I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Five Destabilizing Trends in Internet Governance

Dr. Laura DeNardis*

TRADITIONAL CHARACTERISTICS OF INTERNET GOVERNANCE

The Internet will soon turn fifty, if one views its inception as the late 1960s milestone when the first packets were exchanged between university research sites over ARPANET. By any measure, the global Internet has been a phenomenal achievement. It has changed the way we interact, work, shop, learn, and carry out our day-to-day lives. It has spurred new industries and launched some of the world's most successful multinational companies. More than three billion people use the Internet and this will quickly grow to five billion. The majority of this new growth will be in the developing world. Every sector of the global economy—including commerce and financial transactions—is now dependent upon the Internet to function. Despite many challenges—from global disparities in access to widespread government censorship and surveillance—the network's growth and success can convey a sense of inevitability that the Internet will continue to be universal, stable, and secure.

Part of what has enabled this growth and success over time is a dependable—albeit constantly evolving—system of Internet governance, meaning the administration and coordination of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies. The Internet is and has always been governed, but there is no single system. Rather, there is layer upon layer of distinct functions, some

* Professor, American University, Senior Fellow, Centre for International Governance Innovation (CIGI).

carried out by the private sector, some by new global institutions, and some by governments. The Internet governance ecosystem can generally be divided into six functions:[1]

1. The administration of critical Internet resources such as names and numbers;

2. The establishment of Internet technical standards (e.g. TCP/IP, HTTP);

3. Access and interconnection coordination;

4. Cybersecurity governance;

5. The policy role of private information intermediaries; and

6. Architecture-based intellectual property rights enforcement.

The Internet requires a great deal of technical and administrative coordination. For example, the unique domain names and numbers (Internet addresses) of cyberspace, as well as the Domain Name System that serves, to some degree, as the Internet's phone book for these unique identifiers, are administered and managed by a variety of entities. These entities include the Internet Corporation for Assigned Names and Numbers (ICANN), private domain name registrars that sell domain name registrations, Internet registries that manage how names and numbers are mapped in a given top-level domain (TLD), and also the United States Commerce Department, which has retained, as of this writing, its historic coordinating role in regard to Internet names and numbers.

Someone also has to establish the technical standards that enable technologies made by different companies to seamlessly exchange information; the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and dozens of other standard-setting organizations have traditionally carried out much of this activity. The work of these relatively new global institutions is largely done by technical experts, who primarily work for private technology companies. In the area of interconnection, telecommunication

[1] LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE (2014).

companies enact private contractual peering and transit agreements for how their networks conjoin bilaterally or at Internet Exchange Points (IXPs) to collectively form the global Internet. Private companies, like Facebook and Google, also directly enact public policy through their terms of service agreements and intermediation policies in regard to privacy, free speech, intellectual rights enforcement, cyberbullying, and other areas that directly affect individual civil liberties. Another critical area of Internet oversight is cybersecurity governance, which is carried out by a combination of public and private institutions.

Across all these areas, governments make laws about cybercrime, identity theft, online privacy, the protection of children online, global online trade, intellectual property, and a host of other national, regional, and international policies related to digital information policy. As this brief list conveys, these various tasks are carried out by a combination of private companies, new global institutions formed to perform specific oversight functions; national laws and policies; and international agreements. A unique feature of Internet governance is that it is carried out not only in regulatory and oversight functions, but also in the actual design and implementation of technology and in the business models that monetize this technology.

These various control points are not merely technical decision points, but also political points of control that affect innovation policy and determine human rights—such as freedom of expression and privacy. How Web standards are designed determines online accessibility for the disabled; social media terms of service make decisions about individual privacy; access regulations, such as net neutrality rulings, make decisions about what counts as a so-called free and open Internet; and the administration of domain names involves resolving trademark disputes and conflicts related to global competition and innovation. Collectively, Internet governance involves a combination of privatized and public oversight, the rise of new transnational organizations, and highly specialized technical design and coordination. This global ecosystem of coordination has kept the Internet operational, expansive, relatively secure, and innovative.

The Internet itself has changed constantly over the past fifty years: most obviously with the rise of the Web in the 1990s, the popularization of social media in the 2000s, the global surge in mobile services and smartphones, and the emergence of the "Internet of Things" in which more things—cars, devices, appliances, wearable technology, and industrial sensors—are connected to the Internet than people. It can be argued that the Internet has also stayed the same in that its underlying technical architecture and administration have

