American Foreign Policy Interests, 36:300–313, 2014

ISSN: 1080-3920 print/1533-2128 online
DOI: 10.1080/10803920.2014.969178

Connected Choices: How the Internet Is Challenging Sovereign Decisions

Melissa E. Hathaway

ABSTRACT Modern societies are in the middle of a strategic, multidimensional competition for money, power, and control over all aspects of the Internet and the Internet economy. This article discusses the increasing pace of discord and the competing interests that are unfolding in the current debate concerning the control and governance of the Internet and its infrastructure. Some countries are more prepared for and committed to winning tactical battles than are others on the road to asserting themselves as an Internet power. Some are acutely aware of what is at stake; the question is whether they will be the master or the victim of these multilayered power struggles as subtle and not-so-subtle connected choices are being made. Understanding this debate requires an appreciation of the entangled economic, technical, regulatory, political, and social interests implicated by the Internet. Those states that are prepared for and understand the many facets of the Internet will likely end up on top.

KEYWORDS cyber; international rights; Internet; multilateral; power; security; sovereign

INTRODUCTION

Modern societies are in the middle of a strategic, multidimensional competition for money, power, and control over all aspects of the Internet and the Internet economy. These struggles are occurring across a range of interrelated economic, technical, regulatory, political, and social spheres and the gamesmanship is intense. The players include multinational corporations, self-organized citizen and interest groups, and state and non-state actors. As such, these areas of tension are multilateral, multistakeholder, and multicultural.

This competition has been increasing in focus, force, and global reach since the birth of the Internet as an e-platform for commerce, information flows, and power projection. In 1985, the potential for national power and wealth changed with the introduction of new top-level domains (e.g., .com). The Internet's potential became obvious in the early 1990s with the invention of the World Wide Web and was confirmed with broadband investments in the Internet's backbone network in the latter half of the decade. Today, the Internet community is able to click-connect-search-and-share information globally and almost instantaneously. The Internet

Melissa E. Hathaway is President of Hathaway Global Strategies, LLC, and Senior Advisor at Harvard Kennedy School's Belfer Center. She also serves as a Senior Fellow and member of the Board of Regents at Potomac Institute for Policy Studies, and she is a Distinguished Fellow at the Centre for International Governance Innovation in Canada. Recently, she was appointed to the Global Commission for Internet Governance (Bildt Commission). She served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. Ms. Hathaway is a frequent keynote speaker on cybersecurity matters and regularly publishes papers and commentary in this field.

facilitates access to and delivery of a wide range of services electronically, including e-government, e-banking, e-health, and e-learning, next-generation power grids, and air traffic control. The Internet also facilitates access to all things tangible, including even military-grade weapons. The devices that connect people, places, and things could offer up to $19 trillion in economic potential;[1] the modernization of industrial infrastructures already represents nearly 46 percent of the global economy (more than $32 trillion).[2] As an instrument of power projection and military capability, today's networked systems, particularly the Internet, challenge traditional ideas of security, stability, and sovereignty.

This infrastructure–Internet entanglement is a strategic vulnerability for all connected societies. The positive impact of the Internet on countries, communities, businesses, and citizens can only be sustained if the service is accessible, available, affordable, secure, interoperable, resilient, and stable. This is why the Internet and its underlying value proposition have become a *national security* matter. Global leaders must wrestle with the fact that their Internet infrastructures and citizen-facing services are vulnerable to interference and that their economic dependence on the Internet will not permit them to abandon the adoption path they are on.[3] They are also trying to diffuse or take advantage of the growing perception by many around the world that the United States has too much "control" over the Internet. The widespread view is that since the Internet was created in the United States, its companies dominate the information communications technology (ICT) marketplace and are generating tremendous wealth for the West. Hence, the United States is perceived to be acting in its own interests to the detriment of others.

This article discusses the increasing pace of discord and the competing interests that are unfolding in the current debate concerning the control and governance of the Internet and its underlying infrastructure. Some countries are more prepared and committed than others to winning tactical battles on the road to becoming an Internet power. Some are acutely aware of what is at stake; the question is whether they will be the master or the victim of these multilayered power struggles as subtle and not-so-subtle connected choices are made. Understanding this debate requires an understanding of the entangled economic, technical, regulatory, political, and social interests implicated by the Internet. Those states that are prepared for and understand its multifaceted nature will likely end up on top.

ECONOMIC INTERESTS

> The importance of money flows from its being a link between the present and the future.[4]

The first strategic area of competition is economic and concerns connectivity and infrastructure development. By the end of 2014, the Internet will be accessible to approximately 40 percent of the global population—most of whom are located in Western and more developed countries. The demand curve and market growth potential for connectivity and Internet penetration for the foreseeable future is likely to come from Asia, Africa, and South America—with these come potential power and influence for their populations.[5] However, the predicate to Internet access is the provisioning of the underlying infrastructure that can deliver affordable broadband Internet services to citizens. Governments and companies are racing to lay the foundations for universal access for citizens, while simultaneously tying access to their economic sustainability and development agendas. This economic activity is being closely tracked by the International Telecommunications Union (ITU), the Inter-Development Bank (IDB), the Organization for Economic Cooperation and Development (OECD), and the World Bank, all of which have been ranking countries on their telecommunications initiatives.

Advancing connectivity requires promoting network and broadband infrastructure expansion. These investments can be costly—and countries may not have the means to deliver high-quality, low-cost infrastructure to remote areas with smaller populations. In the days of the landline telephone-system, revenue was incurred through an inter-carrier international settlement system that negotiated a price per call based on origination and termination. This collection system helped pay for telecommunication infrastructure improvements aimed at reaching more and more citizens. However, in today's Internet Protocol (IP) environment, the concept of a "call" has no direct counterpart. Internet service providers (ISPs) may pay transit fees based

on capacity or use settlement-free peering, thus bypassing the payment scheme previously imposed by inter-carrier international agreements. Content providers that offer their services via the networks of infrastructure operators using an over-the-top (OTT) model pose further challenges to this model. OTT content and services providers include Google, Facebook, PayPal, Amazon, Skype, and others. These OTT providers consume bandwidth through their delivery of volumes of information to users transiting the infrastructure—usually for free. Sometimes these services can degrade the quality of the infrastructure operators' own telecommunication services, including core services, because they are using more than their "fair share" of bandwidth. Infrastructure operators are thus forced to make additional investments to ensure that they can provide their customers with the low-latency, high-quality experience that they demand 24 hours a day, 7 days a week. To further complicate matters, the majority of the OTT companies are headquartered in the United States.

