IP JUSTICE

An International Civil Liberties Organization that Promotes Internet Freedom, Innovation Policy, and Balanced Intellectual Property Laws
www.ipjustice.org

IP JUSTICE JOURNAL: Internet Governance and Online Freedom Publication Series

Internet Architecture as Proxy for State Power

By Laura DeNardis, Ph.D. ~ 15 August 2015

Internet Freedom in the Age of Internet Control

The Internet is no longer just a communication system. It is also a control system in which more objects than people are connected to the network. Society is moving from a world in which content is digitally mediated to one in which all of life is digitally mediated. Beneath content, the Internet's physical and logical infrastructure is the technical scaffolding holding up basic systems of finance, commerce, transportation, industrial control systems, and surveillance technologies, as well as social interactions and access to knowledge. Already measured in billions, there will soon be 50 billion objects online ranging from wireless heart monitors, home alarm systems, weather sensors, surveillance monitors, cars, energy system sensors, and drones.[i] In cyberspace, the Internet of Things is rapidly morphing into the Internet of Self, aggregating not only cyber physical systems but everything from communications to commercial transactions to biometric identifiers. What are the prospects for Internet freedom in this context?

Internet freedom is no longer merely about content. Fundamental human rights depend upon an underlying system of technological infrastructure that creates the conditions for innovation and civil liberties online. These conditions are not preordained but have to be deliberatively designed into technical architecture, which in turn creates the conditions for economic and expressive liberty online. Since the Internet's inception, its development has embodied aspirational principles that have influenced how the network is both designed and administered.

The Internet Society, the not-for-profit organizational home of the Internet Engineering Task Force (IETF), has described these technical characteristics as "Internet invariants," the enduring principles that have shaped how the Internet is designed and administered.[ii] These technical norms include *global reach*, the potentiality of any end device to reach any other regardless of location, and *interoperability* among devices made by different manufacturers. They also include *permissionless innovation* in which anyone can introduce a new Internet application without a gatekeeper's consent as well as a network marked by *accessibility* and *general purpose* support of any application or service. The Internet Society's invariants related to governance include *collaboration among stakeholders, mutual agreement*, and the principle of *no permanent favorites* so essential for ongoing Internet innovation. As Internet engineer Leslie Daigle has summarized, "A network that does not have these characteristics is a lesser thing than the Internet as it has been experienced to date."[iii] While imperfect and always marked by conflicting interests and competing values, these norms have contributed to the Internet's growth, its architectural capacity for open innovation and expression, and a stable system of Internet governance.

Several trends in various governments' Internet policies are in tension with the technical stability and openness of Internet governance and architecture. These developments exist well outside of the enormous attention to the functions performed by the Internet Corporation for Assigned Names and Numbers (ICANN). There is not a single system of Internet administration, but many layers of distinct functions, many carried out by the private sector, some by new global institutions, some by governments, and some by all of the above in shared coordination arrangements. Even ICANN's oversight of names, numbers, and protocol parameters is distributed across domain name registrars that sell domain name registrations, governments, and Internet registries that administer names and numbers in a given top-level domain (TLD). Other functions of Internet governance include: the establishment of technical standards by the IETF, the World Wide Web Consortium (W3C), and others; interconnection agreements among private network operators; cybersecurity governance; the policymaking role of private information intermediaries such as Facebook and Google via their terms of service and privacy policies; and technical architecture-based intellectual property rights enforcement. [iv] All of these functions have policy implications ranging from privacy to property to speech rights.

Beyond the intrinsic public interest implications embedded in keeping systems of Internet infrastructure operational, another feature of Internet governance involves the phenomenon of governments attempting to use the very infrastructure of the Internet for geopolitical objectives having nothing to do with Internet operations. This phenomenon can be loosely termed the "turn to infrastructure" in Internet governance.[v] Policymakers view systems of Internet infrastructure and governance as part of their arsenal for achieving various political and economic objectives.

This paper extends this concept of examining the phenomenon of *governance by Internet infrastructure*, such as using authoritative DNS registries, as they exist, to enforce intellectual property rights, to the phenomenon of *governance by tampering with Internet infrastructure*, in other words, imposing statutory, technical, or other requirements to modify the actual design of Internet technical architecture for purposes completely extraneous to keeping the Internet operational. Discrete examples of this phenomenon include: government interest in weakening encryption technologies to achieve national security and law enforcement goals; nation-specific data localization laws; and attempts to politically impose modifications to the Domain Name System (DNS) for content control. Many of these policies conflict with how technologies work in practice and also create challenges for civil liberties online. The rising geopolitical attention to the Internet and inextricable linkages between human rights and infrastructure provide a moment of opportunity to assess potential implications of politically driven infrastructure modifications for the future of Internet stability and freedom.