embodied a specific set of aspirational principles shaping the design and administration of the network and, in turn, contributed to the growth and generative qualities of cyberspace. The *Internet Society* (ISOC) has referred to these principles as "Internet invariants," suggesting "it's important to understand what is actually important and unchanging about the Internet—the invariants that have been true to date."[2] Some of these invariant principles suggested by ISOC include: *global reach*, the ability of any endpoint to address any other endpoint regardless of location; *general purpose*, the capacity to support a wide range of applications and services; *permission-less innovation*, a condition in which anyone can choose to establish a new service or application that connects over the Internet without having to seek consent from a gatekeeper; *accessibility*, the capability for anyone to get online as a user or producer; and *interoperability* among diverse networks. Some of the general governance principles ISOC mentions include *collaboration among stakeholders*, *mutual agreement*, and there being "*no permanent favorites*" so that innovation can continuously occur. As distinguished Internet engineer Leslie Daigle has said, "[t]hese conditions need to be maintained as the Internet continues to evolve. A network that does not have these characteristics is a lesser thing than the Internet as it has been experienced to date."[3]

These design and coordination traditions, while imperfect and always involving tensions between both competing stakeholders and competing values, have contributed to a relatively stable system of governance, as well as constituting the technical norm of open platforms upon which content can flow and nearly any service connect. This universality and interoperability have contributed to the trust necessary for investment, industry adoption, and social reliance on the network.

Unfortunately, this stability and potential for growth cannot be taken for granted. Several developments in both the perception and substance of how the Internet is governed directly contravene many of these traditions. These potentially destabilizing conditions in Internet governance include:

---

[2] *Internet Invariants: What Really Matters*, INTERNET SOCIETY, Feb. 3, 2012, http://www.internetsociety.org/internet-invariants-what-really-matters.

[3] Leslie Daigle, *On the Nature of the Internet*, GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES NO. 7, Mar. 2015, https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf.

1. A measurable loss of trust in cyberspace due to high-profile cybersecurity breaches and increasing public awareness of government surveillance;

2. An emerging phenomenon of governments co-opting the Domain Name System for outside purposes such as censorship, surveillance, and intellectual property rights enforcement;

3. Uncertainty about the outcome of the United States transitioning its historic oversight of certain coordinating functions of Internet names and numbers;

4. Tangible attempts to overlay national borders on the global Internet, such as through infrastructure restrictions and data localization; and

5. A resurgence in proprietary and differentiated approaches designed to prioritize certain business models, services, and content over others.

This essay elucidates these structural changes in the Internet governance ecosystem and suggests how they require global resolution to forestall negative implications for the future of innovation, individual rights, and the stable constitution of technical infrastructure in the Internet's next decades.

DESTABILIZING FACTOR #1: A LOSS OF TRUST IN CYBERSPACE

Even while there is growing societal dependence on the Internet, there is a loss of trust in this very system. This concern stems from several phenomena. One is increasing public awareness of government surveillance online. A 2014 global poll of more than 23,000 Internet users in twenty-four countries found that two thirds of users were more concerned about digital privacy than they had been in the prior year (see Figure 1).[4] This poll was taken in the year following U.S. intelligence contractor Edward Snowden's disclosures about the expansiveness of NSA surveillance practices online.

---

[4] Centre for International Governance Innovation & Ipsos, *CIGI-Ipsos Global Survey on Internet Security and Trust*, CIGI, https://www.cigionline.org/internet-survey (reached 23,376 Internet users in twenty-four countries, and was carried out between October 7, 2014 and November 12, 2014).