Both national leaders and infrastructure operators feel threatened by this complex ecosystem. The entities that can "control" information flow can also assert or extract economic and political leverage. The perceived or very real inequality of who monetizes access to the Internet on the one hand, and who benefits from that access on the other, remains part of the ongoing debate. First, countries are seeking mechanisms to pair market access with cost-recoverable investments to pay for the infrastructure modernization that the twenty-first century digital society is demanding. Some leaders are looking to the regulatory environment and international treaty venues, such as those convened by the ITU, to assert power over ISPs and OTT providers. Second, the market liberalization of the past two decades may give way to the resurgence of state-run telecommunications companies that, acting as ISPs, would be the conduit for citizens to reach the Internet. This gives nations more "control" over private or quasi-private providers, allowing them to channel the proceeds into their own economy. Depending on the argument made, this could be perceived as a barrier to market access. For example, the German government recently made a decision to phase out the use of Verizon Communications services by 2015 and transition to Deutsche Telekom to provide communications services to German government agencies. The change was made because of concerns about network security and citizen privacy.[6]

A related aspect of the economic competition that has emerged around the Internet involves the movement of data across borders. For example, the Transatlantic Trade and Investment Partnership (TTIP) and the Trans-Pacific Partnership (TPP) are regionally based free trade agreements, both of which are seeking to increase economic growth. The parties to these agreements will have to enable the free flow of data across borders if they wish to facilitate commerce. Yet, some countries are seeking mechanisms to protect their data, declaring that there needs to be data sovereignty for national security purposes. Can the data assume the "flag" of the country in which it was created?[7] The controversy is particularly challenging in an era where data is stored in multiple centers and geographic locations to enable citizen access on demand. This raises two fundamental legal and political questions. First, does the data assume the citizenship of its creator or of the country in which it is stored? Second, what happens when the data is shared or backed up across multiple data centers in multiple geographic locations? The intermediaries (i.e., those who enable cross-border digital trade), will inevitably have an impact on national economies. They could also assert control in terms of influencing who benefits and who pays, thus presenting potential security challenges. For example, some countries may want to impose a jurisdictional right to inspect all data communications, while others may demand that organizations use indigenous "preferred" service providers and store data locally, thus forcing data to fall under local laws and giving potential access to law enforcement and intelligence services.

At the same time, efforts to promote the development of Internet Exchange Point (IXP) facilities to enable the quick transit of data through IP interconnections have accelerated. As countries strive to connect citizens in remote geographic locations, they will need multiple IXPs to ensure low-latency delivery while striving to ensure end-to-end quality of service. Meeting these demands will also require operators of IXP facilities to take measures to further the security, safety, continuity, sustainability, and robustness of their infrastructure. As a result, the companies or countries that build these IXPs will

have a great deal of power over network traffic and the content that transits through those pipes.

The actors that dominate market access to and provision of the Internet will have the opportunity to assert control over information flows as well. If this power struggle continues along its current trajectory, future Internet growth will be dominated by the East and the South, and a new set of governments and constituents will seek to assert their voice, leverage, and market power to achieve their own economic, political, military, and societal goals. The United States heretofore has been perceived as the dominant player—perhaps even the colonial power of the Internet—not least because it has been the main developer and provider of Internet technologies and services. It is also perceived as being the main financial benefactor of the Internet. Today, however, the United States and its innovation centers of excellence are struggling for access and influence and may soon face displacement as new market leaders emerge around the globe.

TECHNICAL INTERESTS

> The supreme art of war is to subdue the enemy without fighting.[8]

The second strategic area of competition that has emerged around the Internet is technical, involving multilateral decision-making bodies and multistakeholder processes. Both sets of constituents are debating who is best suited to govern the technologic foundations of the Internet. It is estimated that in the next five years, the Internet population will double and that the number of connected devices will reach at least 50 billion.[9] The effects of the Internet of Everything (IoE)—the devices that connect people, processes, data, and things—will place considerable demands on existing institutions and governance mechanisms, some of which have long-standing practices and natural leaders. Competition over Internet-related technical interests is being waged on five fronts: infrastructure, protocols, standards, security, and content.

Infrastructure

The underlying infrastructure of the Internet is constantly changing. ISPs come in many forms and sizes and go by many names: the phone company, the cable company, the wireless company, the satellite company, and others. In the future, the Internet may be provisioned by an unmanned aerial vehicle (UAV) or high-altitude balloons to connect those in rural and remote areas who have no Internet access.[10] ISPs are increasingly measured by their speed of service (e.g., upload and download times at megabits per second [Mbps]). The most technologically advanced cities in the world enjoy speeds of up to 100 Mbps and hope to advance beyond 1,000 Mbps.[11] In 2014, about 25 major ISPs carry 80 percent of the world's Internet traffic. By 2020, the number of ISPs carrying Internet traffic will likely change as new delivery technologies emerge (e.g., UAVs and balloons). Of course, these new technologies will have to navigate international politics as international conventions, administered by the ITU, determine allocation and use of radio spectrum. These technologies may also come under scrutiny for their need to loiter in sovereign airspace.[12] So, when companies like Google expand their market position to gain more control of the Internet backbone to deliver their services without intermediaries, they should not be surprised that they face opposition. These new technologies and projects also threaten to displace the traditional providers (e.g., China Unicom, Nippon, Telefonica, Telegraph, Telephone, Telstra, Verizon, and Vodaphone) that, in turn, are putting pressure on their governments and multilateral organizations to intervene to protect their interests. In some cases, defending the interests of the traditional providers is also convenient for the country because it advantages indigenous companies and enables the government to assert control over those who are trying to evade regulation and payment schemas.

Protocols

In addition to competition for the delivery path of the Internet, competition around how data moves through the Internet has also emerged, adding further complexity to the management of the Internet. First is the Domain Name System (DNS). Think of this as the "telephone directory" for the Internet in the sense that "[d]omain names are human-friendly names that are translated into Internet Protocol (IP) addresses, for example, www.acme.com is a domain name, and 216.27.178.28 is its IP address."[13] Second are

the individual protocols that are assigned to devices. The Internet of the twentieth century was designed to accommodate approximately 4.3 billion addresses,[14] and was enabled through the Internet Protocol version 4 (IPv4). The Internet of the twenty-first century, however, demands a much richer supply of addresses to accommodate the IoT uptake and field more than 50 billion devices. It also requires the adoption of the IPv6 protocol, which will open up 340 trillion, trillion, trillion (3.4×10^{38}) unique addresses.