Geopolitical Back Doors in Encryption Protocols Can Weaken Internet Security

New digital technologies, and new patterns of technology usage, always complicate the question of how to balance individual privacy and law enforcement. Consider the following statement: "Cell phones… are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[vi] The statement was not uttered on a late night comedy show but penned by United States Supreme Court Chief Justice John Roberts in a Supreme Court ruling about cell phone privacy. In *Riley v. California*, the Court took up the question of whether police are constitutionally permitted to search cell phones without a warrant. The Supreme Court ruled that warrantless searches of cell phones constituted a Fourth Amendment violation and were impermissible. Cell phones were deemed inherently different, privacy-wise, from other items a person might carry because of their enormous storage capacity, their ability to hold personal photographs, medical records, locational information, and other data stored over long periods of time, and because different types of information contained on a cell phone, in combination, reveal much more than a particular record. Does a right to encryption follow?

In an almost Orwellian turn, searching a phone raises more privacy issues than searching a house, as "a phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in any form..."[vii] The same technologies and networks that have provided unprecedented opportunities for freedom of expression and content aggregation, along with advances in storage and processing power, have also provided unprecedented opportunities for government surveillance. American government contractor Edward Snowden's 2013 disclosures about the expansiveness of National Security Agency (NSA) surveillance practices provoked a number of reactions from governments, the technical community, and other stakeholders. In December of 2013, the United Nations General Assembly adopted a resolution on the right to privacy in the digital age, affirming that "the rights held by people offline must also be protected online."[viii]

The Internet's technical community has called for "hardening the Internet" with greater end-to-end encryption.[ix] The consensus position of the IETF is that pervasive surveillance, whether of content or protocol metadata, is "a technical attack" that should be addressed by protocol design choices that would, at a minimum, make indiscriminate surveillance more expensive or less feasible.[x] By 2014, the Internet Architecture Board released a statement suggesting that encryption throughout the protocol stack be a norm and a default approach in order to restore trust in the Internet.[xi] Google announced it would “always use an encrypted HTTPS connection when you check or send email,” effectively preventing someone from ‘listening in’ even if accessing email from an open public Wi-Fi network.[xii]

One government response to these trends has been a call for building backdoors into encryption protocols and implementations so that agencies can readily access information. In an era of rising Islamic terrorism and associated employment of Internet technologies for recruitment and strategic communication, national security and law enforcement agencies, of course, turn attention to online intelligence practices and oppose efforts of technology companies to make these practices more difficult. For example, United States FBI Director James Comey has criticized corporate efforts to implement end-to-end encryption, arguing that encryption could prohibit law enforcement efforts to access vital information and calling for a reconsideration of encryption.[xiii] In the UK, a proposed bill could require private technology companies to build backdoors to user data as a tool for combatting global terrorism.[xiv]

Encryption has always been a politically charged technology, and one that historically has been embroiled in conflicts between individual privacy and national security. Conflicts have manifested as questions about legally restricting encryption strength (e.g. key length), banning certain types of encryption, or imposing export restrictions. The United States at one point regulated encryption along with firearms under International Traffic in Arms Regulations (ITARS). Initiatives to build “back doors” into encryption are part of an ongoing trajectory of political tensions over a technology inherently designed to provide security (e.g. public key authentication) and privacy.

One problem with “back doors” – no matter how well meaning - is that they build in inherent security vulnerabilities that could be exploited for other purposes. As Apple CEO Tim Cook warned, “If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people’s accounts. If they know there’s a key hidden somewhere, they won’t stop until they find it.”[xv]

The Global Commission on Internet Governance, an independent group chaired by Sweden’s former Prime Minister Carl Bildt, has issued a consensus recommendation that:

> “Governments should not create or require third parties to create ‘back doors’ to access data that would have the effect of weakening the security of the Internet. Efforts by the Internet technical community to incorporate privacy-enhancing solutions in the standards and protocols of the Internet, including end-to-end encryption of data in transit and at rest, should be encouraged.”[xvi]

Security experts, in their report “Keys Under Doormats,” raise similar concerns about building encryption backdoors: “These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.”[xvii]

The early 21st century has thus far been marked by numerous high-profile cybersecurity breaches, some geopolitically motivated, such as the Sony Pictures attack and presumably the massive data breach at the US Office of Personnel management (OPM). In the US alone, contemporary data breaches at large companies such as Target, Home Depot, and Premera Blue Cross have affected almost 200 million citizens. The concept of deliberatively designing additional security vulnerabilities into the Internet's infrastructure is incongruous.