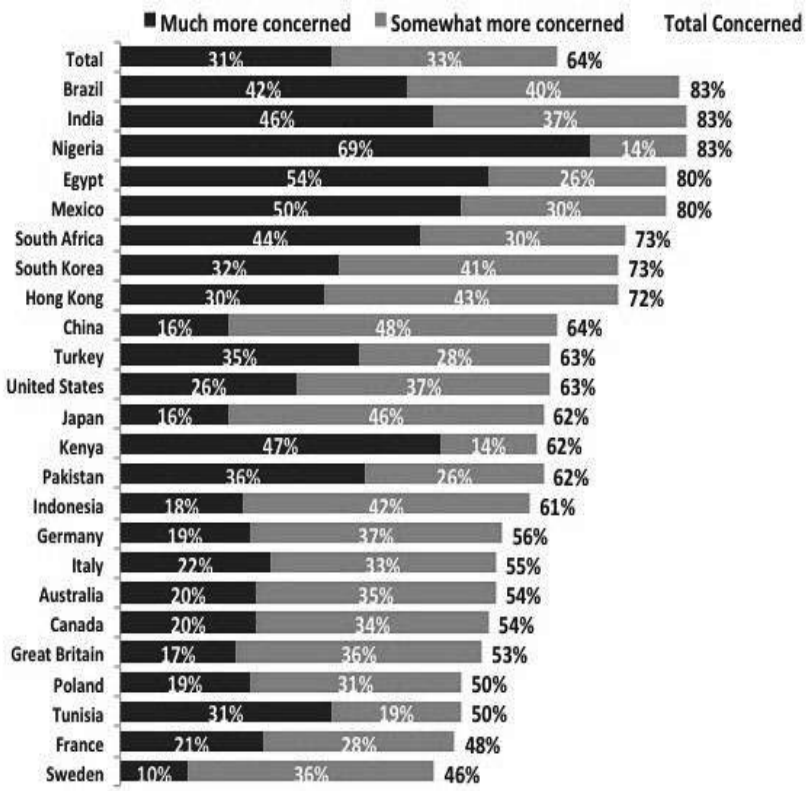

Figure 1. CIGI-Ipsos Global Survey on Internet Security and Trust

A separate United States-only survey conducted by Pew Research Center sought to assess the ways American users changed their online behavior, among those aware of government surveillance programs. The survey found that twenty-five percent of Americans altered their behavior in at least one way, such as how they used search engines, email, cell phones, or text messaging.[5] Publicity over government surveillance has also unmasked the essential role of the private sector in making surveillance possible. The underlying business models that support search engines, email, and other online services are based on online advertising revenue. The public benefits by using free

[5] *See* Lee Rainie & Mary Madden, How People Are Changing Their Own Behavior, Pew Research Survey, Mar. 16, 2015, http://www.pewinternet.org/2015/03/16/how-people-are-changing-their-own-behavior/#some-americans-are-adopting-specific-online-strategies-to-hide-their-information-from-the-government.

platforms—search engines, social media, email, and information aggregation sites—but this industry is funded by the collection and monetization of personal data through systems of highly customized online advertising. The intermediation and collection of data are what make government surveillance possible.

Some loss of trust has also arisen from high-profile cybersecurity breaches, such as the massive data breach experienced by U.S. retailing giant Target,[7] or the Sony Pictures attack.[8] During the 2013 holiday season, hackers compromised department store Target's computer systems and stole the credit card and personal information of forty million customers, including addresses of seventy million customers. In response to a class action lawsuit, Target offered to pay settlements totaling $10 million. The data breach not only led to a loss in customer confidence and the resignation of Chief Executive Gregg Steinhafel, but also raised questions about the role of private companies in protecting consumer data. Target responded to these concerns by committing to introducing the Chief Information Security Officer position and providing additional security training for employees.[8] Shortly after the Target data breach, home improvement retailer Home Depot disclosed that hackers stole the credit card information of fifty-six million customers after infiltrating the retailer's payment systems with malware.[9] In addition to gaining access to this vast trove of credit card data, the hackers also stole email addresses of fifty-three million customers.[10] While absconding with financial information like credit card numbers is frequently the

---

[6] Target Press Release, Target Provides Update on Data Breach and Financial Performance (Jan. 10, 2014), http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.

[7] Rachel Emma Silverman & Ben Fritz, *Data Breach Sets off Upheaval at Sony Pictures*, WALL ST. J., Dec. 4, 2014. http://www.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799.

[8] Sara Halzack, *Target Data Breach Victims Could Get up to $10,000 Each from Court Settlement*, WASH. POST, Mar. 19, 2015, http://www.washingtonpost.com/news/business/wp/2015/03/19/target-data-breach-victims-could-get-up-10000-each-from-court-settlement/.

[9] Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, WALL ST. J., Sept. 18, 2014, http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[10] Home Depot Press Release, The Home Depot Reports Findings in Payment Data Breach Investigation Confirms Prior Guidance (Nov. 6, 2014), https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

purpose of data breaches, incidents involving the infiltration of insurance companies' networks raise concerns over the targeting of medical data and other sensitive personal information. In the most extensive breach of medical records, as of this writing, hackers compromised medical data, Social Security numbers, and other sensitive information of eleven million customers of health insurer Premera Blue Cross.[11]

Those who view governments as a source of consumer data protection in these private industries have to be reminded that personal data breaches are a commensurate problem in the public sector. In addition to exposing sensitive personal information, government data breaches can also constitute a threat to national security when classified, as well as personal, information is accessed.

After breaching the networks of the Office of Personnel Management (OPM), a group of hackers, believed to be based in China, gained access to personal information and Social Security numbers of an estimated twenty-two million current and former U.S. federal employees.[12] After first reports on the breach of employment data, government representatives also cautioned that hackers might have had access to sensitive security clearance data.[13] Another data breach that was intrinsically tied to national security and international relations revolved around the infamous cyberattack on Sony Pictures that unfolded prior to the release of *The Interview*, a comedy about two journalists tasked with assassinating North Korean leader Kim Jong-Un. After a wave of cyberattacks against Sony, a group identifying as "Guardians of Peace" claimed responsibility and requested the cancellation of the movie's release.[14] While the data breach primarily garnered attention for the leak of controversial email exchanges between Sony executives and the leak of unreleased

---

[11] Reuters, *Premera Blue Cross Says Data Breach Exposed Medical Data*, N.Y. TIMES, Mar. 17, 2015, http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html.