The transition to IPv6 poses at least two challenges. First, the providers of the transport layer—those who deliver the Internet service—will need to ensure interoperability between IPv4 and IPv6 devices. A translation mechanism is needed to enable IPv6-only hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4-only infrastructure.[15] This will require ISPs to invest in the necessary technology to enable a seamless experience for their global users. Developing this mechanism is not an insignificant cost. The second challenge derives from the nature and perceived "nationality" of the entity that is in charge of the global coordination of the DNS Root, IP addressing, and other Internet Protocol resources—the Internet Assigned Numbers Authority (IANA), a department within the Internet Corporation for Assigned Names and Numbers (ICANN). The IANA functions are coordinated with and funded by the United States Department of Commerce's National Telecommunications and Information Administration (NTIA). This perceived influence of the United States over the timing and allocation of Internet addresses and how the "telephone directory" of the Internet moves data is problematic.

The fact that the United States (via ICANN) is seen as controlling the protocols of the Internet is, indeed, the reason why many international venues are debating the merits of multistakeholder administration versus multilateral governance. Some countries believe that moving some functions of the Internet into a more global UN-like forum would ensure fairer distribution of the Internet resources needed for their digital societies. Russia and China are certainly lead advocates for this approach. Other countries, too, echo this call for global governance and are advocating for the Internet Governance Forum (IGF) to be transformed into a World Internet Council to become the steward of the Internet.[16] Some global leaders posit that this would be more representative of their countries', corporate, and citizens' interests and make the how and why decisions are made more transparent. To diffuse the growing distrust in United States' involvement in the IANA functions, in March 2014 the U.S. government announced its intent to transition its role and asked ICANN to convene global stakeholders to develop a proposal for that transition plan.[17] Of course, this may not quell the desire to move the administration and governance of Internet resources into a multilateral venue.

Standards

The Internet society of the twenty-first century demands an interoperable Internet and devices that connect to that modernized infrastructure designed to work on any ISP backbone using standard protocols. This is where standards-setting bodies emerge as a strategic leverage point to influence the design specifications of the next generation of Internet products and services. There are a number of standards organizations, but two principal organizations affect the global marketplace in this area.[18] The first is the Internet Engineering Task Force (IETF), which manages the process of creating Internet standards. During this process, a "specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, [and then it] is adopted as a Standard by the appropriate body and is published."[19] The second organization is the International Organization for Standardization (ISO), an international standards-setting body comprising representatives from various national standards organizations. Its technical process leads to "endorsed" international standards that are often the benchmark that global corporations must design for and deliver to. Of course, there are many other standards-setting bodies, but these two affect much of the global Internet device and service market. Therefore, whoever designs these standards, creating that interoperability for global opt-in and global uptake, will also have a dominant presence in the market. Corporate and government players alike are positioning themselves to influence the outcomes of these two organizations because their decisions will determine market share, market influence, and, subsequently, market control.

Security

Surveillance, piracy, criminal activity, intellectual property theft, and physical harm/destruction are on the rise, with the Internet enabling much of it. As a result, securing the Internet infrastructure and the data and services that transit through it has become of paramount importance, sparking global debate and discord. Views differ on what is to be secured, how to secure it, and who should perform the duties. Some countries are turning to ISPs, which have unparalleled access to global networks, to provide upstream security for downstream devices. Initiatives of this type include blocking spam seen in transit, identifying compromised devices owned by customers, quarantining infected devices and blocking their access to the Internet, identifying and blocking sources of distributed denial of service attacks, and minimizing frequency and duration of network outages and route disruption. But this represents only one layer of the current amalgam of security actors.

Others are advocating for a system to ensure the security and management of the DNS Root. A single root is needed to ensure global uniqueness regarding names (both administration and allocation). Multiple roots might fragment the Internet, causing latency, misrouting, and potentially degrade Internet interoperability. As noted, some countries believe that the United States, through ICANN, is unfairly administering the system and are arguing for an alternative, more regional or local system of governance with multiple roots. Their arguments are further fueled by newspaper headlines about United States' monitoring and surveillance practices as well as its potential manipulation of data encryption standards.[20]

The regionalized Internet argument has other security undertones that may affect data routing and OTT providers. For example, France and Germany are considering a Schengen routing system for data in Europe.[21] But this raises another question: Is the intention of this proposal to better protect the privacy of their citizens or is it to control digital trade and cross-border data flows? In 2012, for instance, Iran announced that it would pursue a national intranet, block services from Google, Yahoo, and Hotmail, and replace them with indigenous and government-led programs like Iran mail and Iran search engine—in line with Iran's plan for a "clean Internet."[22] The emergence of other similar national intranets with national (non-Western) services is occurring more frequently, especially in the shadow of media reports about the scope of U.S. surveillance and intelligence-gathering activities.

Measures designed to secure the traffic, and the related infrastructure, come in many forms. Some are pushing for a Domain Name System SECurity (DNSSEC), which would make it possible to validate the authority of a query and response and ascertain whether the signed data has been changed during transport. The latter would limit interception and surveillance mechanisms. Others argue that ISPs should have a process or framework for securing Border Gateway Protocol (BGP) announcements (i.e., how data moves from one ISP to another) that includes specific technical procedures and protocols to ensure that routes cannot be "hijacked," rerouted, or brought offline. In April 2010, for example, BGP users received an alert regarding a prefix hijack by China's largest ISP—China Telecom. Internet traffic was rerouted for approximately 15 minutes as a result, affecting both Chinese and American Internet traffic. This event "underscores the vulnerability of the BGP routing infrastructure and reminds us that, if intentional, the criminal could store, alter or just throw away the traffic."[23] The fact that BGP is vulnerable to hijack, and that it has been done on a number of occasions, has led to a desire by many countries to want to know where all of their traffic has been and where it will be routed.

