Spring 3-21-2014

# Moving Beyond Regulatory Mechanisms: A Typology of Internet Control Regimes

Richard Reid Hunt
*Portland State University*

# Moving Beyond Regulatory Mechanisms:

# A Typology of Internet Control Regimes

by

Richard Reid Hunt

A thesis submitted in partial fulfillment of the
requirements for the degree of

Master of Science
in
Political Science

Thesis Committee:
Bruce Gilley, Chair
David Kinsella
Wu-chang Feng

Portland State University
2014

**Abstract**

This paper examines national Internet control from a policy regime perspective. The mechanisms through which governments attempt to control the Internet may be developed and implemented by different institutions and agencies, or fall outside of a formal regulatory structure entirely. As such, the totality of the institutions and practices of national Internet control is better conceptualized not as a regulatory regime, but as a control regime. After a survey of the critical policy and control dimensions, a six-part typology of control regimes is proposed. The purpose of this study and typology is exploratory. With comparative research about Internet control regimes at a relatively early stage, this paper aims to enable the formation of concepts and hypotheses about the interrelationship, or co-presence, of key distinguishing variables in different Internet control regimes.

## Table of Contents


Abstract i

List of Tables v

List of Abbreviations vi

I. Chapter One: Internet Policy Primer 1

A. Introduction 1

B. Internet Regulatory Regimes 4

C. Internet Control Regimes 8

D. Research Question and Argument 12

E. Study Outline 13

II. Chapter Two: Methodology for Analysis 14

A. Review of Existing Analysis 14

B. Typological Approach 16

a. Descriptive vs. Explanatory 18

b. Analysis of Similar Typologies 21

C. Typology Dimensions 25

a. Ideas 25

1. Governing regime type 26

2. Regulatory paradigm 28

3. ICT development goals 30

4. Norms 32

b. Internet Penetration 33

c. Institutional Arrangement 36

1. Access 37

2. Functionality 39

3. Activity 42

i. Enforcement at the source 43

ii. Filtering 47
iii. Surveillance 49
iv. National information shaping strategies 52
d. Interests 53
e. International Factors 55
f. Incidents 57
D. Methodology Summary 58
III. Chapter Three: Typology Categories 62
A. Cuban, Chinese, and Russian Models 62
a. Cuban Model 64
b. Chinese Model 67
c. Russian Model 72
B. Developmental Model 77
a. ICT and Development 80
b. Control Mechanisms 83
C. United States Model 85
a. Regulatory Backdrop 86
b. Key Interests 91
c. Functionality control 93
d. Surveillance 96
D. European Model 97
a. Regional Policy 98
b. National Policy 105
c. Surveillance 108
d. Key Interests 111
IV. Chapter Four: Conclusion 114
A. Research Summary 114

B. Research Significance, Limitations, and Analysis 117

C. Opportunities for Further Research 119

V. References 121

VI. Appendix: Freedom on the Net vs. Freedom in the World Scores 152

## List of Tables


| | |
|---|---|
| 2.1: Typology of Democratic Regimes | 17 |
| 2.2: Goal of Typology | 18 |
| 2.3: Mearsheimer's Tragedy of Great Power Politics | 19 |
| 2.4: Four Rationals of the Mass Media | 22 |
| 2.5: Regulatory Paradigms | 27 |
| 2.6: ICT Development Goals | 30 |
| 3.1: Typology of Internet Control Policy Regimes | 58-59 |

## Abbreviations

ACTA — Anti-Counterfeiting Trade Agreement

AOL — America Online

ASEAN — Association of South East Asian Nations

BGP — Border Gateway Protocol

BPO — Business-Process Outsourcing

CALEA — Communications Assistance for Law Enforcement Act [United States]

CCP — Chinese Communist Party [China]

CIA — Central Intelligence Agency [United States]

CIS — Commonwealth of Independent States

CNNIC — China Internet Network Information Center [China]

COICA — Combating Online Infringement and Counterfeits Act [United States]

DDOS – Distributed Denial of Service Attack

DPD — Data Protection Directive [European Union]

DRD — Data Retention Directive [European Union]

DNS — Domain Name System

DNSSEC — Domain Name System Security Extensions

DSC — Digital State Capacity

DSL — Digital Subscriber Line

ECD — Electronic Commerce Directive [European Union]

ECJ — European Court of Justice

ENISA — Agency for Network and Information Security [European Union]

FDI — Foreign Direct Investment

GATS — General Agreement on Trade in Services

GDP — Gross Domestic Product

GDPR — General Data Protection Regulation [European Union]

ICANN — Internet Corporation for Assigned Names and Numbers

ICI — Information and Communications Infrastructure

ICP — Internet Content Provider

ICT — Information Communication Technology

IGO — Intergovernmental Organization

INHOPE — International Association of Internet Hotlines

INTCEN — European Union Intelligence Analysis Centre [European Union]

ISO — International Organization for Standardization

IP — Internet Protocol

ISP – Internet Service Provider

IT — Information Technology

ITU –International Telecommunications Union

LLDCs — Landlocked Developing Countries

MII — Ministry of Information Industry [China]

MIT — Massachusetts Institute of Technology

NAFTA — North American Free Trade Agreement

NIST — National Institute of Standards and Technology [United States]

NSA — National Security Agency [United States]

NSP — Network Service Provider

NTIA — National Telecommunications and Information Administration [United States]

OECD — Organisation for Economic Co-operation and Development

ONI — OpenNet Initiative

OSP — Online Service Provider

PIPA — Protect Intellectual Property Act [United States]

RIAA — Recording Industry Association of America

SIGINT — Signals Intelligence

SOPA — Stop Online Piracy Act [United States]

TCP — Transmission Control Protocol

TIA — Tunisian Internet Agency [Tunisia]

TRIPS — Trade Related Aspects of Intellectual Property Rights

UDP — User Datagram Protocol

UN — United Nations

UNCITRAL — United Nations Commission on International Trade Law

URL — Universal Resources Locator

WAP — Wireless Application Protocol

WB – World Bank

WGIG — Working Group on Internet Governance

WIPO — World Intellectual Property Organization

WSIS — World Summit on the Information Society

WTO – World Trade Organization

WiMAX — Worldwide Interoperability for Microwave Access

3G — Third Generation [Mobile telecommunications technology]

4G — Fourth Generation [Mobile telecommunications technology]

# Chapter One

## Internet Policy Primer

### Introduction

All of the major works on state control of the Internet—including Lessig's *Code and Other Laws of Cyberspace* (1999), Kalathil and Boas' *Open Networks, Closed Regimes* (2003), Goldsmith & Wu's *Who Controls the Internet* (2006), and Deibert's *Access* series (2008; 2010; 2011)—open with a now-familiar narrative: In the early 1990s, the expansion of the Internet was widely perceived as a threat to the nation-state status quo. The full potential and commercial applicability of the technology was still unknown, of course, but prominent policy makers and tech pundits agreed that this network-of-networks would soon facilitate the circumvention of traditional barriers of distance and borders, while the technology's decentralized architecture—a labyrinthine web of channels and routers—would place the medium outside the reach of any one state's direct control.[1]

Skeptical readers might question the pervasiveness of this ostensibly "conventional" wisdom. Did a majority—or even a slight plurality—of pundits and policy makers in the 1990s *really* believe that the Internet could function outside of the regulatory reach of national governments? Or have rhetorical framing devices and cherry-picked quotes simply been reproduced enough times to lend credence to a faulty premise?[2]

Upon closer examination, aspects of this narrative do seem misleading given the diversity of arguments and policy positions in circulation. Still, variations of the "ungovernable" claim were quite common and clearly permeated the policy dialogue.[3] Prominent

[1] The term *Internet* first appeared in 1974 in reference to a technology that connected numerous networks using an Internet protocol communication suite. Protocol here refers to the process through which computers transfer bits of information over networked wires, and Internet Protocol (IP) and Transmission Control Protocol (TCP) were the first networking protocols defined in this standard. By the early 1990s, the term Internet became shorthand for all computer networking activities (Schulte, 2013, p. 3).

[2] In the wake of the Arab Spring, for instance, Malcolm Gladwell (2010, Oct. 4; 2011, Feb. 2) and other prominent authors published articles swatting down maximalist claims about Twitter toppling dictators. But the pollyanna arguments Gladwell and others engaged with were largely unattributed, and its doubtful that many observers really believed that Twitter *caused* the Arab Spring or similar uprisings. See Rosen (2011) for other examples.

[3] See Johnson and Post (1995) and Shields (1996).

international relations theorists, economists, and cyber-enthusiasts agreed that the Internet would amplify the disruptive effects of globalization on international regulatory regimes.[4] Some Silicon Valley ideologues went a step further, arguing that the Internet was the vanguard technology of a coming wave of social and economic change that would crash against the borders of national governments and smash the chains that tethered humanity to territorial rule.[5]

"The Internet cannot be regulated," MIT Media Lab founder Nicholas Negroponte famously pronounced. "It's not that the laws aren't relevant, it's that the nation-state is not relevant. Cyberlaw is, by nature, global and we're not very good at global law" (Higgins & Azhar, 1996, Feb. 5, p. 9).[6]

Negroponte could not have been more mistaken. Drezner (2008), Goldsmith and Wu (2006), and other authors have detailed the extent to which great power states (and the private interests they represent) are the *primary* actors in the global governance of the Internet—although the terms "global governance" and "global law" are themselves misleading as they underemphasize the extent to which national law and less formalized control mechanisms linked to national governments are the most fundamental controls on Internet access, activity, and functionality.

While Negroponte's statement and similar claims were obviously incorrect, it is true that the era of self-regulated, "open Internet" did persist from the technology's development in the 1960s until the dot-com tech boom in the late 1990s (Palfrey, 2010).[7] But policy makers' hands-off approach during this period ultimately reflected a lack of

[4] *The Economist's* Frances Cairncross articulated the globalization argument in her book The *Death of Distance* (2000): "Government jurisdictions are geographic. The Internet knows few boundaries. The clash between the two will reduce what individual countries can do. Government sovereignty, already eroded by forces such as trade liberalization, will diminish further" (p. 177, quoted in Drezner, 2007, p. 93).

[5] See Barbrook and Cameron (1996) for a summary and critique of this perspective, which the authors famously refer to as the "Californian ideology."

[6] Negroponte's *Being Digital* (1996) is one of the ur-texts of cyberutopianism.