Data Localization Laws Can Promote Fragmentation Rather than Universality

Internet infrastructure design does not map neatly onto national borders. Seeing a simple traceroute of packets moving from point A to point B helps illustrate how transmission paths depend on efficient routing rather than circumscribed borders. Physical infrastructure - fiber optic cable, antennas, switching centers, and server farms – resides within fixed geographic locations. But the distributed storage and processing systems and the flow of packets over this architecture do not comport with national boundaries. Even an exchange of information between two network operators within a single country can potentially route through an Internet Exchange Point (IXP) in another region. Companies can locate customer support centers in any location around the world. A retail company with a .COM address can reside anywhere in the world. Large multinational companies such as financial services firms use network systems spanning the globe rather than neatly circumscribed within a nation's border. Large content companies (e.g. Google) and Content Delivery Networks (e.g. Akamai) globally distribute content to bring it closer to users via replication (mirroring) and caching. Companies optimize information distribution across servers based on traffic patterns and variables such as bandwidth, processing power, and storage capacity.

A significant shift in policymaking has been the introduction of laws regulating where private companies store data and how infrastructure is physically configured. Much of the policy interest in imposing borders around Internet infrastructure has cited foreign surveillance, and in particular, the expansive NSA surveillance program as inducements. Political interest has ranged from wanting to avoid switching traffic through a US-based IXP in order to route around the United States to investing in new undersea cable routes, to data localization approaches requiring companies to store customer data on servers located within a nation's borders or otherwise controlling the cross-border movement, sharing, taxation or storage of customer information. Data localization laws, in particular, are already in place or pending in many countries.[xviii] A Russian law requiring companies to store data of Russian citizens within the nation's border takes effect in late 2015.

There are engineering, innovation, and civil liberties complications embedded within these policy-driven alterations to Internet infrastructure. "Holding" data in a fixed location is incompatible with engineering principles like reducing latency, load balancing, and basic traffic engineering. It is also incommensurable with business models predicated upon global customer bases and workforces. As civil society advocates have expressed, it moves the Internet from a *de facto* universal network to "a world with country-specific 'internets' that don't connect with each other to form today's global network."[xix] Large content intermediaries like Google have also expressed concern. In testimony before the Senate Judiciary Subcommittee on Privacy, Technology and the Law, Google's Director for Law Enforcement and Information Security, Richard Salgado, warned that data localization laws could result in the "Balkanization of the Internet" and constitute a challenge to the "free and open Internet that we benefit from today."[xx]

From an innovation perspective, consider the prohibitive cost burden to new entrepreneurs having to locate servers in any country in which they wished to operate. New entrants would not be able to compete in global markets. Only already-dominant companies would have the resources to comply with infrastructure localization requirements, a violation of the principle of "no permanent favorites." These laws would also have effects far beyond the tech industry. Sectors ranging from financial services to retail have large data stores of customer information that routinely cross borders for customer service, billing services, or direct delivery of information and goods to customers wherever they are in the world. Data localization laws apply to these companies as well. A McKinsey & Company survey of chief executives in the financial services sector revealed concern about data localization regulation, with problems ranging from increased organizational complexity to constraints on efficiency due to having to locate employees and infrastructure in local markets.[xxi]

From a civil liberties standpoint, the ensuing concentration of data in data localization scenarios could actually facilitate new forms of efficient surveillance,[xxii] either by the home nation or through foreign surveillance. Before data localization laws become a global norm, there is an opportunity for governments to rethink the potential political, economic, and technical collateral damage of these policies.

DNS Modifications Can Affect Internet Stability

The Domain Name System is another layer of the Internet's infrastructure which has attracted policymaker attention. The DNS translates human-friendly domain names, such as IPJustice.org, into corresponding binary numbers called Internet Protocol (IP) addresses. As such, it can be referred to as the Internet's phone book. This is a critical technical function involving the resolution of hundreds of billions of queries a day via servers located in every corner of the world. It is also a function that carries public interest implications, shaped by DNS technical design features. The hierarchical DNS provides points of control for redirecting queries away from certain websites, whether for censorship or intellectual property rights enforcement. The names and numbers the DNS administers are designed to be globally unique identifiers, both necessitating some degree of centralized coordination and also creating the conditions for IP addresses to be used as unique personal identifiers, in combination with other information.