Still others are arguing for different protective measures for facilities, infrastructures, and even content. Protective measures date back to the original 1934 International Telegraph Convention, which gives states the ability to stop messages that "may appear dangerous to the safety of the State or would be contrary to the laws of the country, public order, or decency."[24] In 1988, public use of the Internet was in its infancy, and the International Telecommunication Regulations (ITRs) compiled that year did not contain explicit provisions for securing the traffic and supporting infrastructure.[25] They did, however, include a reference for Member States and the Operating Agencies to avoid "technical harm" (Article 9). This "special provision" was added as a reaction or afterthought at a time when Member States were faced with the release and propagation of the Morris Worm that affected 10 percent of the Internet's

computers and disrupted Internet services for days.[26] Today, such a provision may translate into arguments to allow states to interfere with communications whose purpose is, indeed, to hinder the internal affairs or undermine the sovereignty, national security, territorial integrity, and public safety of other states.

Security arguments are being used to empower governments to advance their economic, political, and military interests in the operational implementation and architecture of the Internet. This weakens multistakeholder processes and venues and, at the same time, boosts market access, disrupts the power and control over Internet governance, and positions states for standards leadership.

Content

Technology innovation over the last 20 years has also led to big changes in data generation, consumption, and analysis. The modern digital society—both people and devices—is generating a lot of data. Looking at the widespread use of tablets, cell phones, cameras, EZ-passes for the highway, cars, smart grid, and so on, we see that we live in a world of near-ubiquitous data generation. This reality is coupled with the declining cost of collection, storage, and new capabilities for processing and correlating data.[27] Moreover, it has led to the emergence of new power brokers—those intermediaries who buy, sell, and correlate data about citizen and device interaction with and over the Internet. Data aggregators amass online and offline information about people, culling details from websites, social media, search engines, buying habits, travel patterns, and even government databases.[28] They use technology and statistical algorithms to combine multiple sources of data to make inferences about individuals, their interests, and the devices they use. They uncover patterns of activities and profile and track individuals—all this has profound implications for government and society, especially in terms of surveillance and censorship. This capability is no longer the sole purview of government intelligence services. In fact, with the right tools, commercial companies like Google, Baidu, Facebook, Tuenti, Badoo, and Renren are just as capable and have access to troves of data.[29]

The content of the flow of data over and throughout the Internet is important because it has significant economic, political, and social value. Those who can tap into that content, therefore, have power. If mined and leveraged properly, this data can help identify the next consumer market (i.e., where to place the next Walmart), help locate suspected terrorists, or dismantle an organized crime syndicate. It can also open new venues to exchange ideas and create new subjects for censorship. In the United States, law enforcement officials (e.g., the Federal Bureau of Investigation [FBI]) use social platforms such as Facebook and Twitter to garner tips about suspected terrorists.[30] On the other hand, some countries use citizens' digital footprints to search for and suppress those who might pose a threat to a regime's stability. For example, in March 2014, Turkish Prime Minister Recep Tayyip Erdoğan instructed ISPs operating in Turkey, including TurkTelekom, to seal off access to social media sites like YouTube and Twitter.[31] This action was taken in response to Turkish citizens having used social media to organize protests across the country against his government's policies. In February 2014, Russia passed a new censorship law demanding that ISPs block access to websites deemed to contain information promoting extremism and/or endangering public safety. As noted by one commentator, the wording of this law can be broadly interpreted to "forbid pretty much anything critical of the ruling government: political opposition, environmental activism, provocative political art, investigative journalism, nonviolent political protest."[32]

Countermeasures are also being fielded to circumvent increased surveillance and censorship. For example, The Onion Router (TOR) is free software and an open network that enables communications (and content) to move around a distributed network of relays run by volunteers all around the world who are circumventing measures to block their communications. It allows people and groups to increase their privacy and security on the Internet and keep some anonymity. Originally developed for the U.S. Navy for the primary purpose of protecting government communications, TOR is now widely used by dissidents, activists, journalists, law enforcement personnel, and military constituents. Some governments facilitate the use of TOR to enable freedom of speech and to promote democratic values. Those governments, however, are often criticized for interfering in the sovereign business of other states—namely

in their regime legitimacy and stability. Of course, many other countries are trying to block the use of TOR (or crack its code) for national security purposes.[33]

Increasingly, we are seeing national leaders interfering with the Internet on behalf of their own interests,[34] with tensions rising between states as a result. Global leaders and citizens in different parts of the world are demanding clarification on data ownership, privacy, and transparency. In short, they want to know what is being done with their data and how it is being used. In addition, many democracies continue to push for Internet freedoms and have declared access to the Internet a human right. More autocratic or authoritarian regimes, however, increasingly view the Internet as a threat. Others, like the United States, in a subtler and more hypocritical way, demand that other countries refrain from censoring their citizens while simultaneously pursuing their own broad-based monitoring and surveillance programs. This, in turn, does not help instill confidence in the legitimacy of the United States for Internet leadership.

Competition to shape the technological foundations of the Internet is strong—not least because it can lead to greater power, control, and monetization of the Internet and the Internet economy. Its future is being debated in a range of international venues and bodies, ranging from the ITU to the IETF to ICANN and ISO. How its functions and features should be governed is also being discussed by entities like the World Economic Forum (WEF) in special meetings like NetMundial[35]—which took place in April 2014 in Brazil—and by commissions like the Global Commission on Internet Governance.[36] It is in these venues that the future course of infrastructure, protocols, standards, security, and control of content will be determined.

REGULATORY INTERESTS

> To widen the market and to narrow the competition is always the interest of the dealers.[37]

The third strategic area of competition is regulatory, which is focused on ensuring that the Internet remains accessible, affordable, secure, stable, and interoperable for everybody. Market mechanisms are being used to assert leverage and control and to change the balance of power, politics, and wealth creation. Countries and companies are at odds in this field. The subtle struggle is focused on how to govern the growth of the Internet—namely what is in the best interests of society and government versus what is in the best interests of companies and their shareholders. The main challenge lies in the fact that the private sector designs, builds, operates, maintains, and restores the very systems that process, transmit, and operate the country's most important information and most vital infrastructures, while governments remain the ultimate guarantor of their citizens' safety and well-being.