[7] Nearly every aspect of the Internet's development occurred under the auspices of the US government and state-funded universities. But US authorities were largely passive custodians for several decades as the Internet expanded from a series of connected intranets to a commercialized "information superhighway" (Goldsmith & Wu, 2006; Eko, 2012).

interest rather than a lack of means. By the end of the decade, states around the globe had begun asserting control of the technology by enacting laws aimed at regulating the segments of the Internet within their domestic borders, or at least staking a claim that these critical parts of the network were within the ambit of their legal jurisdiction. National governments—democratic and authoritarian—worked in coordination with private tech companies to erect a variety of information and e-commerce controls, and the view that cyberspace was beyond the reach of real-space regulation faded (Palfrey, 2010; Lessig, 2006).

No incident better symbolized this shift than Bill Clinton's visit to an Internet café in Shanghai in 1998. After speaking with the young and enthusiastic clientele, the President joked to reporters that China's efforts to "crack down" on the Internet would be like "trying to nail Jell-O to the wall"—a prediction that proved widely off-the-mark (Goldsmith & Wu, 2006, p. 90). Only months after Clinton's off-the-cuff remarks, the Chinese government criminally prosecuted three prominent democracy activists for their *online* efforts to organize an opposition political party—the "China Democracy Party," which one of the activists had tried to register officially in the wake of Clinton's visit (Rosenthal, 1998, Dec. 19, p. 5). That same year, the government initiated the so-called Great Firewall project, a global Internet filtering system developed over the next five years for a staggering estimated cost of $160 million (The Economist, 2013a, April 6; Hagestad II, 2012, p. 253).

The mechanisms governments employed to regulate and control the Internet reflected diverse policy goals and varying levels of enforcement capability. This chapter describes the emergence and function of *Internet regulatory regimes*, which are generally—but not exclusively—focused on the economic aspects of the Internet at the national level.[8] Internet regulation at the international level also covers economic and develop-

[8] The term *regulation* generally describes an array of public policies explicitly designed to govern economic activity and its consequences at the level of the industry, firm, or individual unit of activity (Eisner, 2000, pp. 5-6).

mental issues, as well as more functional aspects of the technology. The chapter then examines *Internet control regimes*, a term Zheng (2008) uses in reference to the government agencies and policy mechanisms that function to control Internet access and activity for political and social reasons, and Yang (2009) uses more broadly in reference to the totality of the institutions and practices of Internet control, including the regulatory regime framework. After explaining why the latter use of the term is more appropriate for comparative analysis, the final section of this chapter identifies the paper's central research question and argument, and outlines the structure of the following chapters.

**Internet Regulatory Regimes**

In the social sciences, the term *regime* generally refers to governmental systems and the institutional frameworks that establish their legal and administrative parameters (Eko, 2012, p. 34). While the term is occasionally applied to an entire governing system,[9] it is more accurate—and more practical—to use the term with reference to a specific policy area. Policy regimes are anchored within a specific institutional structure encompassing both formal rules and decision-making procedures and informal rules of action based on shared principles, norms, and beliefs. The policy regime analytical framework developed as a variation of regime theory geared towards policy formulation and implementation at the national level (Wilson, 2000). This framework is especially useful for analyzing Internet policy, as it allows us to identify explicit links between policy makers, policy, and mechanisms of control.

Internet policy is often presented as a *regulatory regime*. Internet regulatory regimes at both the national and international level are focused on the economic implications and applications of the Internet and related Information and Communication Technology (ICT),[10] although the regulatory framework also captures intervention on behalf of

[9] As political columnist William Safire (2007) famously summarized, "a *regime* is a government you don't like" (p. 298).

[10] The term *Information and Communications Technology* (ICT) refers to all technologies and devices used in managing and processing information systems. ICT is a critical social and economic concept, as it is considered one of the three major technological breakthroughs—alongside steam power and electricity—of the

the "public interest"—a concept subject to varying interpretations. The emergence of the Internet as a commercial platform disrupted existing regulatory models and mandates that had traditionally distinguished media policy from telecommunications policy. The former developed as a means to shape the conduct and content of the mass media (namely, the press and broadcasting outlets) as media of *public* communication. Telecommunications policy, in contrast, was perceived as a more technical policy field concerning the inter-state communication between *individuals* by technological means—i.e. radio, telephone, wire, cable, and satellite (Psychogiopoulou & Anagnostou, 2012; Freedman, 2008).

The browsable format of the Internet that has existed for slightly more than two decades muddles this distinction by placing press and broadcast content on a telecommunications platform alongside a variety of independent and user-generated content, and its integration across economic sectors invites further policy interventions from a variety of political, economic, social, and cultural actors and interests (Psychogiopoulou & Anagnostou, 2012; Freedman, 2008).[11] Furthermore, the digital data flowing across the Internet is no longer just web text and relatively small packet exchanges; it now includes massive *Big Data* bundles of financial transaction data and mobile communications.[12] An oft-cited McKinsey Global Institute report notes that Big Data has become integrated into nearly every industry and business function, and is now as important a factor of production as labor and capital (Manyika, Chui, Brown, Bughin, Dobbs, Roxburgh, & Byers, 2011).[13]

modern era (Edquist & Henrekson, 2006). For the purposes of this paper, its important to understand that ICT's most important contemporary function is serving as the physical conduit of digital data. Although at one time ICT was weighed equally between analogue and digital technology, today nearly all information is transmitted digitally. This digital revolution began with the adoption and proliferation of digital computers and digital record keeping, and effectively amplified the transformative power of the ICT revolution (Küng, Picard, & Towse, 2008, p. 3).

[11] The application most commonly associated with the Internet is the *World Wide Web*, a site-linking hypertext system developed in 1991. But the World Wide Web should not be considered synonymous with the Internet—it is simply one application that operates using the network. Other Internet-enabled software includes email, file transfer protocol, and a variety of peer-to-peer file sharing programs (Solum, 2009, pp. 48-49).

[12] The MGI report defines Big Data as datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze (Manyika & Chui, 2011, p. 1).

[13] MGI estimates that, by 2009, nearly all sectors in the US economy had at least an average of 200 terabytes of stored data per company with more than 1,000 employees. 200 terabytes is more than twice the

Internet regulatory policy is thus reflective of the technology's dual functional role as content platform and digital data distribution system.

The three commonly identified models of national Internet regulation are not dissimilar from other public policy regulatory approaches: a "command-and-control" or state model, in which public authorities make the rules, enforce them, and punish those who breach them; a self-regulation model, in which private sector actors largely make the rules and implement them collectively without any public intervention; and a co-regulation model, in which policy drafting, implementation, and enforcement are spread between a number of public and private actors, but initiated and overseen by the state (Kleinsteuber, 2004; Frydman, Hennebel, & Lewkowicz, 2012). Although this framework presents a useful starting point for Internet policy regime analysis, it is at once too broad in application, as the United States, European Union member states, and various developmental countries utilize regulatory approaches that can be characterized as co-regulatory, and too narrow in conceptual scope, as laws and regulations are only as effective as a government's capability to enforce them. For the purposes of comparative analysis, a country's regulatory approach is better conceptualized as a policy backdrop against which diverse control mechanisms operate rather than a policy blueprint that dictates the mechanisms application.

The effectiveness of any of these regulatory models varies from country-to-country and from activity-to-activity. National regulation of the Internet generally works well when the regulated activity is well defined in existing law and all of the parties to the regulated activity are identifiable and located within the physical territory of the nation-state. Published content on the web, for example, is subject to laws on defamation. Internet fraud is subject to criminal sanction. And peer-to-peer file sharing of copyrighted material subjects users to civil or criminal liability. With regard to these examples and more complicated e-commerce issues, the role of national law is critical even if its pres-

---

size of US retailer Wal-Mart's data warehouse in 1999 (Manyika & Chui &, 2011).

ence is often taken for granted. But national regulation of the Internet is inherently costly and ineffective when the object of regulation is either content that originates outside of national boundaries or the architecture of the Internet itself. These two regulatory issues are sometimes related, as regulation of architecture may be a means to more effective regulation of content (Solum, 2009, pp. 68-69, 75).

Internet regulation at the international level—often referred to as *Internet governance*—has proven just as complicated and problematic as national regulation, due in large part to states' differing levels of economic and telecommunications infrastructure development, and widely varying perspectives on which contentious speech and content issues merit government intervention on behalf of public interest claims. What international regulation exists consists of an assortment of UN resolutions, conventions, and treaties to which most of the countries of the world agree, either as individual nations or within the framework of regional economic or political groupings. International regulation of the Internet primarily covers electronic commerce and electronic signatures, intellectual property, and child pornography (Eko, 2001; Eko, 2008).

This rather narrow range of issues underscores the primacy of national law in Internet policy development with one important exception: the Domain Name System (DNS), which translates easily memorized domain names (e.g. nytimes.com, wikipedia.org, pdx.edu) to route-specific numerical IP addresses. By providing a global distributed keyword-based redirection service, the DNS is a critical component of the functionality of the Internet. But even this supposedly global system is decidedly national: "root authority" for DNS administration rests with the Internet Corporation for Assigned Names and Numbers (ICANN), a California-based nonprofit organization under contract to the US Commerce Department and overseen by the United States government. Other global governance bodies, including the World Summit on the Information Society (WSIS) and the Working Group on Internet Governance (WGIG), are also involved in functional Internet issues, but their role is more marginal.

**Internet Control Regimes**

While most national Internet policy can be characterized as regulatory in that it addresses e-commerce, technological development and harmonization, and public interest issues through familiar policy making procedures, other important aspects of Internet control operate outside of a formal regulatory framework. Case studies of Internet policy under authoritarian regimes are clearly capturing control mechanisms that occur at arm's length from the government to assure plausible deniability. Such mechanisms include harassment and violence against online reporters and activists, sophisticated online propaganda efforts on behalf of political parties and actors, and coordinated denial of service attacks against particular websites and servers.

Other non-regulatory mechanisms reflect the intervention of different government agencies into the Internet policy process. Extensive surveillance programs have been created under the purview of law enforcement and state security agencies in both democratic and authoritarian regimes that allow government actors extensive access into users' digital communications. While some of these surveillance activities are integrated into regulatory policy (such as mandates that Internet service providers retain browsing records), other aspects of surveillance are covert (such as signals intelligence operations) and effectively ancillary to formal regulatory efforts. For the purposes of Internet policy analysis, what matters is the degree to which surveillance programs grant the government "control" over the technology, not whether the policy objectives of the programs are perceived as positive (monitoring of a human trafficking ring) or negative (interception of messages between environmental activists).