Because the DNS inherently contains content (domain names) it is therefore a speech space embroiled with controversies such as free expression and intellectual property rights considerations. Trademark disputes are difficult enough, involving ICANN's Uniform Dispute Resolution Policy (UDRP) and ICANN's contractual relationship with domain name registrars and registries.[xxiii] There are many other complicated questions. What new top-level domains

(TLDs) may be introduced in a universal Internet supporting divergent cultural norms across regions (e.g. .GAY, .SUCKS, .WINE)? What happens when territorial interests clash with private trademark holders, as when countries with the Amazon rainforest within their borders objected to the proposal from Amazon, Inc. to introduce and operate a .AMAZON TLD? ICANN is at the center of decision making around these critical speech and property policy problems. Thus, the global attention to ICANN and, in particular, the ongoing and politically charged question of how to transition the US government's historic oversight functions to a global multistakeholder community.[xxiv]

The DNS also raises privacy policy conflicts in the query resolution process. DNS queries are almost always unencrypted.[xxv] A contemporary policy concern involves the question of enhancing privacy in DNS queries versus keeping this information unencrypted for law enforcement or other purposes. How this lookup information is retained and shared potentially exposes information about websites queried, which may contain private or sensitive information such as visiting websites addressing medical, substance abuse, or mental health issues.

As these examples convey, the DNS in its day-to-day operation already implicates complicated rights issues. A separate circumstance involves government efforts to modify or block DNS records and architecture to achieve objectives unrelated to keeping the Internet operational or dealing with public policy questions arising in normal DNS operation.[xxvi] The most routine example is the practice of using the DNS to block access to websites infringing intellectual property rights, such as those offering pirated movies or selling counterfeit luxury goods or pharmaceutical products.[xxvii] Domain name seizures have been regularly carried out by the US Department of Homeland Security's Immigration and Customs Enforcement (ICE) group. These redirections can occur by requesting that the authoritative Internet registry responsible for a top-level domain (e.g. .org, .com) remove the data mapping the infringing domain name or redirect it to another server, such as one containing a law enforcement message. When the registry operating the appropriate TLD is in a different jurisdiction, an alternative with greater potential repercussions for technical stability and universality involves local DNS redirection. When it is not possible to request a query redirection in the universal record maintained by an authoritative registry, presumably because the registry is extra-jurisdictional, it is possible to approach a local, albeit non-authoritative DNS operator to disregard the universal name and number mapping for the infringing site and instead modify it in local records. This technique changes the DNS from one that is universally consistent to one that has inconsistent records that vary by region. This same local redirection technique is used by governments to censor certain websites, such as blocking access to Twitter in countries with repressive information policies. One technical vulnerability caused by altering the universality of DNS records is the possibility, as has occurred, of locally modified records being broadcast more globally and creating security complexities related to the use of DNSSEC for cryptographically authenticating DNS records.

Identity theft techniques already exploit security vulnerabilities in the DNS to appropriate and alter queries (called DNS injection techniques) with the purpose of redirecting a user to a fraudulent site to extract financial information or to collect information for identity theft. These same techniques are sometimes used to censor content as part of the Great Firewall of China.[xxviii]

Once it becomes the norm for the DNS to be altered for content blocking and manipulation, it will be difficult to veer the DNS back toward universal consistency. Consideration of the technical implications to Internet stability, security, and universality, as well as the human rights implications of over-blocking and censorship, is critical before the DNS becomes the default gatekeeper for almost any type of blocking or security attack.

The Future of Internet Governance Should Consider Implications for Technology

One of the most pressing 21st century developments in Internet governance is the increasing entanglement between often well-meaning government policies and Internet infrastructure alterations. Much attention to Internet governance focuses on the *global institutions* of Internet governance (e.g. ICANN), *content regulations*, the public interest implications of *technical design*, or, increasingly, the role of technology *corporations* in establishing public policy. There are also many points of infrastructure intervention in which governments can help promote the health of the global Internet: the deployment of IXPs, IPv6 adoption, open standards, or restoring trust in the system through security cooperation. In addition to interrogating sociopolitical effects of technology on society; what are the potential effects of government policies on the stability and security of the technology?