It is thus the responsibility of governments to facilitate the market to meet the economic and national security interests of their citizens. Most of the time this encompasses the provisioning of citizen-facing services like water, electricity, and telephone access. Now that the Internet affects these and other citizen-essential services, governments are evaluating whether the Internet is in need of some sort of market corrections. The challenge, however, is establishing what exactly should be governed. Is it the functional areas of infrastructure provisioning, DNS administration, the standards-setting processes, and the security thereof? Or is it the actual facilities, devices, companies, and market access that need to be governed? Each country is using different market levers, in the form of legislation and regulations, to assert control, manage risk, build security back into the infrastructure, and maintain political stability. For example, the European Parliament has released a draft legislative directive on "Measures to Ensure Network and Information Security."[38] This directive, if passed, would legally bind member states to be compliant with specific criteria, adopt appropriate steps to manage security risks, and report serious incidents to their national competent authorities. The directive is targeted to the operators of critical infrastructures, such as energy, transport, financial services, and health care, and to key providers of information society services, such as e-commerce platforms, social networks, and so on. The United States has signaled a similar intent to regulate broad industry sectors in Presidential Executive Order 13636 on "Improving Critical Infrastructure Cybersecurity."[39]

Other countries are turning instead to international treaty mechanisms to affect the market as

well as contain political and social unrest. For example, in 2012, the ITU convened a World Conference on International Telecommunications (WCIT) to update and revise the International Telecommunications Regulations (ITRs).[40] The ITRs define the general principles for the provision, operation, and compensation of international telecommunications services. The WCIT represented a perfect venue for countries seeking to assert more control over many aspects of the Internet, including facilitating an accounting mechanism to compensate for the infrastructure improvements needed to carry the ever-growing Internet (voice, data, and video) traffic and to initiate security requirements for key facilities and networks. At the conclusion of the meeting, some 89 nations signed a new treaty and approximately 55 did not. The United State led the dissenting block, which had advocated for either maintaining the status quo or no change at all to existing ITRs, and has been criticized for its position ever since. At the time of negotiation, Ambassador Terry Kramer, the United States lead negotiator, stated, "[w]e are disappointed with revisions that expand the treaty scope to Internet-related matters and content. We believe these provisions reflect an attempt by governments to regulate the Internet and its content, potentially paving the way for abuse of power, censorship and repression."[41]

As one might expect, the debate or intent to govern the growth and assert control over the Internet did not end with the WCIT meeting in Dubai in 2012. In fact, many policy issues have extended into the discussions of the World Telecommunication/Information and Communication Technology Policy Forum (WTPF), the World Telecommunication Standardization Assembly (WTSA), the World Summit on the Information Society (WSIS), the Internet Governance Forum (IGF), and the UN General Assembly—to name a few. Other issue areas are coming forward in these venues, including: promoting IPv6 deployment and advancing connectivity by promoting IXPs; advancing DNSSEC; generating a road map for future evolution of Internet governance; providing reliable tools for e-commerce, banking, private communications, and so on, to move toward a more secure Internet; establishing work programs and guidelines for defining telecommunication development questions and priorities; and identifying properties for global Internet cooperation.

POLITICAL INTERESTS

> Governments will always play a huge part in solving big problems. They set public policy and are uniquely able to provide the resources to make sure solutions reach everyone who needs them. They also fund basic research, which is a crucial component of the innovation that improves life for everyone.[42]

The fourth strategic area of competition is political. The Internet has become a political platform for messaging. Political actors now have the opportunity to perform on a global stage and compete to persuade multiple audiences at the same time, articulating policies and investments needed for strength in, and dominance of, the digital economy, and that ultimately serve their own interests. They articulate the benefits quite clearly in terms of Gross Domestic Product (GDP) growth, job creation, access to information, and the ability to innovate. They also communicate the challenges in terms of threats to society, and the need to prepare for action and defend critical infrastructures, services, businesses, and citizens from malicious cyber-activities. With each speech given or initiative carried out, they position themselves for economic, political, and military leverage, power, and dominance.

As they communicate with their citizens—the constituency that holds the key to their power, legitimate or not—they highlight the rights of the individual to Internet access, better education, employment opportunity, economic well-being, and privacy. When speaking to industry and government leaders, they highlight the need for partnership, emphasizing the link between delivery of citizen-essential services and state responsibility (in the manner by which the state dictates and by which a company can make a profit). But does their success in arguing for such deep partnership mean that a specific industry is working for national economic, political, and military interests? Sub-rosa messages are also being conveyed, but the question of what market levers does a state need to impose to ensure collective market dominance and hence mutual economic growth remains.

Finally, some leaders are signaling thresholds and trying to establish norms of acceptable behavior for other leaders.[43] Their intent is to protect the value of their current and future digital investments and to preserve the importance of the Internet for their

political and economic interests. For example, President Xi Jinping has openly announced China's dual focus on developing technology and ensuring cybersecurity. These two aspects, he asserted, are "two wings of a bird" and require an overall plan to advance both simultaneously.[44] Chancellor Merkel has stated that "a 'cyber dialogue' is needed to set mutual privacy standards and legal frameworks . . . to to catch up to rapidly advancing technology."[45] President Putin has discussed similar governance issues, stating that "establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union . . . [should be a] priority on the international agenda."[46] And, President Obama has shared his viewpoint and concerns by stating that "America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property."[47]

Ultimately, the Internet remains both a global commons and part of each nation's sovereign infrastructure, and thus activities in cyberspace must continue to navigate two sets of demands: national interests and global interests. The forms of competition and tension discussed in this article are about different power struggles. They are also about those leaders who are using sophisticated strategies to forge complementary activities that ultimately serve their and their countries' interests. For those in the middle of this competition, it is important that they recognize that the gamesmanship and strategies are multifold. Perhaps this is why government intervention in this field tends to be more pronounced and pervasive—from controlling market access to subsidizing market entry and market share to imposing greater security requirements (and gaining access to intellectual property) to increasing censorship and surveillance practices for security and stability purposes. Political leaders are responsible for articulating a vision and establishing general principles and policies to achieve their goals and, accordingly, are constantly trying to advance their agendas using policy, law, market mechanisms, regulation, standards, and other initiatives. The evidence is clear, you just have to look for it.

SOCIAL INTERESTS

> Advances in the technology of telecommunications have proved an unambiguous threat to totalitarian regimes everywhere.[48]

The fifth and final strategic area of competition concerns the social aspects of the Internet and whether the Internet should be considered a citizen right or privilege. In less than two decades, the Internet has evolved from an opt-in service, where citizens and governments were able to *choose* whether or not to participate in the Internet society, to a compelled infrastructure that *requires* participation in order to reap its benefits and deliver essential services to citizens. This, in turn, is changing perceptions regarding citizens' rights and privileges. It is also shifting the power and perception of ownership.