Eriksson and Giacomello (2009) note that the concept of control is not only associated with general notions such as "governance," "influence," and "authority," but is also "distinctively linked to the law and technology, including the methods and means of governing the performance of any apparatus, machine, or system" (p. 206, footnote 2). This usage of control in the term's operative sense captures *all* of the mechanisms of technical

control. But some analyses of Internet control focus more narrowly on government and private actor intervention into the *social* and *political* dimensions of the technology. Control in this context does not exclude more nuts-and-bolts regulatory issues, but the focus is more on the policy *aims* of different actors vis-à-vis the particular Internet activity or development issue being targeted. Yang (2009) and Eko (2012), for example, contextualize Internet control policy as an aspect of *governmentality*—the cultural and social context out of which modes of governance arise and by which they are sustained. Many regulatory policies do fall within this conception—especially those reflecting public interest claims or state security goals—but control in this context also captures informal and extralegal mechanisms operating outside of normal regulatory parameters.[14]

Warf (2013) notes that because the state is not a "monolithic entity but composed of diverse agencies, sometimes working at cross-purposes," it is more instructive to think of Internet control efforts in terms of "multiple, sometimes contradictory authorities that invoke diverse strategies of suppression of various groups and individuals for a broad array of reasons and motivations" (p. 47). Although not all control efforts should be characterized as suppressive, the recognition that multiple agencies and stakeholders are involved in the policy making process is important. Zheng's 2007 book *Technological Empowerment: The Internet, State, and Society in China* details how the inherent contradictions in the Chinese government's approach to the Internet have produced two distinct Internet policy regimes: an Internet *regulatory* regime and an Internet *control* regime. The regulatory regime represents policies developed by the Ministry of Information Industry and the China Internet Network Information Center to facilitate the development of the Internet while managing its growth and profitability. The control regime represents policies developed by the Central Propaganda Department and State Council Information Office to limit content access and squelch political discourse (Zheng, 2008, pp. 49-50).

[14] "Control" in this usage has a distinctly negative connotation—much more so than "regulation," a concept generally supported by the public and associated with positive policy outcomes.

The tension between these two regimes produces conflicts of interest among different state agencies, and inefficiencies in enforcing hard and soft forms of control. For the moment, the control regime maintains the upper hand through its strategic use of coercive measures. Recent evidence, however, suggests that control regime efforts may be slowing Internet traffic and hindering the use of cloud-computing services. This architectural flaw will eventually reduce China's global competitiveness in e-commerce, which could cause a shift in the dynamic between the regulatory and control regimes (The Economist, 2013b, April 6; Mozur & Tejada, 2013, Feb. 13).[15]

Zheng's work is narrowly focused on China, but the policy dichotomy he identifies is not unique to the country, or even to a particular governing regime type. Whether the case is the United Arab Emirates or the United States, there is ample evidence that the diverse mechanisms of control employed by different government agencies represent divergent and even conflicting policy objectives. In Europe, for example, the EU Data Protection Directive imposes strict data privacy requirements on software and Internet companies, while the EU Data Retention Directive obliges all Internet service providers to retain users' browsing data for future access by law enforcement.

The diversity of Internet policy objectives necessitates a broad Internet policy regime analytical framework. It is important to recognize that even when regulation and control efforts reflect divergent policy goals, they rely upon many of the same mechanisms for execution and enforcement. Filtering technology that blocks access to websites hosting child pornography—a form of content illegal in nearly every jurisdiction—may also be used to block human rights websites, and surveillance systems established by state security agencies to intercept messages between terrorist cells may also capture communications between civil society groups. The regulatory regime / control regime division is further muddled by the subjective normative context of public interest Internet policy. What appears to be an egregious and illegitimate form of content "control" in

[15] The latter observation is my own.

one country or region may be a perfectly acceptable form of regulation in another. In the United States the conception of the Internet as a marketplace of ideas suggests a standard that—except in very limited circumstances—the government may not regulate online "speech" on the basis of its subject matter or viewpoint. In Europe, however, online speech restrictions are much more common and generally supported by the public. France and Germany both restrict online content labeled as "hate speech."

While Zheng (2007) identifies a clear division between the regulatory and control regimes in China, Yang (2009) defines the country's Internet control regime as the "totality of the institutions and practices of Internet control" (p. 47). While the author's usage of "control" in this particular analysis is intended to reflect governmentality, the passage effectively captures the broader notion of control identified by Eriksson and Giacomello (2009), and tracks closely with Wand's (2012) concept of Digital State Capacity (DSC), which refers to the ability of the state to manage and control digital information within its jurisdiction.

Employing a broad Internet control regime definition that includes all relevant control mechanisms—including those within the regulatory framework—is the best way to fully capture a government's ability to manage, regulate, and otherwise manipulate the technology towards particular policy goals. National-level Internet control regimes, then, comprise the totality of national institutions and practices of Internet control, including the regulatory policies and mechanisms which promote e-commerce development and allow for government intervention in widely agreed upon law enforcement and public interest areas (e.g. child pornography, counterterrorism, and identity theft), as well as the policies and mechanisms which allow for contested and possibly extralegal intervention into online social and political activities.

Using this broad control definition allows for a more effective comparative approach. The annual country-level "Internet Freedom" reports from Reporters Without Borders, the OpenNet Initiative, the Open Society Foundation, and Freedom House all

differ in their respective methodological and descriptive approaches, and the book length policy literature also lacks a consistent analytical framework. Case studies of Internet policy under authoritarian governing regimes tend to focus on examples of content filtering and repressive actions against activists. Case studies of Internet policy in the United States and Europe tend to focus more on copyright protection and development issues—although that focus has shifted of late following revelations about the surveillance capacity of the National Security Agency. Many accounts across regime type tend to lump mechanisms that control access *to* the Internet in with mechanisms that control activity *on* the Internet, including filtering, surveillance, and enforcement at the source. By focusing on *all* relevant aspects of control, we can more accurately categorize mechanisms common to both authoritarian and democratic governing regimes, while positioning them within a standardized analytical framework.

**Research Question and Argument**

The research question for this paper is as follows: What are the different Internet control regimes at the national level and how are they different? Several corollary questions then emerge: (a) What does "control" of the Internet constitute and what are the technical mechanisms through which it can be achieved; (b) What are the variations in the strategic and administrative aspects of Internet control; (c) Why do different governments adopt particular control regimes; and (d) What are the results, limitations, and unintended consequences of control efforts?

I argue that the wide range of Internet control regimes can best be classified using a six-part typology based on dimensions derived from standard comparative public policy analysis broadly, and from Internet policy and policy regime literature more specifically. I identify several key distinguishing variables, including governing regime-type, institutional arrangement, and institutional capacity.

**Study Outline**

This paper proceeds as follows: Chapter Two details existing approaches to comparative Internet policy analysis, explains why a typological approach is best for identifying and distinguishing Internet control regimes, and outlines the typology dimensions, which are derived from public policy literature. Chapter Three lays out the six typology categories: Cuban model, Chinese model, Russian model, Developmental model, United States model, and European model. Finally, Chapter Four provides an overview of the research, explains its significance, and identifies opportunities for future research.

# Chapter Two

## Methodology for Analysis

### Review of Existing Analysis

The bulk of Internet policy analysis takes a comparative approach that examines particular censorship and control techniques on a country-by-country basis. Although these profiles are often compiled in larger reports that identify emergent trends, they do not specify or group countries by Internet policy type, as that concept remains largely undefined in these works. Rather, countries are organized along an axial "more-or-less free" scale based on basic and observable standards of free expression and evidence of filtering and censorship. Reporters Without Borders, the OpenNet Initiative, the Open Society Foundation, and Freedom House all put out annual country and region reports related to "Internet freedom" that outline and document censorship policies and practices. These reports all slightly differ in methodological and descriptive approaches. The OpenNet Initiative reports are perhaps the most detailed, especially on issues of ICT architecture and specific censorship techniques—e.g. filtering and IP redirects. Freedom House's *Freedom on the Net* reports are the best known and most cited, and the methodology employed is quite similar to that used for the organization's annual *Freedom of the World* report.[1]

The *Freedom of the Net* report examines the level of Internet freedom through a set of questions and accompanying subpoints, which are organized into three groupings: obstacles to access, limits on content, and violations of user rights. Through a careful reading of country profiles and scoring one can ascertain that countries receiving similar total scores may be using substantially different control techniques. For example, Myanmar (total score of 75 out of 100) has an extremely low rate of Internet penetration (1 percent) owing to an underdeveloped telecommunications infrastructure. The military regime is thus able to control the Internet largely through limiting access (*obstacles to*

[1] Freedom of the World assigns countries political rights and civil liberties scores rather than regime-type designations (beyond the ordinal Free / Partly Free / Not Free labels).

*access* score of 20 out of 25). Saudi Arabia (total score 70 out of 100) has relatively high levels of Internet penetration (54 percent), especially in urban areas. The government thus controls Internet content primarily through a sophisticated filtering system (*limits on content* score of 24 out of 40) and harsh laws on libel and defamation (*violation of user rights* score of 32 out of 40).

Some authors have attempted to categorize the mechanisms governments use to control digital content, and then identify states most associated with particular censorship and surveillance trends. Deibert (2010), for instance, identifies and defines three generations of controls, with each progression representing both shifting policy goals and technological advances. First-generation controls focused on denying access to particular Internet data through the use of filtering technology that blocks access to servers, domains, keywords, and IP addresses. This stage was led by states such as China and Saudi Arabia, but specific filtering practices and policies varied widely, even within the same regions. The second-generation controls aimed to create legal and normative environments and technical capabilities that would enable state actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery. China was again a leading actor in this phase, but some of the covert technical mechanisms that characterize the second-generation controls were especially pronounced in Kyrgyzstan, Tajikistan, and other former Soviet republics in the run ups to elections and during demonstrations. The third-generation of controls represent a shift from reactive to proactive policy, and involves the construction of state actor capabilities for competing in informational space with potential adversaries and competitors. The leader here is not China but Russia, where filtering is largely non-existent but sophisticated information shaping strategies expand the state's ability to manipulate and control cyberspace.