[12] Brigid Bowman, *More than 22 Million Affected by OPM Hack*, ROLL CALL (July 9, 2015, 4:04 PM), http://blogs.rollcall.com/hill-blotter/more-than-25-million-affected-by-opm-hack/?dcz=.

[13] Associated Press, Second Hack of Federal Records Hit Intelligence and Military Personnel, The Guardian, June 12, 2015, http://www.theguardian.com/technology/2015/jun/12/hacking-personnel-data-4-million-federal-workers.

[14] Arik Hesseldahl, *Sony Hackers Offer to Withhold Stolen Data from Promised Leak*, RE/CODE, Dec. 14, 2014, http://recode.net/2014/12/14/sony-hackers-offer-to-withhold-stolen-data-from-promised-leak/.

movies, the hackers also gained access to a wide range of personal information—including the Social Security numbers of 47,000 Sony employees.[15] While North Korea denied any involvement in the cyberattack, the controversy over *The Interview* shows how data breaches are used as political weapons, raising questions not only about free expression and international relations, but also about the stability and security of Internet infrastructure. This combination of government surveillance, private data collection, and human security complexities has, by extension, resulted in the measurable loss of trust in the governments, private companies, and institutions that run the Internet.

[15] Saba Hamedy & Meg James, *Sony Hit with Lawsuit by Former Employees over Email Leaks*, L.A. TIMES, Dec. 16, 2014, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-class-action-lawsuit-employees-20141215-story.html.

Company/Institution Attacked	Number of Records Breached	Additional Information
Target	Credit card information of 40 million customers, personal information of 70 million customers	Target offered to pay $10 million to settle data breach, committed to new Chief Information Security Officer position
Home Depot	Credit card information of 56 million customers, email addresses of 53 million	Malware went unnoticed for several months
Premera Blue Cross	Medical and financial data of 11 million customers	Largest publicly-known breach of medical information to date
United States Federal government	Personnel information and social security numbers of an estimated 22 million current and former federal employees and associates	Chinese hackers suspected to be behind breach of OPM network; separate attack may have compromised sensitive security clearance information
Sony	Vast amount of data, including email exchanges and unreleased movies; personal information, including Social Security numbers of 47,000 employees	Hackers claiming responsibility pressured Sony to halt release of *The Interview*. After movie theaters refused to show the movie, the movie's original release date was cancelled and it was later released in limited theaters

DESTABILIZING FACTOR #2: THE DOMAIN NAME SYSTEM AS A PROXY FOR BROADER GEOPOLITICAL CONFLICT

A second destabilizing trend is the co-opting of infrastructures of Internet governance, especially the Domain Name System, for purposes completely outside of their originally constructed technical and policy functions.[16] Most infamously, the Egyptian government turned to private interconnection and access systems to cut off Internet and phone service to its citizens. Denial of service and other cybersecurity attacks are increasingly used by governments to disrupt alternative media and dissident voices, and by hackers as a political statement against governments.[17] Law enforcement and large media content companies are turning to infrastructures of Internet governance to enforce intellectual property rights through so-called "three strikes laws" that cut off Internet access to a household if repeated infringement occurs.[18] These cases raise concerns about free expression and economic liberty, as well as collateral damage to the Internet itself.

The co-opting of the Internet's Domain Name System (DNS) is perhaps the clearest example of this turn to infrastructures of Internet governance for content control and for carrying out a variety of external objectives. The DNS is a massive global system that translates Internet names (e.g., cnn.com) into numbers (binary IP addresses) so that users can locate online resources.[19] To provide a sense of a scale, the number of such queries resolved per day measures in the hundreds of billions range. Unique binary Internet addresses identify the virtual location of devices connecting to the Internet, whether assigned permanently or temporarily for a session. Instead of typing in a long series of 0s and 1s, Internet users type a name, such as www.wikipedia.org, and then the DNS translates between the name humans use and the numbers digital devices use to locate a virtual

---

[16] Laura DeNardis, *Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance*, 15 J. OF INFO. COMM. AND SOC'Y 720, 720-38 (2012) (referred to as "the turn to infrastructure" in Internet governance).

[17] John Palfrey, Ethan Zuckerman, Hall Roberts, Jillian York & Ryan McGrady, *2010 Report on Distributed Denial of Service (DDoS) Attacks*, BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY, Dec. 20, 2010, http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Rights.

[18] *See, e.g.*, Joe Karaganis, ed., *Media Piracy in Emerging Economies*, SOCIAL SCIENCE RESEARCH COUNCIL, Mar. 2011, http://piracy.americanassembly.org/wp-content/uploads/2011/06/MPEE-PDF-1.0.4.pdf.