In 2011, a group of nations formed the Freedom Online Coalition to advance Internet freedom—free expression, association, assembly, and privacy online.[49] During the 2014 NetMundial meeting, participants agreed that human rights should underpin Internet governance principles.[50] Echoing the UN Human Rights Council's 2012 decision,[51] they declared that the rights that people enjoy offline must also be protected online in accordance with existing international human rights treaties and legal obligations.[52] Some of these rights include freedom of expression, freedom of association, privacy, freedom of information, and access to information. But if citizens really are to enjoy these rights, then what mechanisms do they have at their disposal to challenge their national leaders when their rights are violated? And who is going to enforce them? Unfortunately, the reality is that the very interconnectedness of people can be denied and that freedom of communication and political freedoms are clearly linked.

For example, many protests were organized in the *favelas* of Brazil leading up to the recent World Cup games. The citizens of historically underserved communities were angry over their living conditions in addition to being incensed about the government's pacification program, which, building on an earlier program, was "designed to seize back control of the areas from drug traffickers and make them safer for the tournament and the 2016 Olympics."[53] They were also angry about the amount of investment

the government was making in the stadiums and facilities needed to support the influx of tourists during the World Cup, arguing that these resources would be better used to improve the living conditions of its own citizens. In addition, they believed that their views were not represented by the quasi-state-controlled media and took matters into their own hands. Citizens became journalists—using their smartphones, digital cameras, and apps such as Twitcast and Twitcam to circulate photos and video so the world could see what was really happening in the streets of Brazil. Venezuela's government is facing outraged citizens, too, and has blocked images on Twitter after violent protests emerged in Caracas seeking redress for "a catalogue of woes that include rampant inflation, food shortages and one of the world's highest murder rates."[54]

A related question is whether the "governed" have a right to own their data or to know what their "governors" (which can include both governments and private actors) are doing with their data? In May 2014, the European Court of Justice (ECJ) ruled in favor of a Spanish citizen's right to privacy and sent a message to the data aggregators and content brokers that privacy is paramount. The ECJ's ruling upholds "European citizens' right to be forgotten," that is, "their right to have embarrassing and currently misleading information deleted from the Internet."[55] Many Europeans celebrated the ECJ ruling against Google, noting that the United States has not curbed the monopolistic behavior of Google and its broad infringement on the privacy of citizens. For some, the ECJ's ruling was Europe's way of mitigating such behavior. Governments are also believed to be infringing on citizens' right to privacy. To address this concern, the U.S. National Security Agency's (NSA) Internet surveillance programs are being scrutinized, and President Obama recently pared down the scope of its collection activities.[56] The United Kingdom and many other Western nations are also reviewing the scope of their intelligence services and some leaders are calling for new laws to govern surveillance programs.[57]

On the other hand, other countries are supplementing their own surveillance practices by passing laws to require that data be stored within their territories, making it easier to intercept, search, or protect. For example, "Russia's Parliament has approved a law similar to China's that would require Internet companies such as Google to locate servers handling Russian traffic inside the country and store user data locally for six months."[58]

Finally, when do the empowered go too far? Governments are increasingly requesting and can even compel private sector assistance in conducting voice or data surveillance. In some cases, there is no territorial limitation on that power. For example, Microsoft is fighting a U.S. government search warrant that compels Microsoft to hand over customer data (e-mails) maintained in a data center operated by one of its subsidiaries located in Ireland. The data in Microsoft–Ireland's possession, custody, or control relates to a drug investigation.[59,60] This type of overt collection and government intervention is compromising the integrity of multinational companies that provision Internet services and store customer data. It also is contrary to and undermines existing international law. Many countries, including the United Kingdom, India, Belgium, the United Arab Emirates (UAE), are passing legislation to compel companies to hand over encryption keys to aid law enforcement investigations and support national security matters. Still others, China among them, are demanding that companies that want to deliver products to their (broadly defined) national security marketplace must turn over the source code for their products. More recently, perhaps in an effort to limit market penetration, a leading Chinese news agency branded Microsoft's Windows 8 operating system as a threat to the nation's information security.[61]

In the next five years, the number of global Internet users will double. That growth will primarily come from China, India, and African nations. Those societies have very different histories, development trajectories, cultural backgrounds, and experiences with government. Freedom of expression may not have the same cultural undertones (and support) as it has in the West. And experience in other areas shows that guaranteeing freedom of, and access to, information can be difficult, even if the necessary legislation is in place. How these new Internet users assert their voice, leverage their market positioning as consumers, and influence power will show us whether they see the Internet as a citizen right or a privilege.

CONCLUSION

> Two roads diverged in a wood, and I—I took the one less traveled by, and that has made all the difference.[62]

We are in the midst of an intense competition for money, power, and control over all aspects of the Internet and the Internet economy. The competition for Internet dominance is being waged across economic, technical, regulatory, political, and social battlefields. The web of relationships between each issue is noteworthy to say the least.

Underpinning this competition is the perception that the United States remains the Internet's superpower, a perception that many around the world would like to see change. The continuous release of information over the past year about the U.S. government's role in Internet surveillance and intervention has accelerated national desires and agendas to transfer Internet governance to venues like the United Nations, ITU, and other international fora, which many perceive to be more legitimate, fair, and transparent. Countries arguing for these significant changes are already establishing their own foothold on Internet matters, while also eroding the positions of the United States (and the West). This situation is also giving rise to private companies that feel violated by their own governments and are losing real market share around the world as a consequence.

Looking to a future where the demand curve and market growth of the Internet are likely to be driven from Asia, Africa, and South America, the United States will not maintain its position of influence unless it develops and delivers a new message focused on economic competitiveness and business opportunity that respects the rights of individuals in their liberty, thoughts, and possessions. Without a new cadre of leaders—both in the government and in the private sector—it will be very difficult for the United States to engage around the globe without being perceived as colonialist or paternalistic. And, the chorus calling for multilateral organizations to seize control over the technical and regulatory underpinnings of the Internet will only continue to grow in volume and power.