Another recent approach could be labeled *schematic.* Zittrain (2003), for example, considers the Internet as a delivery chain, with control mechanisms and policies designed specifically for different points along the route, and Ziccardi (2012) considers Internet fil-

tering policies at different nodes along the Internet's physical architecture. The schematic approach is especially useful for looking at censorship approaches within a hardware and tech capacity context. However, it has some clear drawbacks for policy analysis. The two polar ends of the digital content distribution chain—producer and recipient—are generally addressed by the same grouping of control policies, while a single, broad policy such as surveillance may be applicable at different stages along the chain.

Third and finally, there is a *regulatory* approach that focuses on how and to what extent Internet controls are located within a larger regulatory environment. This approach is especially important as it integrates policy paradigms and policy maker motivations, and outlines the role of regulators—the public or private bodies capable of influencing the behaviors of actors. Frydman, Hennebel, and Lewkowicz (2012) detail the command-and-control and self-regulation models, and build upon Zittrain's (2003) framework to identify co-regulatory mechanisms—the legal devices designed by both public and private players to put pressure on the points of control to achieve some regulatory result.

**Typological approach**

The wide range of Internet control regimes can best be classified using a typological approach. A typology is a useful technique for (a) classifying complex phenomena without oversimplifying, (b) clarifying similarities and differences among cases to facilitate comparison, and (c) incorporating interactive effects. Typologies generally (d) provide a comprehensive inventory of all possible kinds of cases, and (e) draw attention to "empty cells" or kinds of cases that have not occurred and perhaps cannot do so, although as I discuss ahead, neither of these functions may be present in particular typologies (Bailey, 1994).

Typologies should be understood as organized systems of types. Scholars sometimes refer to their analytic typology categories as "ideal types" to signify that these categories are broad abstractions that may not consistently serve to classify empirical cases.

The ideal type concept is closely associated with Weber—although Bailey (1994) notes the sociologist's usage of the term is often misunderstood and thus misapplied. Examples of ideal type typology categories are found in the writings of Schmitter (1974), Luebbert (1991), and Hall and Soskice (2001). In all of these studies, the authors proceed to classify empirical cases within their identified abstract categories.[2] Collier, LaPorte, and Seawright (2008, pp. 161-162) suggest that international relations scholars often frame their typological cases as ideal types in recognition that cases—often states or governing regimes—grouped together under any one category usually cannot be understood as being perfectly equal. Rather, the "claim is that they do indeed fit in a particular category, and not in another. The resolution here may be a simple recognition that categorization entails a process of abstraction" (p. 162).

The proposed typology outlined in this paper is not intended to exhaustively capture and exclusively categorize every country's respective Internet control regime configuration. Rather, the goal is to identify the most common *and* most prominent control regime types. The typology identifies groupings of countries exhibiting densely linked shared characteristics and presents them as "models"—effectively ideal types. Several of the models use a label derived from an exemplary empirical case (Cuban model, Chinese model, Russian model, United States model), while two others use less country-specific labels (developmental model and European model) to indicate that no one country exhibits clarity across all relevant dimensions. These category types would thus appear to straddle the line between criterion types and constructed types. The former possess all of the relevant features or dimensions of the type *and* exhibit extreme clarity on all features. The latter is generally not an extreme or accentuated form of the type, but rather a more common or central empirical form analogous to a measure of central tendency (Bailey,

[2] In Luebbert's (1991) analysis of political-economic regimes in interwar Europe, for instance, the author states although it is "seldom difficult to locate interwar European societies [among his identified regime types]," "the extent to which the societies corresponded to the idealized model of the regime varied" (p. 3).

| Elite Behavior | Structure of Society | |
|---|---|---|
| | ***Homogoneous*** | ***Plural*** |
| *Coalescent* | Depoliticized democracy | Consociational democracy |
| *Adversarial* | Centripetal democracy | Centrifugal democracy |

**Table 2.1:** Typology of Democratic Regimes (Liphart 1977, p. 107, taken from Caramani, 2008, p. 89.)

1994, pp. 19-23).[3] However, the exemplary cases in the country-label category types do not necessarily display "extreme clarity" on *all* features, although they do exhibit pronounced accentuation on the distinguishing dimensions. More importantly, they are also "models"—or prototypes—in the sense that other countries within the respective grouping mimic or adopt their control (and development) techniques. The constructed type label is thus more accurate. The United States model would appear to be an exception, as the category type applies to only one country. However, as I explain, the unique characteristics of the US model may eventually be embraced by other countries, and the label could eventually capture a grouping of countries.

The dimensions for my typology are drawn from *policy regime* literature (especially Wilson (2000)) and from relevant Internet policy analysis (especially Eriksson & Giacomello (2009), Wand (2012), and Deibert (2008; 2010; 2011)). Categories were selected after careful reading of country profiles from Freedom House, the OpenNet Initiative, and other organizations and publications. The typology draws from and refines Eko's (2001; 2008) Internet regulatory typology—discussed ahead in greater detail—which is largely based on a single (albeit multifaceted) dimension of *governmentality.*

**Descriptive vs. Explanatory.** Typologies generally take one of two forms: descriptive or explanatory. Descriptive typologies identify the attributes that comprise a particular type and serve to distinguish one type from another. Gerring (2011) identifies

[3] All empirical cases are expected to deviate to some extend from the constructed type.

| | Descriptive | Classificatory | Explanatory |
|---|---|---|---|
| **Analytical Move(s)** | Define compound concepts (types) to as descriptive characterizations. | Assign cases to types. | Make predictions based on combinations of different values of a theory's variables. Place data in relevant cells for congruence testing and comparisons to determine whether data is consistent with theory. |
| **Question(s) Answered** | What constitutes this type? | What is this a case of? | If my theory is correct, what do I expect to see? Do I see it? |
| **Example** | What is a parliamentary democracy as opposed to a presidential democracy? | Are Britain and Germany parliamentary or presidential democracies? | According to the normative variant of the democratic peace theory, what foreign policy behavior is predicted from a dyad of two mature parliamentary democracies? Do the bilateral foreign policies of Britain and Germany agree with that prediction? |

**Table 2.2:** Goal of Typology (Elman, 2004, p. 97)

several varieties of the descriptive approach. Simple typologies focus on a single dimension that distinguishes variations of a larger concept. For example, polities may be classified in Aristotelian fashion as monarchies (rule of one), oligarchies (rule of few), and democracies (rule of many). In a matrix typology, the typology categories are the product of an intersection of categorical variables. Lijphart's (1977) fourfold typology of democratic regimes (Table 2.1) is a good example of this approach. Other descriptive typology varieties include temporal, taxanomy, configurational, and sequential. Although descriptive typologies serve primarily to describe and categorize types, they may also be associated with the formulation and testing of explanatory claims. The contrasting types contained in a descriptive typology, for instance, may be the outcome to be explained in a given study (Collier, LaPorte, & Seawright, 2008, p. 153).

| | *Exemplar* | *In-regional behavior* | *Extra-regional behavior* |
|---|---|---|---|
| ***Continental great powers*** | Germany | Attempt regional hegemony while balancing against other states. | Unclear. Case studies suggest balance against any would-be regional hegemons. |
| ***Island great powers*** | Great Britain | Balance against any would-be regional hegemons. | Unclear. Case studies suggest balance against any would-be regional hegemons. |
| ***Regional hegemons*** | United States | Balance against other states to maintain regional hegemony. | Balance against any would-be regional hegemons. |

**Table 2.3:** Mearsheimer's The Tragedy of Great Power Politics (from Elman, 2005, p. 309).

Elman (2005) notes that in an explanatory typology, the descriptive function is modified by its theoretical purposes as constituent attributes comprising each type are extracted from the variables of a preexisting theory (Table 2.2). The dimensions of the property space (its rows and columns) reflect alternative values of the theory's independent variables, so each cell is associated with predicted values of the theory's intervening or dependent variables. This effectively changes the descriptive question being answered from "What constitutes this type?" to "If my theory is correct, what do I expect to see?" (pp. 296-298). As an example, Elman uses the explanatory typology implicit in Mearsheimer's (2001) *The Tragedy of Great Power Politics*. As displayed in Table 2.3, the *types* of state in Mearsheimer's implied typology are represented in the rows, and the columns show whether the state is acting in its own or another region. The content of the cells are the states' predicted intra- and extra-regional behavior (Elman, 2005, p. 309).[4]

My proposed typology is decidedly descriptive in that it identifies the compounds of conceptual attributes (the policy regime dimensions) that comprise particular types

[4] Elman (2005) goes on to extend the typology to reach a more complete property space listing, and to demonstrate that Mearsheimer under-specifies the range of structural conditions that great powers can confront.

(Internet control policy regime models). However, because the *Institutional arrangement* dimension of the typology captures the control mechanisms through which particular control regimes are able to exert control, it effectively answers an important "how" question, and thus contains an explanatory element that forms a link between a purely bottom-line descriptive account and a causal mechanism-based explanatory narrative. In addition, because the policy regime analytical framework pulls from both international relations theory and public policy analysis, the boundaries and definitions for particular dimensions are fuzzy.[5] As such, many of the typology's cells (property spaces) are best labeled as *thick* descriptions.

With comparative research about Internet control regimes at a relatively early stage, this typology is intended to enable the formation of concepts and hypotheses about the interrelationship, or co-presence, of key distinguishing variables in different Internet control regimes.

**Analysis of Similar Typologies**. By employing a multidimensional policy regimes framework, I have attempted to expand and improve upon previous media and Internet regulatory typologies—namely Peterson, Schramm, and Siebert's (1956) seminal *Four Theories of the Press* (henceforth FTP) and Eko's (2001; 2008) more recent typology of Internet regulatory regimes. FTP presented a tidy explanatory typology, spelled out in book's subtitle: "The Authoritarian, Libertarian, Social Responsibility and Soviet Communist Concepts of What the Press Should Be and Do." The basic question addressed in the book was *why* do the mass media appear in widely different forms and serve different purposes in different countries? The authors identify several explanatory factors, including the level of economic and technological resources in a country, the degree of urbanization, and social-cultural disposition. But a "more basic reason"—and the book's central organizing claim—is that "the press always takes on the form and coloration of the

[5] Wilson (2000, p. 272) concedes that it is not always clear where state regimes, policy regimes, and sub-policy regimes begin and end.

social and political structures within which it operates. Especially, it reflects the system of social control whereby the relations of individuals are adjusted" (pp. 1-2).