The three policy examples this article addresses – encryption backdoors, data localization, and DNS alterations – share several characteristics. They are examples of government interest in altering the design of Internet infrastructure to achieve policy objectives. They all raise questions about the implications of these alterations for the stability and security of the Internet itself; for civil liberties; and for the pace of innovation online.

Each of these alterations raises questions about the possibility of technical fragmentation and the state of Internet "universality." Since the non-interoperable and fragmented 1990s era of proprietary online systems like Prodigy and the early America Online service, the desire for a consistent and universal system in which any device could reach any other device has always been a given for the public Internet. Of course, corporate Intranets and security-intensive networks supporting sensitive information have designed access controls and restrictions into the system. It is also easy to argue that a world with access divides, language barriers, and economic disparities hardly constitutes a universal Internet. But the technological building blocks for universality are present. These examples also suggest the types of security concerns that can arise from governmental interventions in Internet infrastructure. Encryption backdoors build in security vulnerabilities that could be exploited for criminal or other activities; data localization approaches concentrate rather than distribute data and can serve as targets for data breaches; DNS modifications can complicate the implementation of DNS cryptographic signing via DNSSEC.

These cases also help emphasize the contradictory values that always exist in Internet policy. On one hand, governments seek to protect citizen privacy with data localization requirements; on the other, they seek to have encryption backdoors to be able to access citizen data. Regardless of which values prevail, it is increasingly important to view Internet governance as not just about keeping Internet infrastructure operational and promoting access to knowledge, innovation, and economic growth. Internet governance and architecture has become a proxy for state power. And this exertion of state power by seeking modifications to Internet architecture must be accompanied by concern for the implications of these technical alterations for Internet stability and security and the characteristics necessary to preserve or promote a free and open Internet.

About the Author

Dr. Laura DeNardis is a globally recognized scholar of Internet governance and technical infrastructure and a tenured Professor in the School of Communication at American University in Washington, DC. Her books include *The Global War for Internet Governance* (Yale University Press 2014); *Opening Standards: The Global Politics of Interoperability* (MIT Press 2011); *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009); and *Information Technology in Theory* (Thompson 2007 with Pelin Aksoy). With a background in information engineering and a doctorate in Science and Technology Studies (STS), her research studies the social and political implications of Internet technical architecture and governance. She is an affiliated fellow of the Yale Law School Information Society Project and served as its Executive Director from 2008-2011. Her expertise and scholarship have been featured in *Science Magazine*, *The Economist*, *National Public Radio*, *New York Times*, *ABC news*, *Bloomberg*, *Time Magazine*, *Christian Science Monitor*, *Slate*, *Reuters*, *Forbes*, *The Atlantic*, the *Globe and Mail*, *Investor's Business Daily*, and the *Wall Street Journal* and she is a frequent speaker at the world's most prestigious universities and events. She is a Senior Fellow of the Centre for International Governance Innovation (CIGI) and currently holds an international appointment as the Research Director for the *Global Commission on Internet Governance*. Domestically, she is an appointed member of the U.S. Department of State's Advisory Committee on International Communications and Information Policy (ACICIP). Dr. DeNardis holds an AB in Engineering Science from Dartmouth College, an MEng from Cornell University, a PhD in Science and Technology Studies from Virginia Tech, and was awarded a postdoctoral fellowship from Yale Law School. Laura DeNardis was elected to membership in the *Cosmos Club* in 2015. She resides in Washington, DC.

[i] Cisco White Paper, Dave Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” April 2011. Accessed at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[ii] Internet Society, “Internet Invariants: What Really Matters,” February 3, 2012. Accessed at http://www.internetsociety.org/internet-invariants-what-really-matters.

[iii] Leslie Daigle, “On the Nature of the Internet,” *Global Commission on Internet Governance Paper Series* No. 7, March 2015. Accessed at https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf.

[iv] Laura DeNardis, *The Global War for Internet Governance*, Yale University Press, 2014.

[v] For an account of this turn to infrastructure for Internet governance, see Laura DeNardis, “Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance,” *Journal of Information, Communication and Society*, Volume 15, Issue 3, February 2012.

[vi] From the Supreme Court opinion *Riley v. California*, 134 S. Ct. 2473 (2014), opinion delivered by Chief Justice John Roberts, June 25, 2014, p. 13.

[vii] *Riley v. California*, 134 S. Ct. 2473 (2014), pp. 20-21.

[viii] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age A/HRC/27/37, p. 2, June 30, 2014. Accessed at http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

[ix] Hardening the Internet” was the title of the Technical Plenary of the IETF 88 meeting of the Internet Engineering Task Force in Vancouver, Canada, in November 2013.