[19] *See, e.g.*, Paul Mockapetris, Domain Names – Concepts and Facilities, RFC 1034, Nov. 1987; and Domain Names - Implementation and Specification, RFC 1035, Nov. 1987.

location online. This system does not actually move information from point A to point B. It serves as a directory explaining where to find something. Hence, the DNS is sometimes referred to as the Internet's phone book.

The DNS is necessary for almost every instance of communication over the Internet, and because of its hierarchical design, it creates a chokepoint that can be used, in effect, to block access to certain content and services, or to monitor what information is being sought online. As such, it has been recognized as a site of economic and political power, having no connection to keeping the Internet operational.

Most prominently, the DNS has emerged as a new tool for blocking access to websites that infringe intellectual property rights, such as selling counterfeit pharmaceutical or luxury products or illegally sharing pirated music and movies. These "domain name seizures" can be accomplished by asking the Internet registry operating each top-level domain (e.g., .com) to remove the data from the authoritative name server or map the domain name to a different server, such as one with a law enforcement message.[20] These seizures have long been ordered by the U.S. Immigration and Customs Enforcement (ICE) agency of the Department of Homeland Security.[21]

There has been tremendous concern in the Internet's technical community over how tampering with the DNS, particularly using local redirection techniques, alters the universality and stability of the DNS. This concern, among others, was part of the online blackout and boycott over the introduction of legislative bills in the United States—the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA)—and how proposed approaches would affect how the Internet works.

The same exact techniques of co-opting the DNS can be used for censorship and any type of content blocking. Cyberattacks—called DNS injection techniques—carry out identity theft and cybercrimes by redirecting queries to a counterfeit site designed to appear legitimate. In all of these cases, the DNS is being co-opted and, in some cases

---

[20] *Advisory Impacts of Content Blocking via the Domain Name System*, SECURITY AND STABILITY ADVISORY COMMITTEE (Oct. 9 2012), https://www.icann.org/en/system/files/files/sac-056-en.pdf (information about the practice and technical implications of domain name seizures).

[21] *Operation in our Sites*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT AGENCY (May 22, 2014), http://www.ice.gov/factsheets/ipr-in-our-sites (information about the practice of domain name seizures).

altered, for various political or economic objectives with no connection to its original function; this raises questions for the future trust and stability in these infrastructures of Internet governance.

DESTABILIZING FACTOR #3: UNCERTAINTY OVER THE TRANSITION OF U.S. OVERSIGHT

The recognition of infrastructure as a means to advance various externalities also raises the stakes over the question of who should control Internet governance and architecture, which leads to the third area of Internet governance destabilization: uncertainty over the role of the U.S. government in Internet oversight. While there is no single system of Internet governance, there is one fairly centralized oversight role: the administration of Internet names and numbers. Each domain name used to virtually locate information, such as american.edu, and each associated binary number that digital devices use to route to this information, must be globally unique. This technical requirement for global uniqueness has necessitated some centralized coordination. The tasks once performed by a single individual are now performed through a global system of institutions.[22] At the helm is ICANN, but various responsibilities are carried out by private companies and global not-for-profit institutions, such as registries that allocate numbers and registrars that assign names. At the heart of this system is the U.S. government because it holds the contract with ICANN, and because the U.S. authorizes changes to the Internet's root zone file, which is the authoritative mapping of top-level domains like .com, .uk, .edu, etc. onto their associated numbers.[23]

A 1998 Memorandum of Understanding between the U.S. Department of Commerce and ICANN commenced the process of internationalizing and privatizing names and numbers coordination,

---

[22] *See* Vinton Cerf, *I Remember IANA*, RFC 2468, Oct. 1998, http://www.rfc-editor.org/rfc/rfc2468.txt (Internet name and number assignment was originally done by respected Internet engineer Jon Postel working at Stanford Research Institute in a function that would eventually be called the Internet Assigned Numbers Authority (IANA); RFC 2468 discusses personal details of Postel's role.).

[23] A detailed description of how Internet names and numbers are administered is available in Laura DeNardis, *The Global War for Internet Governance*, ch. 2, *Controlling Internet Resources*, Yale University Press 2014.

while also retaining accountability to the U.S. government.[24] The most contentious, long-term, international concern has been the authority of the Commerce Department to approve changes to the root zone file. Since 1998, the American position has continuously asserted that internationalization and privatization would continue, although U.S. authority via the contractual arrangement with ICANN and authorization of root zone file changes have continued. Volumes of scholarship have addressed the long history of global tensions over American oversight of names and numbers.[25]