*Four Theories of the Press* (1956) offered a simple, persuasive schema that matched the main categories of Cold War-era political systems and was intelligible within the broader division into First, Second, and Third worlds. Its limitations became apparent, however, as the Cold War concluded, globalization increased, and the clear lines between political systems began to blur. Even as new variants—including "development" and "democratic-participant" (McQuail, 1983)—were added to keep pace with political transformations, the idea that the political and social roots of the printed press should still serve as frame of reference for all mass communication analysis within particular national borders seemed increasingly unpersuasive. Most contemporary references to the work's influence also note its numerous deficiencies. Hardy (2012, p. 12) identifies many of the common critiques of *FTP*, including its ethnocentric perspective, its inconsistent structure, and its problematic assumptions. Hardy argues persuasively that the key failing of the book's approach is that the authors did not empirically analyze relationships between *actual* media structures and social systems. Rather, the focus is on the rationals or theories by which those abstract systems legitimate themselves (Table 2.4). In spite of its global claim, the book provides scant empirical comparative analysis. Only the United States, Britain, France, Germany, and the Soviet Union (Russia) are examined in any detail, while other Western countries, such as Canada and Australia, are barely mentioned. While my ideal type categories do focus on exemplary examples, in most cases a large grouping of similar countries is identified.

Drawing inspiration from Peterson, Schramm, and Siebert's (1956) work, Eko developed a typology of Internet regulatory regimes based on international, regional, and national, political, economic, cultural, moral, and social realities. Eko, a communications professor at the University of Iowa, is the only author to date to present such a typology, which he first outlined in a 2001 article in *Communication Law & Policy*, and later

**FOUR RATIONALES FOR THE MASS MEDIA**

| | AUTHORITARIAN | LIBERTARIAN | SOCIAL RESPONSIBILITY | SOVIET-TOTALITARIAN |
|---|---|---|---|---|
| Developed | in 16th and 17th century England; widely adopted and still practiced in many places | adopted by England after 1688, and in U.S.; influential elsewhere | in U.S. in the 20th century | in Soviet Union, although some of the same things were done by Nazis and Italians |
| Out of | philosophy of absolute power of monarch, his government, or both | writings of Milton, Locke, Mill, and general philosophy of rationalism and natural rights | writing of W. E. Hocking, Commission on Freedom of Press, and practitioners; media codes | Marxist-Leninist-Stalinist thought, with mixture of Hegel and 19th century Russian thinking |
| Chief purpose | to support and advance the policies of the government in power; and to service the state | to inform, entertain, sell — but chiefly to help discover truth, and to check on government | to inform, entertain, sell — but chiefly to raise conflict to the plane of discussion | to contribute to the success and continuance of the Soviet socialist system, and especially to the dictatorship of the party |
| Who has right to use media? | whoever gets a royal patent or similar permission | anyone with economic means to do so | everyone who has something to say | loyal and orthodox party members |
| How are media controlled? | government patents, guilds, licensing, sometimes censorship | by "self-righting process of truth" in "free market place of ideas," and by courts | community opinion, consumer action, professional ethics | surveillance and economic or political action of government |
| What forbidden? | criticism of political machinery and officials in power | defamation, obscenity, indecency, wartime sedition | serious invasion of recognized private rights and vital social interests | criticism of party objectives as distinguished from tactics |
| Ownership | private or public | chiefly private | private unless government has to take over to insure public service | public |
| Essential differences from others | instrument for effecting government policy, though not necessarily government owned | instrument for checking on government and meeting other needs of society | media must assume obligation of social responsibility; and if they do not, someone must see that they do | state-owned and closely controlled media existing solely as arm of state |

Table 2.4: Four Rationals For the Press (from Peterson, Schramm, & Siebert, 1956, p. 7)

expanded in a 2008 encyclopedia entry in *The International Encyclopedia of Communication*. The author identifies neo-mercantalist, culturist, Euro-communitarian, gateway, Confucianist, Arab-Islamist, and developmentalist national and regional Internet regulatory regimes, as well as an international Internet regulation model comprising binding multilateral conventions, resolutions, and declarations. Eko's 2012 book *New media, old regimes: Case studies in comparative communication law and policy* also references the typology, and specifies that the seven categories reflect different "governmentalities"—a concept developed by Michel Foucault to refer to the organized practices (mentalities, rationalities, and techniques) through which governments attempt to create the subjects (the governed), and the social, economic, and political structures in and through which particular policies can best be implemented.

While Eko's (2012) approach is a very useful starting point, it has one critical shortcoming: Although governmentality is a multifaceted concept, governmentality-based comparative analysis tends to focus on a single characteristic of a country or society that reflects and exemplifies deeper structural conditions. Each of Eko's category type labels signifies such a pronounced attribute: the neo-mercantalist model captures Internet regulatory regimes characterized by libertarian economic principles, the culturist model captures Internet regulatory regimes characterized by protection of national culture and language, the development model captures Internet regulatory regimes characterized by the use of the Internet for economic and political development, etc. But governmentality as a single variable does not adequately (in some cases) or consistently (in others) serve to categorize cases. Eko presents France as the exemplary culturist case, yet the country would also seem to fit within the Euro-communitarian model. Saudi Arabia, likewise, could arguably be categorized under either the gateway model or Arab-Islamist model. A multi-dimensional typology that accounts for all relevant policy attributes and uses constructed type category labels is a better way of categorizing Internet policy regime cases. My typology uses Eko's work as starting point, but disaggregates the governmentality

variable into its component parts, which are then sorted into the relevant policy regime dimensions.

**Typology dimensions**

The dimensions for my proposed typology are drawn from *policy regime* literature—particularly the model advanced by Wilson (2000), which consists of four dimensions: power, policy paradigm, institutional arrangement, and the policy itself. I have altered the dimension categories somewhat to best reflect the subject, and added several additional categories to fully capture all of the relevant variables.

**Ideas.** At a second order level, ideas may refer to *systems* of ideas or ideologies which link together a wide range of phenomena, and which connect to and influence policy proposals. But in practical policy analysis, ideas generally refer to the relatively discrete policy packages of measures which may be selected and implemented as actual policy (John, 1999, pp. 42). The policy process is permeated by competing ideas about the "good life" and the best policy goals and tactics to achieve it. Policy-making participants advocate their respective policy ideas and engage with one another to try to win their case (John, 1998, pp.144-145).

Wilson's (2000) policy regime model captures this practical definition of ideas under the concept of "policy paradigm." A policy paradigm refers to an intellectual construct containing a set of ideas shared by the policy actors, including critical assumptions about the policy problem's cause (and those responsible for causing it), its seriousness, its pervasiveness, and the appropriate governmental response. The policy paradigm thus shapes not only the ways problems are defined, but the types of solutions offered, the kinds of policies proposed, and the "identity" of the policy actors (Wilson, 2000; Capano, 1999).[6] Policy paradigms and the ideas and assumptions undergirding them are constructed by (a) the academic discourse of researchers and intellectuals; (b) professionals and practitioners directly engaged with the issue; (c) interest group leaders and organizations

[6] Capano's (1999) discussion of policy paradigms draws from Hall (1993) and Jenson (1989).

advancing a particular policy agenda; and (d) the interaction of policy makers with the individuals and organizations identified above. Paradigms are disseminated through the media, political speeches, policy debates within government, and even day-to-day communication in homes, schools, and places of work (Wilson, 2000).

When a policy paradigm is shared by all of the relevant members of the policy sector, it can understood to be hegemonic. However, when policy actors embrace different policy paradigms, there is a conflict that must be resolved in a favor of a dominant paradigm—although that label suggests an alternative paradigm still exists or will emerge in the future (Braun & Busch, 1999). A dominant policy paradigm tends to stabilize a policy regime over the long term in several ways. First, it structures perception of the policy in ways that obstruct the emergence of alternative policy definitions and policy solutions. Second, it promotes the belief that existing arrangements are rational and natural and alternatives are irrational or impossible. Finally, it legitimizes the regime and contributes to its long-term stability (Wilson, 2000, p. 259).

A survey of relevant literature suggests that there are four critical components to Internet policy paradigms: governing regime type (political context), regulation model (regulatory context), ICT development goals (economic context), and the values and criteria by which policy goals are defined and recognized (normative context).

***Governing regime type.*** Milner (2006) posits that the uneven diffusion of the Internet across the globe has been driven by neither technological nor purely economic factors alone—rather, it is "political factors, especially domestic institutions" that matter for the adoption of new technologies because they "affect the manner and the degree to which winners and losers from the technology can translate their preferences into influence" (p. 178). The author hypothesizes that authoritarian leaders perceive the disadvantages of the Internet as outweighing its advantages, and are thus less likely than democratic leaders to promote Internet development. Using indicators of diffusion (such as users or hosts per capita) as proxies for government policy toward the Internet, Milner's

analysis indicates that a country's regime type matters greatly, even when controlling for other economic, technological, political, and sociological factors.

Milner's work (2006) and other early analysis of Internet diffusion suggested that the only effective way to completely control the Internet was to limit its growth or even keep it out of a country entirely. However, a strategy of limiting Internet infrastructure is not sustainable, as it also limits the state's ability to harness the technology's economic benefits. The *Dictator's Dilemma* theory—a variation of Huntington's famous King's Dilemma—suggests that authoritarian states will either adopt technologies thought to threaten political control, or face economic stagnation and other pressing legitimacy issues (Kedzie, 1997). The recent trend is both academic and media accounts is to highlight authoritarian regimes' ability to maintain technical and surveillance advantages over their own Internet architecture, and to use legal, normative, and market constraints to limit political challenges. Analysis of Singapore, China, and the United Arab Emirates suggests that governments can successfully bifurcate "economics" from "politics" (Wand, 2012; Boas, 2006).

It is also necessary to emphasize that there is a tremendous amount of policy variation within any given regime label. Even the world's democracies understand the same technologies in very different ways. They may have similar policy goals—e.g. more efficient government, improved access to information—but will implement tech initiatives and regulations in substantially different fashions (Rogerson & Milton, 2010). For instance, Hallin and Mancini (2004) identify three very different media models within Western democracies: the Mediterranean or 'Polarized Pluralist" model; the North / Central European or "Democratic Corporatist" model; and the North Atlantic or "Liberal" model. As these titles suggest, each model emerged in and is representative of different countries and regions, but each model is also centrally defined by political system characteristics.