[x] Stephen Farrell and Hannes Tschofenig, *Pervasive Monitoring Is an Attack*, IETF RFC 7258, May 2014. Accessed at www.rfc-editor.org/rfc/rfc7258.txt.

[xi] “IAB Statement on Internet Confidentiality,” November 14, 2014. Accessed at https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/.

[xii] Official Google blog posting by Nicolas Lidzborski, Gmail Security Engineering Lead, “Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability,” March 20, 2014.

[xiii] Spencer Ackerman, “FBI chief wants 'backdoor access' to encrypted communications to fight Isis,” *The Guardian*, July 8, 2015. Accessed at http://www.theguardian.com/technology/2015/jul/08/fbi-chief-backdoor-access-encryption-isis

[xiv] Theo Priestly, “All Instant Messaging Could be Killed in the UK within Weeks,” *Forbes*, July 13, 2015. Accessed at http://www.forbes.com/sites/theopriestley/2015/07/13/all-instant-messaging-could-be-killed-in-the-uk-within-weeks/.

[xv] Tim Cook cited in Matthew Panzarino, “Apple’s Tim Cook delivers blistering speech on encryption, privacy,” *TechCrunch*, June 2, 2015. Accessed at http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.lxuz8g:KaZu.

[xvi] Statement by the Global Commission on Internet Governance, “Toward a Social Compact for Digital Privacy and Security,” April 15, 2015. Accessed at https://www.ourinternet.org/publication/toward-a-social-compact-for-digital-privacy-and-security/.

[xvii] Hal Abelson et al., “Keys under doormats: Mandating insecurity by requiring government access to all data and communications,” Computer Science and Artificial Intelligence Laboratory Technical Report, *MIT*, 2015. Accessed at http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8.

[xviii] *Anupam Chander and Uyen Le, "Data Nationalism," Emory Law Journal, Vol. 64, No. 3, 2015.*

[xix] Emma Llanso, Center for Democracy and Technology, CNN op/ed "How Politicians are Trying to Break the Internet," September 5, 2014. Accessed at http://www.cnn.com/2014/09/05/business/opinion-internet-post-snowden/.

[xx] Written testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google, before the Senate Judiciary Subcommittee on Privacy, Technology and the Law hearing on "The Surveillance Transparency Act of 2013," November 13, 2013. Accessed at http://services.google.com/fh/files/blogs/google_testimony_transparency_nov132013.pdf.

[xxi] James Kaplan and Kayvaun Rowshankish, "Addressing the Impact of Data Location Regulation in Financial Services," *Global Commission on Internet Governance Paper Series* No. 14, May 2015.

[xxii] Ania Nussbaum, "Russia's data law will hurt its economy," *Wall Street Journal*, June 18, 2015. Accessed at http://blogs.wsj.com/digits/2015/06/18/russias-data-law-will-hurt-its-economy-think-tank/.

[xxiii] See, for example, David G. Post, "Internet Infrastructure and IP Censorship," *IP Justice Journal*, 1 August 2015. Accessed at http://www.ipjustice.org/digital-rights/internet-infrastructure-and-ip-censorship-by-david-post/.

[xxiv] For background on the IANA transition, see, for example, Emily Taylor, "ICANN: Bridging the Trust Gap," *Global Commission on Internet Governance Paper Series* No. 9, March 2015. Accessed at https://ourinternet-files.s3.amazonaws.com/publications/gcig_paper_no9.pdf.

[xxv] Stephane Bortzmeyer, IETF Draft, "DNS Privacy Considerations," January 7, 2015. Accessed at https://tools.ietf.org/html/draft-ietf-dprive-problem-statement-01.

[xxvi] A detailed delineation of various approaches to co-opting the DNS is addressed in Samantha Bradshaw and Laura DeNardis, "The Politicization of the Internet's Domain Name System: Implications for Internet Security, Stability, Universality, and Freedom," Refereed paper presented at the 56th Annual International Studies Association Annual Conference, New Orleans, 2015

[xxvii] For information about the practice and technical implications of domain name seizures, see Security and Stability Advisory Committee (SSAC), "Advisory Impacts of Content Blocking via the Domain Name System," 2012, available at https://www.icann.org/en/system/files/files/sac-056-en.pdf.

[xxviii] Jonathan Zittrain and Benjamin Edelman, "Internet Filtering in China," *IEEE Internet Computing*, March/April 2003. Accessed at http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan011043.pdf.