Counteracting these calls for change requires a new message that can unify nations in a common vision of how the Internet and its underlying technologies can foster trust, fuel global economic growth for all, and empower citizens. A thorough action plan that brings together a broad set of countries and participants to work toward this vision, jointly and across borders, and in partnership with government and non-state actors, is the way forward.

Who will stand up and be the guarantor of the Internet's future? America's strategic interests are at stake and, as in David versus Goliath, the world is now rooting for David to win.

Notes

1. World Economic Forum, ''The Global Information Technology Report 2014: Rewards and Risks of Big Data,'' 2014, http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf.
2. General Electric, ''Industrial Internet: Pushing the Boundaries of Minds and Machines,'' November 26, 2012, 13, http://www.ge.com/europe/downloads/IndustrialInternet_AEuropeanPerspective.pdf.
3. Melissa E. Hathaway, ''Toward a Closer Digital Alliance,'' *SAIS Review* XXX, no. 2 (November 18, 2010).
4. John Maynard Keynes, ''The General Theory of Employment, Interest, and Money,'' chapter 21 *in The Theory of Prices*, https://www.marxists.org/reference/subject/economics/keynes/general-theory/ch21.htm.
5. Internet Penetration by Region, http://www.internetworldstats.com/stats.htm.
6. Anton Troianovski and Danny Yardin, ''German Government Ends Verizon Contract,'' *The Wall Street Journal*, June 26, 2014, http:// online.wsj.com/articles/german-government-ends-verizon-contract-1403802226.
7. Some countries are debating the merits of keeping data contained inside the geographic boundaries of their home country. If the data leaves the geographic borders, then it must be marked or ''flagged'' accordingly.
8. Sun Tzu, *The Art of War*, chapter 3 (New York: Oxford University Press, 1963).
9. Dave Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything* (San Jose, CA: Cisco Internet Business Solutions Group, 2011), http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
10. Google launched Project Loon to use a global network of high-altitude balloons to connect people in rural and remote areas who have no Internet access. It began as a pilot in New Zealand and is expanding into Africa and elsewhere. For more on this, see http://www.google.com/ loon/.
11. Rediff Business, ''20 Best Broadband Providers in the World,'' November 14, 2013, http://www.rediff.com/business/slide-show/slide-show-1-special-20-best-internet-broadband-providers-in-the-world/20131114.htm#2.
12. Kevin Fitchard, ''Politics Could Pop Google's Project Loon,'' *Business Week*, June 24, 2013, http://www.businessweek.com/articles/ 2013-06-24/politics-could-pop-googles-project-loon.
13. Melissa E. Hathaway and John E. Savage, ''Stewardship of Cyberspace: Duties for Internet Service Providers,'' March 2012, 15, http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.
14. S. Bradner and A. Mankin, ''The Recommendation for the IP Next Generation Protocol,'' *RFC 1752*, January 1995.
15. SixXS, ''IPv6 Transition Mechanism/Tunneling Comparison,'' https://www.sixxs.net/faq/connectivity/?faq=comparison.
16. ''EU Internet Governance: Franco-German Alliance,'' EurActiv.com, July 11, 2014, http://www.euractiv.com/sections/

innovation-enterprise/eu-internet-governance-franco-german-alliance-303421.
17. United States Department of Commerce, ''NTIA Announces Intent to Transition Key Internet Domain Name Functions,'' March 14, 2014, http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.
18. Other international standard-setting bodies include: the Institute for Electrical and Electronics Engineers (IEEE), the Organization for the Advancement of Structured Information Standards (OASIS), and World Wide Web Consortium.
19. The Internet Engineering Task Force, ''The Internet Standards Process,'' Revision 3, http://www.ietf.org/about/standards-process.html.
20. Joab Jackson, ''NIST Denies NSA Tampering with Encryption Standards,'' *PC World,* September 10, 2013, http://www.pcworld.com/article/2048510/nist-denies-nsa-tampering-with-encryption-standards.html.
21. ''Weighing a Schengen Zone for Europe's Internet Data,'' *Deutsche Welle*, February 20, 2014, http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482.
22. Melissa E. Hathaway and Alexander Klimburg, ''Preliminary Considerations: On National Cyber Security,'' chapter 1 in *National Cyber Security Framework Manual* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, December 2012).
23. Melissa E. Hathaway and John E. Savage, ''Stewardship of Cyberspace: Duties for Internet Service Providers,'' March 2012, 15, http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.
24. International Telecommunications Union, ''The Constitution of the International Telecommunications Union, Preamble'' (see Article 34), http://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx.
25. The 1988 ITR was signed by 178 countries and is a recognized global treaty. The purpose of the ITR treaty was to facilitate global interconnection and interoperability of international telecommunications networks by establishing a regulatory framework to govern traffic flows between telecommunication network operators; address international routing, charging, accounting, and billing between operators; assure quality of international services; and encourage avoidance of harm to networks and services. The regulations are credited with providing for economic growth via the e-economy and development around the world by liberalizing telecommunications and creating interoperability among network providers.
26. Robert Morris, Jr., a graduate student in Computer Science at Cornell University, wrote an experimental, self-replicating, self-propagating program called a *worm* and injected it into the Internet on November 2, 1988. This Internet worm, named after Morris, brought ten percent of Internet-connected systems to a halt. Morris was tried and *convicted under the Computer Fraud and Abuse Act of 1986*.
27. The White House, ''Big Data: Seizing Opportunities and Preserving Values,'' May 1, 2014, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.
28. The Federal Trade Commission, ''Data Brokers: A Call for Transparency and Accountability,'' May 2014, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
29. Jain Sorav, ''40 Most Popular Social Networking Sites around the World,'' Social Media Today, October 6, 2012, http://www.socialmediatoday.com/content/40-most-popular-social-networking-sites-world; and TechWatch, ''Top 10 IT Data Aggregators,'' 2014, http:// www.jazdtech.com/techdirect/leaf/Data-Management/Database-Tools/Data-Aggregation.htm.
30. Joe Sterling, ''FBI Says It's Using Facebook, Twitter to Find 'Wanted Terrorist,''' *CNN*, October 3, 2012, http://www.cnn.com/2012/10/03/ justice/massachusetts-fbi-terrorist/.
31. Earl Zmijewski, ''Turkish Internet Censorship Takes a New Turn,'' Renesys, March 30, 2014, http://www.renesys.com/2014/03/turkish-internet-censorship/.
32. Yasha Levine, ''Putin Ramps up Internet Censorship, Citing Google and Snowden to Ensure Public Support,'' *Pando Monthly*, March 20, 2014, http://pando.com/2014/03/20/putin-ramps-up-internet-censorship-citing-google-and-snowden-to-ensure-public-support/.
33. The TOR Project, ''Censorship,'' https://blog.torproject.org/category/tags/censorship.
34. The TOR Project, ''About,'' https://www.torproject.org/about/overview.html.en.
35. NetMunidal, ''Global Stakeholder Meeting on the Future of Internet Governance,'' http://netmundial.org.
36. The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future Internet governance, http://www.cigionline.org/activity/global-commission-internet-governance.
37. Adam Smith, ''Wealth of Nations, '' vol. X, in *The Harvard Classics* (New York: P.F. Collier & Son, 1909), 14.
38. European Commission, *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union (COM(2013) 48 final)* (Brussels: European Commission, 2013).
39. The White House, Executive Order 13636, ''Improving Critical Infrastructure Cybersecurity,'' February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
40. International Telecommunications Union, ''Final Acts of the World Administrative Telegraph and Telephone Conference Melbourne, 1988: International Telecommunications Regulations,'' Geneva, Switzerland, 1989, https://www.itu.int/dms_pub/itu-t/oth/3F/ 01/T3F010000010001PDFE.pdf.
41. Wayne Rash, ''WCIT Treaty Talks End in Dubai with Walkout of U.S. and Allies,'' *E-Week*, December 15, 2012, http://www.eweek.com/cloud/wcit-treaty-talks-end-in-dubai-with-walkout-of-us-allies/.
42. Dana Goldstein, ''5 Questions for Bill Gates: The Full Interview,'' Daily Beast, January 24, 2010, http://www.thedailybeast.com/articles/2010/01/25/5-questions-for-bill-gates-the-full-interview.html.
43. There are multiple venues where norms setting is taking place. The United Nations's Government Group of Experts, for example, facilitates dialogue among states to reduce risk and protect critical national and international infrastructure. It seeks consensus among nations on the applicability of the UN Charter, international law, and the principles of state