Authoritarian regimes exhibit similar policy diversity, although there are a few

key common denominators. Kalathil and Boas' (2003) seminal work *Open Networks, Closed Regimes* surveyed how eight authoritarian and semi-authoritarian countries—China, Cuba, Singapore, Vietnam, Myanmar, the United Arab Emirates, Saudi Arabia, and Egypt—employed and regulated the Internet, and found different results, as the regimes did not attempt to suppress information flows over the Internet in the same fashion. Recent country profiles reports from Freedom House and the OpenNet Initiative reveal the same sorts of variation. There was, however, evidence of censorship in all of their case studies, suggesting a common strategy if not tactic.

Furthermore, the Pearson correlation coefficient for Freedom House's 2013 Freedom in the World score and the 2013 Freedom on the Net score for the 60 countries receiving both is 0.85. This is a strong positive correlation, which means that high Freedom in the World variable scores go with high Freedom on the Net variable scores (and vice versa).[7] [See Appendix 1].

***Regulatory paradigm.*** Information and Communication Technology (ICT) sectors, including the Internet, have always existed within a regulated environment, although the extent and applicability of this regulation has expanded considerably over the past two decades. It should be emphasized that it is not only the degree of state intervention, but also its objectives and instruments that determine the classification of a country within the Internet control typology. A full accounting of control mechanisms will be provided later in the paper, but three Internet regulation paradigms can be identified here that provide a policy backdrop against which more targeted regulatory actions can be said to occur. The three paradigms are: self-regulation, government regulation ("command-and-control"), and co-regulation (Cave, Simmons, & Marsden, 2008; d'Udekem-Gevers & Poullet, 2001).

Self-regulation occurs when regulatory authority—the power to create and enforce rules—is formally delegated to a private entity, although punishment for non-com-

[7] The P-Value is $< 0.00001$. The result is significant at $p < 0.05$.

| | |
|---|---|
| *Command-and-control* | Public authorities make the rules, enforce them, and punish those who breach them. |
| *Self-regulation* | Private tech sector actors largely make the rules and implement them collectively without any public intervention. |
| *Co-regulation* | Policy drafting, implementation and enforcement is spread between a number of public and private actors, but initiated and overseen by the state. |

**Table 2.5:** Regulatory Paradigms

pliance may still be enforced by and through the state.[8] Modern self-regulation began in the United States with industry associations that defined their own codes of conduct, and limited membership to those willing to obey these rules. Self-regulation is often perceived as the preferred mode of regulation for the Internet because the technology is new and still evolving. Both public and private actors recognize that legislation passed into law reflecting existing market dynamics and user behavior may soon be outdated and ineffectual. Thus legislation is expected to trail, not anticipate, new technology. Self-regulation performed internally within the tech industry allows a greater degree of flexibility in rules and practices, especially with regards to new fields of development. The US system of Internet regulation has often been described as self-regulatory (Peng, 2005; Kleinsteuber, 2004, pp. 62-64).

Under a command-and-control regulatory model, government authorities or a specialized government agency make the rules, enforce them, and punish those who breach them. Under such an arrangement, government regulators fix standards on certain activities (the command) and establish mechanisms for monitoring and enforcement (the control). Command-and-control establishes recognized and observed operational parameters and compliance obligations, and thus creates a relatively stable platform for regulatory participants. Its legitimacy is particularly strong in times of crisis where

[8] Self-regulation may also be found where there is *no* state regulation, although this is less common.

sentiment demands more intensive and legalistic rules. However, critics often note that command-and-control regulations are inefficient, inflexible, and discourage innovation, and that such an approach is not well matched to the technological realities of the Internet (O'Sullivan & Flannery, 2011; Frydman, Hennebel, & Lewkowicz, 2012).

Co-regulation encompasses a range of different regulatory phenomena, all involving complex interaction between general legislation and a self-regulatory body (Marsden, 2011b).[9] Co-regulation generally provides "backdrop powers" for governments to intervene in the event that markets fail or constitutional rights such as freedom of expression are endangered. It also constitutes multiple stakeholders, including consumers and citizens, and this inclusiveness results in greater legitimacy claims. Co-regulation is often identified with "new governance" trends in environmental and financial regulation during the late 1990s, yet it also reflects the emergence of ICT policy during that period. Marsden (2011a) argues that co-regulation is "becoming the defining feature of Internet regulation in Europe," and may "prove the most appropriate model to respond to other dynamic technologically led and globalized fields of regulatory activity" (p. 242).

***ICT development goals.*** In an examination of media policy paradigms in the United States and Western Europe, Val Cuilenburg and McQuail (2003) find that the most influential causes of change are probably the ambitions of media corporations and governments alike to benefit from the economic opportunities offered by Information and Communication Technology (ICT), and the Internet more narrowly.[10] The authors argue that the emerging policy paradigm for media and ICT is primarily driven by economic

---

[9] Frydman, Hennebel, and Lewkowicz (2012, pp. 133-134) argue that the meaning of co-regulation is twofold: as a concept of legal theory, it may refer to a legal model in which norm-drafting, implementation, and enforcement are not under the sole authority of the state, but rather spread among a number of players, both public and private; in a more practical sense, co-regulation refers to a form of governance based on the voluntary delegation or transfer to private actors of the burden of all or part of the drafting, implementation, and enforcement of norms.

[10] As noted in footnote 10, the term Information and Communications Technology (ICT) refers to all technologies and devices used in managing and processing information systems. For the purposes of this paper, its important to understand that ICT's most important contemporary function is serving as the physical conduit of digital data.

| | |
|---|---|
| *Foreign Direct Investment* | ICT infrastructure may serve as an inducement for FDI. Market-seeking FDI is particularly attractive in developing countries favoring import substitution strategies. |
| *Value-added Technology* | ICT can increase the productivity and competitivess of the local economy—particularly among tech-intensive industries and services. |
| *Social Development* | ICT may be used to achieve social and community development goals related to civic organization, education, and increased economic agency. |

**Table 2.6:** ICT Development Goals

and technological logic, although it retains certain normative elements from the previous regimes.

It is widely recognized that ICT can act as a catalyst for development and enable change across all economic sectors, especially in combination with other growth-promoting policies (Economou, 2008, March 27-28). Countries at different levels of development have tried to harness ICT in three fundamental ways that correspond to different roles ICT may play in the economy (Table 2.6). First, countries have developed and promoted their national ICT infrastructure and industry (both hardware and software) to attract both market seeking and efficiency seeking foreign direct investment (FDI). Market seeking FDI is especially attractive in developing countries favoring import substitution strategies. Efficiency seeking FDI is essentially a form of vertical integration aimed at reducing costs by moving or replicating different stages in the production to more cost-efficient or market-proximate areas of operation. Both approaches may involve the establishment of manufacturing and assembly facilities either with a local partner or a wholly owned subsidiary (Hanna, 2003).

Second, countries have utilized ICT as a general purpose, value-added technology that can increase the productivity and competitiveness of the local economy—particularly among ICT-intensive industries and services. The impact of investment in ICT

infrastructure may span beyond targeted industries into all types of information-based and business-support services. There is a growing awareness among both advanced and poor countries that this is where most of the economy-wide benefits are likely to be (Hanna, 2003).

Third and finally, countries may use ICT development as a part of larger policy strategy for social and community development. For developing countries, these policy goals may be pursued in coordination with nongovernmental organizations and other civil society actors working to increase education opportunities and economic agency. ICT has powered global civil society movements for causes such as debt relief, banning land mines, and providing HIV drugs in poor countries, and allowed local economic networks to better integrate into global markets and supply chains (Hanna, 2003).

***Norms.*** Norms are best thought of as the values and criteria by which policy goals are defined or recognized by policy makers. While norms are a component of the Internet control typology, they are not its most salient feature. Content filtering and other censorship mechanisms in Myanmar and Cuba, for instance, reflect different social and political values, but both countries have a similar institutional arrangement through which censorship occurs.

Governments that seek to implement Internet control mechanisms—particularly filtering—typically invoke the "protection of public morality" as a justification, although terrorism has emerged as a favorite rationale of late. Authoritarian regimes often cite intentionally vague notions of national security and social stability. The specific type of content blocked or otherwise censored varies considerably from region-to-region and regime-to-regime. Middle Eastern governments are the most likely to block material deemed heretical or sacrilegious; Western countries are more active in protection of intellectual property, including restrictions on illegally downloadable movies and music; while France and Germany block sites for virulent hate speech. The OpenNet Initiative divides regime filtering efforts into four categories: political, social, conflict / security,

and Internet tools (Warf, 2013, p. 46; Bidgoli, 2006, pp. 353-354).

The institutions used to enforce Internet control policies are typically outgrowths of older media regulatory regimes, and policy language specifying the kind of prohibited Internet content is often drawn directly from existing legislation and decrees addressing prohibited newspaper, radio, and broadcast media content. As such, it may be assumed that when governing regimes shift—especially from authoritarian to democratic—there will be equally dramatic shifts in media and Internet policy. In Spain, for instance, a new media structure emerged after Franco's authoritarian rule that was characterized by extraordinarily high levels of pluralism and liberty—all principles solidly rooted in the democratic constitution of 1978 (Gunther, Montero, & Wert, 2000).

However, the example of Spain is something of an anomaly. Case studies of media policy in post-Communist Eastern Europe suggest that media regulatory institutions may retain authoritarian characteristics even after a democratic transition (Jakubowicz & Sükösd, 2008). In part, this is because laws and politics governing the media are deeply socially embedded, and can be thought to represent cultural as well as institutional forces (Verhulst & Monroe, 2013). Media regimes in new democracies are often transformations of existing institutions that carry with them the norms and power relations of the old regime (Voltmer, 2012, p. 235). This perpetuation of institutional practices can easily filter down to Internet policy. In Tunisia, for example, a number of restrictive Internet laws from the Ben Ali-era remain on the books, and there have been efforts to reinstate the Tunisian Internet Agency's filtering system to block pornography and other morally offensive content. Furthermore, the sentencing of two young bloggers to seven years in prison for charges relating to their posting of caricatures of the Prophet Muhammad on Facebook has prompted serious concerns among free expression advocates (Freedom House, 2012).