The U.S. contractual relationship with ICANN and, especially, oversight of changes to the root zone file, long predate Snowden surveillance disclosures, WikiLeaks controversies, Facebook privacy concerns (and Facebook itself), Internet boycotts over SOPA and PIPA, the Stuxnet worm, and many other high-profile Internet governance sagas. However, these broader controversies have served to heighten attention to the unique role of the United States government in overseeing Internet names and numbers. In the immediate aftermath of the mass government surveillance disclosures, the already extant international pressure to internationalize control of names and numbers escalated significantly, such as through a Brazilian-hosted global conference known as "NETMundial: The Global Multistakeholder Meeting on the Future of Internet Governance," at which the U.S. oversight of names and numbers was the primary focus of deliberations.[26]

In March of 2014, just prior to the NETMundial gathering, the National Telecommunications and Information Administration (NTIA) of the Commerce Department announced that the United States would transition oversight to the "global multi-stakeholder

---

[24] Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers (Nov. 25, 1998), https://www.icann.org/resources/unthemed-pages/icann-mou-1998-11-25-en.

[25] *See*, *e.g.*, MILTON MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE (2002); JOHN MATHIASON, INTERNET GOVERNANCE: THE NEW FRONTIER OF GLOBAL INSTITUTIONS (2008); LEE BYGRAVE & JON BING, INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS (2009).

[26] *See* NETmundial Multistakeholder Statement, NETMUNDIAL (Apr. 24, 2014), http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

community" by 2015, under certain conditions.[26] The announcement was met with a great deal of international enthusiasm, but was politicized in the United States with some calling the transition "Obama's Internet surrender."[27] The deadline for the transition was later extended to the fall of 2016, with the specifics of the transition not yet determined.

This is both a symbolic and a real power struggle. If the transition fails to occur smoothly, this could result in political reactions that assert national sovereignty, but are detrimental to the universal characteristics of the Internet, such as the introduction of alternative Internet roots or greater government efforts to mandate the localization of infrastructure and data within borders—described next.

DESTABILIZING FACTOR #4: ATTEMPTS TO OVERLAY NATIONAL BORDERS ON THE GLOBAL INTERNET

The Internet began as an American network but has grown into an international network of networks available on every continent and, to some extent, in every country. Of course, the Internet is not universal in the sense that very real barriers of access, culture, language, and censorship exist. It is universal, however, from the technical design standpoint of having the capacity and potentiality to connect to anywhere in the world regardless of location, types of access, devices used, or applications available. In part, this ability to connect from anywhere has provided network design flexibility for technology companies. For example, customer service centers, DNS services, and enormous server farms may be geographically situated in entirely different locations. Site location decisions can be made based on market conditions, labor availability, or technical expediency. Government regulations in each respective region have always applied and created the parameters for regulating content, access, and many other areas such as antitrust, computer fraud and abuse, and conditions for competition.

---

[26] *NTIA Announces Internet to Transition Key Internet Domain Name Functions*, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (Mar. 14, 2014), http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

[27] *See, e.g.*, L. Gordon Crovitz, Commentary, *America's Internet Surrender*, WALL ST. J., Mar. 18, 2014. http://www.wsj.com/articles/SB10001424052702303563304579447362610955656.

A significant structural shift in the role of governments in altering Internet infrastructure involves attempts to directly regulate how private companies implement infrastructure and where this infrastructure is located. For example, there are tangible political movements to localize or fragment the Internet by creating national borders around technologies. Immediately after NSA surveillance disclosures, political reactions ranged from statements about wanting to route around the United States to avoid switching traffic through the many dominant Internet exchange points in the US to creating quite walled-off Internet services that simply do not interconnect to U.S. users, services, and networks.

The most specific of these proposals involve "data localization" requirements. Data localization is a general term for a range of specific prohibitions and requirements, such as mandating that content intermediaries store customer data within the country in which the customer resides, restrictions on when or how data is able to "cross borders," taxes on data exports, requirements for consumer consent, and rules about storing duplicate or backup data locally. Data localization laws already exist in many countries and others are forthcoming.[28] For example, a Russian law requiring companies to store the data of Russian citizens within the Russian border took effect in late 2015.

The CIGI-Ipsos survey on Global Internet Security and Trust polled approximately 23,000 users and found that Internet users around the world somewhat favor this type of data localization.[29] Yet, from an engineering, innovation, and civil liberties perspective, data localization creates challenges. Technology companies, whether social media providers, search engines, information aggregators, or other intermediaries, faced with data localization requirements are forced to retool networks. New entrants would not be able to compete globally because of the investment costs of locating infrastructure physically within each potential market.

The effects of such regulation extend far beyond the tech industry. A McKinsey & Company survey of chief executives in the financial services sector revealed the concern regarding such regulation, with impacts ranging from increased organizational complexity to

---

[28] Anupam Chander & Uyen Le, *Data Nationalism*, 64 EMORY L. J., 677, 680 (2015).