sovereignty and responsible state behavior to cyberspace. Additionally, the Organization for Security and Cooperation in Europe (OSCE) has been working on confidence-building measures to reduce the risks of conflict stemming from the use of ICT. The report from that work was published in December 2013.
44. Shannon Tiezzi, ''Xi Jinping Leads China's New Internet Security Group,'' *The Diplomat*, February 28, 2014, http://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/.
45. See, for example, http://washington.cbslocal.com/2014/05/02/merkel-difficulties-yet-to-overcome-in-us-spy-scandal/.
46. Jerry Brito, ''The Case against Letting the U.N. Govern the Internet,'' *Time*, February 13, 2012, http://techland.time.com/2012/02/13/the-case-against-letting-the-united-nations-govern-the-internet/.
47. The White House, ''Statement by the President on the Cybersecurity Framework,'' February 12, 2014, http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework.
48. Stephen Kotkin, ''How Murdoch Got Lost in China,'' *The New York Times*, May 4, 2008, http://www.nytimes.com/2008/05/04/business/ media/04shelf.html?_r=0.
49. Freedom Online Coalition formed in 2011 in The Hague, The Netherlands. The coalition has grown from 15 to 23 member countries, http://www.freedomonline.ee/about-us/Freedom-online-coalition.
50. NetMundial, ''NetMundial Multi-Stakeholder Statement,'' April 24, 2014, http://netmundial.org/netmundial-multistakeholder-statement/.
51. United Nations General Assembly, Human Rights Council Twentieth Session, ''The Promotion, Protection and Enjoyment of Human Rights on the Internet'' (A/HRC/20/L.13), June 29, 2012. Office of the High Commissioner for Human Rights, http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403231_text.
52. Including the International Covenants on Civil and Political Rights and Economic, Social and Cultural Rights, and the Convention on the Rights of Persons with Disabilities.
53. Luke Bainbridge, ''How Social Media Gives New Voice to Brazil's Protest,'' *The Guardian*, April 26, 2014, http://www.theguardian.com/ world/2014/apr/27/social-media-gives-new-voice-to-brazil-protests.
54. Frank Bajak, ''Venezeula Cuts off Internet, Blocks Communications for Protestors,'' *The Huffington Post*, February 21, 2014, http://www.huffingtonpost.com/2014/02/21/venezuela-internet_n_4832505.html.
55. Henry Farrell, ''Five Questions about the European Court of Justice's Google Decision,'' *The Washington Post*, May 14, 2014, http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/05/14/five-key-questions-about-the-european-court-of-justices-google-decision/.
56. The White House, Presidential Policy Directive 28, ''Signals Intelligence Activities,'' January 17, 2014, http://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf.
57. Warwick Ashford, ''Most NSA Spy Data Relates to Innocent Internet Users, Report Shows,'' ComputerWeekly.com, July 7, 2014, http://www.computerweekly.com/news/2240223999/Most-NSA-spy-datarelates-to-innocent-internet-users-report-shows.
58. Ilya Khrennikov and Anastasia Ustinova, ''Putin's Next Invasion, the Russian Web,'' *Business Week*, May 1, 2014, http://www.businessweek.com/articles/2014-05-01/russia-moves-toward-china-style-internet-censorship.
59. Ellen Nakashima, ''Microsoft Fights U.S. Search Warrant for Customer E-Mails Held in Overseas Server,'' *The Washington Post,* June 10, 2014, http://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416aef0a7-11e3-914c-1fbd0614e2d4_story.html.
60. On July 31, 2014, Judge Loretta A. Preska of the United States District Court for the Southern District of New York upheld the position of The United States Government. However, the Court granted a stay of its decision pending appeal to enable Microsoft to appeal. See Joseph Falcone, *US Federal Court Orders Microsoft to Produce E-Mail Content Stored Outside the United States* (New York: Herbert Smith Freehills LLP, 2014).
61. Wyane Williams, ''China Brands Windows 8 a Threat to Its National Security,'' Beta News, June 5, 2014, http://betanews.com/2014/06/05/china-brands-windows-8-a-threat-to-its-national-security/.
62. Robert Frost, ''The Road Not Taken,'' in *The Poetry of Robert Frost: The Collected Poems, Complete and Unabridged* (New York: Holt, Henry & Company, Inc., 1969).