**Internet penetration.** Internet use levels are strongly correlated with income (World Bank, 2012, p. 17). Generally speaking, countries with lower per capita income

have lower Internet access or usage levels. These nations, of course, also lack many other elements of infrastructure. Hargittai's (1999) work is one the earliest work detailing this relationship. The author compared Internet connectivity (measured as penetration) levels in eighteen Organisation for Economic Co-operation and Development (OECD) member countries. Hargittai found that economic wealth (measured by gross domestic product, or GDP, per capita) and telecommunications policy were the most salient predictors of a nation's Internet connectivity. Two years later, Norris (2001) undertook a cross-national comparison of 179 countries, examining the relationship between a variety of social, economic, and political factors and the number of people online in each nation. Norris found that economic development and investment in research and development were the overriding factors in the level of Internet adoption. Neither education nor the level of democratization were significantly linked to citizen usage (West, 2005, pp. 141-142).

Levels of Internet penetration have risen substantially since those two works in both developed and developing countries. But the digital divide remains substantial. According to World Bank development indicators (2012) for 2010, there were an average of 74.7 Internet users per 100 people in high-income economies, 34 users per 100 people in upper middle-income economies, and only 5.4 people per 100 in low-income economies. Warf (2013, p. 22) emphasizes that access to the Internet is "deeply conditioned by where one is," which is in turn a reflection of existing topographies of wealth, class, gender, ethnicity, and power. As discussed ahead, Internet penetration rates shape the contours of Internet control policy.

Some of the most cited assessments of telecommunications and ICT development within particular regions and countries come from market research and consultancy firms, such as BuddeComm, Taylor Nelson Sofres, and the Global Web Index. Projections and snapshot figures from these firms can be found in peer reviewed journals, IGO reports, and major newspapers. While these groups do not always outline their methodology, their success depends upon a reputation for accuracy, and their research—both free and

paywalled—on Internet and mobile penetration, e-commerce, and social media usage is appropriate for comparative studies.

The International Telecommunication Union, a specialized agency of the United Nations, also provides telecommunications and ICT data for 200 economies, including infrastructure, access, and usage information. The cited figures and statistics are generally provided by national government agencies. The Organisation for Economic Co-operation (2011a; 2011b) uses a similar set of indicators, including:

- Internet users per 100 inhabitants
- Internet subscriptions in total
- Broadband subscriptions per 100 inhabitants
- Availability of digital subscriber lines
- Households with access to a home computer
- Households with access to broadband
- Mobile users per 100 inhabitants
- Wireless-broadband subscriptions

Quantitative analyses of ICT-related research questions tend to use Internet users per 100 inhabitants as an independent variable, or Internet *and* mobile users per 100 inhabitants as these variables together act as a measure of the level of digital communications (see Wand, 2012; Fielder, 2012; Best & Wade, 2009). Broadband Internet is significant because of its substantially increased connection speeds (compared to dial-up), which allow for a greater variability of Internet use—such as an increase in allowable file viewing size—and a fixed line ("always on") connection that does not tie up a household's main phone line. Dial-up modem connections have a maximum speed of 56,000 bytes per second, while a DSL broadband connection can translate data at 5 million bytes per second (CERIAS, 2013). From 2005 to 2010, the percentage of people in industrialized countries accessing the Internet via broadband DSL or cable connections rose substantially. In this same period, the number of mobile phone users reached 3 billion,

meaning that nearly one out of every two people on the planet owned a mobile phone. In 2013, the number of mobile subscriptions was expected to pass 7 billion, meaning that the vast majority of the global population now owns a mobile device (Etoh & Powell, 2005; Sauter, 2012, pp. 4-5).

The inclusion of mobile phone statistics is especially important because of the global expansion of 3G—and now 4G—networks. 3G, or third generation, mobile network technology represented a substantial functional leap from 2G in that it allowed for full Internet service connection. A concurrent development during this time was the smartphone, which combined the abilities of a palmtop computer with a mobile phone, leading to widespread demand for 3G service. After Apple entered the mobile domain with their iPhone in 2007 and Google followed with the Android a year later, technological innovation on mobile devices decoupled from the telecoms industry and moved toward IT-based software companies. A 2010 ITU report speculated that at current growth rates, web access by mobile devices and laptops is likely to exceed web access from desktop computers by 2015 (Etoh & Powell, 2005; Sauter, 2012, p. 5; ITU, 2010).

**Institutional arrangement.** Wilson (2000) includes "institutional arrangement" as part of his policy regime model. Institutional arrangement refers to a policy's organization within government, the policy-making arrangements through which policy is developed, and the implementation structure through which it is applied. Wand's (2012) digital state capacity model can be considered an institutional approach to Internet policy analysis. Digital state capacity is a multifaceted concept that can be divided into (a) potential ability, which rests on underlying institutional factors; and (b) application, which is premised on policy objectives and driving ideology (pp. 45-47). In this Internet control regime typology, application is largely captured by the paradigm component within the *Ideas* dimension.

For the purposes of Internet control, the most relevant part of the institutional arrangement is the implementation structure through which policy is applied. The Internet

control regime's policy-making arrangements and organization within government are both irrelevant if the implementation structure is not effective. To best capture this structure, I use a framework developed by Eriksson and Giacomello (2009). The authors argue that government control of the Internet occurs across three dimensions: (1) access to the Internet, (2) functionality of the Internet, and (3) activity on the Internet. These dimensions do overlap to some extent, but the framework still illuminates policy options and constraints vis-à-vis each dimension.

Effective control across all three dimensions—especially activity—is contingent upon the potential ability aspect of Wand's (2012) digital state capacity concept, which I refer to here simply as "institutional capacity." Per Wand, there are four critical aspects of potential ability: financial, as Internet control bureaucracies are expensive to build and maintain; technical, as monitoring and filtering tools require development and customization; human resources, in both quantity (numbers of personnel assigned to surveillance and censorship) and bureaucratic quality, and finally institutional corporate cohesion, .i.e. the willingness of individuals within institutions to comply with edicts from regime leaders and enforce institutional goals. This last aspect is addressed within the *Ideas* typology dimension, and I only reference it tangentially here. As the state is rarely the sole actor applying Internet control mechanisms, institutional capacity may also extend to oversight of private and corporate actors, especially tech companies that function as information intermediaries.

What follows is a brief summary of Eriksson and Giacomello's (2009) three dimensions, with special emphasis given to control mechanisms associated with *activity* on the Internet, since they are the most commonly deployed mechanisms across regime type and arguably the most important.

***Access.*** Internet access shapes the contours of Internet control policy. Access refers to the ability of citizens to connect and use the Internet. Eriksson and Giacomello (2009) argue that controlling access involves (1a) controlling the means of access (com-

puters and Internet service providers), and (1b) controlling the Internet's physical architecture (cable networks, routers, satellites, etc.). Both state and nonstate actors may exact varying degrees of control on one or both of these areas.

Means and levels of access vary considerably across regime types and developmental status. Ward (2013, p. 48-49) notes that in impoverished states in which penetration rates are low and users rely heavily on Internet cafés, control mechanisms are easy to implement and resistance is futile. As personal computer prices fall, Internet access expands, and users grow more technologically adept, the initial control mechanisms become less effective and the Internet user populations becomes more difficult to manage. In addition, rising incomes, literacy rates, and technical skills often produce modernizing elites who actively resist censorship through organized means. Authoritarian regimes recognize this phenomenon, and thus try to keep access levels within their institutional span of control. This incremental approach reflects a recognition by policy makers and policy analysts that "[i]nformation infrastructure is politics" (Howard, Agarwal, & Hussain, 2011, p. 9), but it is a difficult balancing act to maintain.

The institutional requirements for controlling access are relatively low as little state intervention or bureaucratic investment is necessary. Until fairly recently, it was still possible for governments to forego Internet infrastructure altogether. The ruling junta in Myanmar, for instance, has long resisted private partnerships to upgrade their antiquated telecommunications infrastructure and expand Internet access,[11] although there is evidence this policy is finely shifting (The New York Times, 2000, Nov. 19; Open Technology Fund, 2013). In less extreme cases, states can control access by putting physical limits on the Internet infrastructure, often by constraining the number of servers, hosts, and Internet providers allowed domestically (McLaughlin, 2003).

Many authoritarian regimes adopt a gateway model of Internet control, in which government agency serves as the *de facto* or *de jure* gateway to the Internet for the entire

[11] As of 2012, less than one percent of the population had access to the Internet (OpenNet Initiative, 2012a).

country, allowing for a high degree of control over both access and activity. In such countries, there is little to no separation of duties between the government, Internet regulatory authorities, Internet service providers, and Internet hosts (Eko, 2012; Kalathil & Boas, 2003).[12] This approach does require a substantial bureaucracy—and possibly the creation of an entirely new agency—in addition to substantial investments in telecommunications hardware. The gateway approach may also empower and expand rent-seeking government agencies. In the Middle East, for example, Internet licensing policies driven by neopatrimonialism and nepotism have accentuated the powers of the state, and enabled strategic government agencies to limit and control access (Warf & Vincent, 2007).[13] Gateway countries may also feature a national language intranet that is isolated from the global Internet by firewalls, proxy servers, and filtering techniques (Eko, 2012; Warf; 2013).

In advanced countries, access is universal and relatively affordable. As more people move online, a more complex, expensive, and cumbersome set of control mechanisms are called for which primarily function to restrict user activity (as discussed ahead). Some have speculated that mobile phones—especially smartphones—may be better able to circumvent the censorship mechanisms described ahead in *Activity*. In China, for instance, some websites are able to set up wireless application protocol (WAP) sites which can only be viewed on mobile phones to feature content that otherwise would be censored. However, a recent investigation into the risks and vulnerabilities of mobile phone services and apps in twelve countries with authoritarian governing regimes suggests the capability of repressive governments to monitor users of mobile phones and block access to Internet content is far beyond levels realized by users and presents significant risks for user privacy and safety (Callanan & Dries-Ziekenheiner, 2012).

***Functionality.*** Functionality refers to the technical quality of Internet usage—spe-

[12] This arrangement is in keeping with Linz's observation of the "low specificity of political institutions" in authoritarian regimes (2000a, p. 160).