[29] Centre for International Governance Innovation & IPSOS, *supra* note 4.

constraints on efficiency due to having to locate employees and infrastructure in local markets.[30]

While creating inefficiencies, managerial and technical complexities, and increased costs for large global businesses, the data localization requirements would be even more onerous in creating financial barriers to small global entrepreneurs and new entrants in local markets. Although data storage could be outsourced to cloud computing intermediaries with a presence in these various markets, the idea of investing in local infrastructure (e.g., servers, people, and networks) in every potential market is an intractable barrier to new business and innovation, and a violation of the principle of "no permanent favorites."

DESTABILIZING FACTOR #5: A RESURGENCE OF PROPRIETARY AND CONTENT-DISCRIMINATORY APPROACHES

Internet innovation and growth are, in part, attributable to open standards, the technical specifications that are freely published, accessible to anyone, and able to provide assurances that new products based on the standard will be interoperable with other products and devices—regardless of location, manufacturer, or application used. In *The Future of the Internet and How to Stop It*, Jonathan Zittrain warned about a shift away from generative technical architectures to closed and proprietary approaches that enable gatekeepers to control what information can be accessed, rather than providing access to the universal Internet.[31] A relatively new trend supporting his thesis is the rise of "zero-rating" services that provide either economic or technical prioritization for some services over others.

Zero-rating services, often collaborations between mobile telecommunication providers and content intermediaries, provide free ("zero-rated") or very low cost access to selected sites. In other words, access to these preferred sites does not count against a subscriber's data caps or billing arrangements. Facebook's Internet.org initiative attracted international attention to zero-rating services. The effort was

---

[30] James Kaplan & Kayvaun Rowshankish, *Addressing the Impact of Data Location Regulation in Financial Services*, GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES NO. 14, May 2015, https://our internet-files.s3.amazonaws.com/publications/no14_web.pdf.

[31] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2009).

a co-operation between Facebook, service providers like Ericsson and Samsung, non-profit organizations, and local groups seeking to increase Internet connectivity in developing nations.[32] Google[33] and Twitter[34] have similarly partnered with mobile providers in select countries to provide users with free access to pages within the Google ecosystem and Twitter, respectively.

The stated objective of these services is to provide affordable access to information for users in the developing world for which access speeds or mobile subscription costs create barriers. These approaches, however, also raise a net neutrality-type concern in that they prioritize free access to select sites and services, and also create a gatekeeping portal, as opposed to equal access to information regardless of the content origination or intermediating company. Such zero-rating initiatives may not even be permissible to operate in the United States because of the potential impact of the still new open Internet rules.

Not surprisingly, zero-rating initiatives have come under criticism for creating a fragmented Internet rather than one that provides equal access to information.[35] Zero-rating initiatives also raise concerns over market barriers for local content providers and developers, and even the creation of potential control points for censorship and surveillance.[36] Debates over net neutrality in developing countries mirror similar concerns in Europe and North America where service providers have come under attack for creating market inequalities by "zero-rating" their own content and partner content.[37]

---

[32] *About Internet.org*, INTERNET.ORG, https://internet.org/about.

[33] *Are You in the Free Zone?*, GOOGLE FREE ZONE, http://googlefreezone.com/.

[34] Sarah Perez, *Twitter's 'Zero' Service Lets Emerging Markets Tweet for Free*, TECHCRUNCH, May 29, 2014, http://techcrunch.com/2014/05/29/twitters-emerging-market-strategy-includes-its-own-version-of-a-facebook-zero-like-service-called-twitter-access/.

[35] Alex Hern, *Facebook Criticized for Creating 'Two Tier Internet' with Internet.org Programme*, THE GUARDIAN, May 19, 2015, http://www.theguardian.com/technology/2015/may/19/facebook-criticised-for-creating-two-tier-internet-with-internetorg-programme.

[36] Jeremy Malcolm, *Net Neutrality and the Global Digital Divide*, ELECTRONIC FRONTIER FOUNDATION, July 24, 2014, https://www.eff.org/deeplinks/2014/07/net-neutrality-and-global-digital-divide.

[37] Antonios Drossos, *Guest Blog: The Real Threat to the Open Internet is Zero-Rated Content*, WORLD WIDE WEB FOUNDATION, Feb. 17, 2015,

On the one hand, these new gatekeeping approaches, which privilege select portals and content, can improve educational opportunities and healthcare in underserved communities. Defending the importance of zero-rating services for closing the global digital divide, some argue that free access to mainstream sites would allow citizens to use additional data to access local sites and services.[39] Zero-pricing initiatives developed by the private sector are also believed to help build local Internet infrastructure by fostering consumer demand,[38] as well as providing more cost-effective and adaptable programs than government efforts that address digital divide issues.[39] They are, however, also part of a graduated shift away from the open Internet in which individuals can choose to access any information on the universal Internet equally to a model in which gatekeepers create technical and economic prioritization for their own content and platforms.

