 111, pp. 31741–31751). Washington, DC: U.S. Government Printing Office.

Newton, A. (2006). *Replacing the Whois protocol—IRIS and the IETF's CRISP working group*. Los Alamitos, CA: IEEE Computer Society Publications Office. Retrieved June 11, 2007, from http://doi.ieeecomputersociety.org/10.1109/MIC.2006.86.

North, D. (1990). *Institutions, institutional change and economic performance*. Cambridge: Cambridge University Press.

Office of the United States Trade Representative. (2003). *United States–Singapore Free Trade Agreement*. Retrieved July 9, 2008, from http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Singapore_FTA/Final_Texts/asset_upload_file708_4036.pdf.

Peters, G. B., Pierre, J., & King, D. S. (2005). The politics of path dependency: Political conflict in historical institutionalism. *The Journal of Politics, 67*(4), 1275.

Raustiala, K. (2002). The architecture of international cooperation: Transgovernmental networks and the future of international law. *Virginia Journal of International Law, 43*(1), 1–92.

Roffe, P. (2004). Bilateral agreements and a TRIPS-plus world: The Chile-USA Free Trade Agreement (TRIPS Issue Paper #4). Ottawa: Quaker International Affairs Programme. Retrieved February 11, 2008, from http://www.quno.org/geneva/pdf/economic/Issues/Bilateral-Agreements-and-TRIPS-plus-English.pdf.

Shapiro, C., & Varian, H. (1999). *Information rules: A strategic guide to the network economy*. Boston: Harvard Business School Press.

Slaughter, A. (2004). *A new world order*. Princeton, NJ: Princeton University Press.

U.S. House of Representatives. (2001). *Oversight hearing on "Whois database": Privacy and intellectual property issues*. Retrieved July 14, 2006, from http://judiciary.house.gov/Oversight.aspx?ID=168.

U.S. House of Representatives. (2002). *Oversight hearing on "accuracy and integrity of the Whois database*." Retrieved August 23, 2006, from http://judiciary.house.gov/Oversight.aspx?ID=139.

U.S. House of Representatives. (2003). *Oversight hearing on "Internet domain name fraud"—The U.S. government's role in ensuring public access to accurate Whois data.* Retrieved August 23, 2006, from http://judiciary.house.gov/Oversight.aspx?ID=58.

World Intellectual Property Organization (WIPO). (1999). *Final report of WIPO Internet domain name process.* Geneva: WIPO. Retrieved July 11, 2006, from http://www.wipo.int/amc/en/processes/process1/report/finalreport.html.