PROSPECTS FOR THE FUTURE OF INTERNET GOVERNANCE

These emerging trends in Internet governance whether originating in the private sector, in technological design changes, or in government regulations, are real and will have real implications for the future of the Internet. The greatest consequence is the possibility of fragmentation. Will there be a universal Internet or a fragmented Internet that varies depending on national boundaries or private gatekeeping? This concern about fragmentation arises in all five of the destabilizing conditions addressed in this paper. The loss of trust in

---

http://webfoundation.org/2015/02/guest-blog-the-real-threat-to-the-open-internet-is-zero-rated-content/.

4. Darrell M. West, *Digital Divide: Improving Internet Access in the Developing World Through Affordable Services and Diverse Content*, CENTER FOR TECHNOLOGY INNOVATION AT BROOKINGS INSTITUTION, Feb. 2015, http://www.brookings.edu/~/media/research/files/papers/2015/02/13-digital-divide-developing-world-west/west_internet-access.pdf.

38 Noelle Francesca De Guzman, *Zero Rating: Enabling or Restricting Internet Access?*, INTERNET SOCIETY, Sept. 24, 2014, http://www.internetsociety.org/blog/asia-pacific-bureau/2014/09/zero-rating-enabling-or-restricting-internet-access.

39 Diana Carew, *Zero-Rating: Kick-Starting Internet Ecosystems in Developing Countries*, PROGRESSIVE POLICY INSTITUTE, Mar. 2015, http://www.progressivepolicy.org/wp-content/uploads/2015/03/2015.03-Carew_Zero-Rating_Kick-Starting-Internet-Ecosystems-in-Developing-Countries.pdf.

institutions of Internet governance is creating geopolitical tensions over who controls various aspects of the Internet. Concern about surveillance is leading governments to introduce policies that superimpose physical boundaries that are simply incommensurate with how the Internet works at an infrastructural and logical (as well as institutional) level. Efforts to tamper with the DNS for content control have raised concerns about whether a universal system for resolving names into numbers will be sustainable. If the transition of U.S. oversight of names and numbers does not proceed, will the response be an introduction of alternative, and potentially, non-interoperable naming systems? Separately, the resurgence of proprietary systems harkens back to the closed online systems of the 1990s. There will be direct implications for access to knowledge, Internet stability and universality, free speech, cross-border trade, and the cost of doing business.

These conditions highlight three characteristics of Internet governance: that this governance extends far beyond traditional governments to include private sector policies and the design efforts of technical communities, that Internet governance conflicts involve some of the most pressing public policies of our time, and that Internet infrastructure is fully recognized as a site of political and economic power and increasingly used as a proxy for broader conflict.

Not surprisingly, the confluence of these circumstances has created rising geopolitical contention in Internet governance. This emergence of contention in Internet governance stems, in part, from the erosion of trust in the system, but also from the increasing recognition of the Internet as a vital political and economic force, in addition to recognition of its underlying infrastructural and institutional system of governance as a point of economic and political power. At the same time, there are divergent social rules and cultural norms within borders that simply do not map neatly onto a technological system (and institutional system) that crosses these borders.

Internet governance will become only more complicated as the Internet continues to move from a network of people to a network of things. The Internet is no longer a communication network, but a control network in which orders of magnitude of more things—industrial systems, home appliances, health monitoring devices, and drones—are connected, rather than people on the planet.

The solution to long-term challenges in Internet governance requires bringing together the political and the technical, rather than dismissing the technical as not politically constructed or the political as not technologically constrained. Outsized attention to civil liberties, such as individual privacy and free speech or values such as national

security and law enforcement, leave the issue of technological stability out of the equation. Concern about the stability of the technical infrastructure must be reintroduced into discussions, rather than serving as a taken-for-granted background system that will simply endure. Technology should equally be viewed as a component of the solution to destabilizing problems.

Solutions require two lenses: a pragmatic operational concern for the stable and secure administration of the Internet and a simultaneous focus on human rights–including communicative expression, individual autonomy and privacy, and economic liberty. As an example, bringing these two concerns together to address the loss of trust in the Internet leads to solutions, such as end-to-end encryption being the default in protocol design and implementation; collaborative security in which businesses and citizens take more proactive measures to secure networks; continued internationalization, rather than nationalization of Internet governance; and greater transparency, limitations, and accountability for the ways in which governments are turning to these infrastructures for geopolitical conflict.

At a minimum, the contemporary array of destabilizing conditions creates a moment of opportunity to set aside the view of Internet governance as "just a technical administration issue" or "clerical function," as some insiders have suggested, and instead view it as a set of distributed and multi-stakeholder responsibilities with profound implications for what will count as economic and expressive liberty in the coming decades.