[13] Even in cases where Middle East governments attempted deregulation to expand access and lower service costs, such efforts ultimately benefited the state by placing more communication platforms and forums under government control (Salhi, 2009).

cifically, (2a) the physical quality of connections (bandwidth and speed); (2b) the quality of communications software (e.g. browsers, instant messaging programs, voice and video services); and finally (2c) the technical protocols of Internet communication (IP, TCP, BGP, UDP, etc.). Technical protocols provide the standardized methods of communication through which digital communication occurs, and is thus one of the most fundamental sources of power in Internet governance (Eriksson & Giacomello, 2009).[14]

Governments may exert a degree of control on functionality through domestic regulation, licensing, and monitoring, but these measures are fairly marginal.[15] Even when Internet infrastructure development is led by national governments, it is almost always in collaboration with international technology firms. In the 1990s, for example, Cisco helped the Chinese government develop that country's Internet infrastructure, and remains a critical player along with several other US companies, including Nortel Networks, Sun Microsystems, and 3COM (Hitt, Ireland, & Hoskisson, 2012; OpenNet Initiative, 2005). The quality of connections and software is thus largely controlled by the market, as private firms are generally responsible for applications, hardware (including architecture), bandwidth, and the speed and stability of Internet connections.[16] Authoritarian governments, however, may occasionally interfere with the quality of Internet connections for political purposes. In the wake of the Arab Spring authorities in Bahrain

---

[14] Lessig's influential book *Code: And Other Laws of Cyberspace* (1999) explained how these protocols (and other examples of Internet code) regulated online conduct in much the same way that legal code regulated "real world" conduct. Because very few legal enforcement mechanisms were embedded in early Internet designs, regulating illegal actions such the sharing of copyrighted works was all but impossible. But, just as Lessig predicted, elements of the code architecture of the Internet have been adjusted to favor regulation instead of circumvent it, and regulating online activity has become considerably easier.

[15] The effect is larger when governments tightly regulate the telecommunications industry or even own major telecommunication firms. State monopolies in the industry are not uncommon, even in democracies. In Ireland, for example, some critics argue that state ownership of the telephone network infrastructure through the company Eircom explains the country's very weak broadband indicators, especially vis-à-vis its economic development peer group. McDonnell (2013), however, argues that Ireland's relatively poor broadband performance should be understood as the outcome of a number of interrelating factors, including a dispersed and low-density population and different market considerations.

[16] Even to the extent that any government can be said to control this aspect of functionality, that level of control does not—at least to my understanding—reflect a policy objective of controlling the production, dissemination, and consumption of digital content.

slowed down Internet access speeds to hamper the real-time uploading and circulation of videos and photos taken during protests and crackdowns (Bahrain Center for Human Rights, 2011).

Governments play a much larger role in developing and maintaining technical protocols, especially on the global scale. The main Internet governance bodies—Internet Corporation for Assigned Names and Numbers (ICANN), World Summit on the Information Society (WSIS), and the Working Group on Internet Governance (WGIG)—represent a policy regime-building collaboration between governments and private actors. The United States and US domained-private actors tend to dominate these bodies, however of late Russia, China, and a number of Middle Eastern countries have been leading efforts to exert greater control in Internet governance through the UN's International Telecommunications Agency (Eriksson & Giacomello, 2009; Thomas, Waters, & Fontanella-Kahn, 2012, August 27). In 2011 this loose coalition of authoritarian regimes proposed a UN General Assembly resolution proposing the creation of a global information security "code of conduct" and asserting that "policy authority for Internet-related public issues is the sovereign right of states" (Gross, 2012, May). Although the resolution failed, the possibility of further action and initiatives on the issue has alarmed many Internet policy observers.

Because most governments play only a marginal role in controlling functionality, the institutional requirements for control are less applicable. To the extent that governments can be said to interfere with the quality of Internet connections, this is likely accomplished through the same gateway institutions that control access. Larger governments more active in global Internet governance may create executive and advisory bodies for that purpose.

Measurements of functionality focus on speed, which is the single most important metric of interest in characterizing the "quality" of Internet connections, especially broadband service. Perceptions about broadband quality inform regulatory policy, end-us-

er behavior (e.g., broadband subscriptions), investments in complementary assets (e.g., content and applications), as well as the traffic management and provisioning decisions of network operators (Bauer, Clark, & Lehr, 2010, p. 2). The speedtest offered by the private web services company Ookla is the best available data source for assessing the speed of ISP's broadband access service.

***Activity.*** Activity online refers to *how* the Internet is used by individuals, organizations, and government agencies. Eriksson and Giacomello (2009) argue that control of online activity can take different forms: (3b) filtering and blocking of websites or programs; (3c) surveillance of online activity, and finally (3d) attempts to manipulate and control social and political discourse through various means of information, propaganda, and entertainment. However, the authors omit (3a) enforcement at the source and intermediary liability, i.e. direct state action against the producers, consumers and hosts of prohibited digital content. As the lettering suggests, I address this form of Internet activity control first as it is generally the first enforcement option. When states cannot control activity at the source, they move to other control techniques.

Specific government policies and laws are used to create a legal justification for government intervention into cyberspace in any and all of the forms noted above. As outlined the *Regulatory* discussion, the Internet has always existed within a regulated environment, although the extent and applicability of this regulation has expanded considerably over the past two decades. National-security and communication laws—including slander, libel, and copyright-infringement—are the most basic legal tools at a government's disposal to create a regulatory oversight of cyberspace. Although new laws may be created to reinforce this framework, in some cases obscure or rarely enforced regulations may be cited *ex post facto* to justify acts of censorship or surveillance.[17] Deibert and Rohozinski (2010b: 25-26) note that while such interventions may have once been

[17] Deibert and Rohozinski (2010b) note that Pakistan cited an old blasphemy law to block access to Facebook after the social media platform hosted a group called "Everybody Draw Muhammad Day." Pakistan lifted the block after Facebook prevented access to the page within Pakistan.

considered "exceptional and misguided," they are becoming increasingly standard. These laws not only grant government writ to act, they also create a climate of fear and intimidation that eventually (and intentionally) produces self-censorship. Wand (2012) argues that a regime's legal and policy framework for Internet control is "as much about perception of risk and coercion as about detailed laws" and that "lack of clarity over boundaries of allowable information can, in fact, be a key policy tool" (pp. 55-56).

*Enforcement at the source.* Zittrain (2003) and Goldsmith and Wu (2006) document how early state-led attempts to regulate prohibited content targeted the endpoints of the network—the sources and recipients of objectionable material—and to some extent the intermediaries (especially ISPs) who host users' content. Today, Internet policy legislation continues to locate specific action at the citizen or service provider level. Under authoritarian governing regimes, this targeting often comes in the form of coercive actions against individuals, including intimidation, arrest, torture, execution (or the implied or overt threat of such actions), while in democratic regimes targeting is generally in the form of civil suits against individual users and litigation and threat of property seizure against domestic ISPs and assorted tech companies with holdings within the state's territorial boundaries (Wand, 2012, pp. 55-56).[18]

At the individual level, regime regulations and the punitive consequences for their violation rest on user identification. Legal actions taken by private companies and their trade associations for audio, video, and software piracy are a clear example of this. The Recording Industry Association of America (RIAA), for example, initiated civil lawsuits through US courts against US citizens in June 2003 (and onward) for illegally downloaded copyrighted material.[19] The organization targeted university students in particular, as peer-to-peer file sharing was and is rife on university campuses. Record labels pursued similar legal action in national courts across the globe. Some countries have even denied

[18] One of the best and earliest examples of this approach is LICRA v. Yahoo case discussed on page 106..
[19] The RIAA was able to do this by identifying the users' respective individual ISP addresses.

Internet access to individuals who repeatedly download copyrighted music and films (Wand, 2012; Gelsthorpe, 2010, pp. 393-394).

Repressive authoritarian governments may also target individual reporters and bloggers for violations of media or security laws, which are often fully applicable to Internet content. Reporters Without Borders maintains a repository of such incidents, which are all too common under authoritarian and even hybrid governance. In China alone, seventy-eight activists are currently imprisoned for online activity, including Nobel Peace Prize winner Liu Xiaobo, who was sentenced on eleven years in prison in 2009 on a charge of "subverting state authority" for posting outspoken articles online and for helping to draft Charter 08, a call for democratic reform (Reporters Without Borders, 2012b).

The institutional requirements for enforcement at the source vary significantly. As noted, effective enforcement requires user identification. Governments with relatively low Internet penetration levels have been able to achieve such identification by funneling users into government-operated Internet cafés, thus combining access mechanisms with activity mechanisms. In Tunisia under Ben Ali, for example, the regime maintained 240 privately owned, government subsidized cafés (called "publinets") across the country, all of which operated under the authority of the Ministry of Communications. The regime was thus able to regulate usage through its control—pursuant to a December 1998 decree—of these important points of access. Publinets were required to maintain a database of their customers and to post a clearly visible poster notifying users of their responsibility to use the Internet in a legal and lawful manner. Similar Internet café policies have been documented throughout Pacific Asia and the Middle East (Wand, 2012; Freedom House, 2011; Zarwan, 2005).

Governments with higher levels of Internet penetration contend with a greater number of home and mobile users, and thus depend more upon intermediary rather than user liability. Deibert (2012) uses the term *intermediary liability* to refer specifically to government regulation of and government coordination with Internet service providers

(ISPs) that provide access *to* the Internet and online service providers (OSPs)—both domestic and international—that provide services *through* the Internet. OSPs like Facebook, Twitter, LiveJournal, and Blogger provide web hosting, publishing services, and complex community interactions to millions of users, most of whom would lack the means and skill necessary to create and maintain such content on their own. While these services have been a net boon for online free speech, they also consolidate a great deal of digital content onto the servers of private companies.[20]

Both domestic and international companies can and do cooperate with governments to act as censors, removing content deemed unacceptable under the justification of legal compliance. Companies that fail to comply with these requirements may risk fines, the loss of their business license, or prosecution (Zuckerman, 2010; Calingaert, 2010).[21] Some countries have circumvented the necessity of this approach by creating homegrown (and state run) versions of social media and online publishing services and hosting them on government-controlled servers. But many other authoritarian-minded countries lack the capacity to create attractive alternatives, and thus face the problem of either blocking these sites entirely or allowing access to an unregulated sphere of the web.[22][23]

[20] Some sources lump ISPs and OSPs together as simply "ISPs." I have largely retained authors' respective usage choices in this paper when quoting or paraphrasing their arguments and observations.

[21] Even Twitter, the much ballyhooed microblogging service forever associated with the Arab Spring and earlier protests in Iran and Eastern Europe, has agreed to restrict "certain types of content" in countries that have "different ideas about the contours of freedom of expression," such as France or Germany, which ban pro-Nazi content (Clark Estes, 2012, Oct 12; Twitter, 2012, Jan. 26).

[22] Filtering only "problematic" content on a site like Facebook is difficult for several reasons. Most notably, while an individual page about Falun Gong (for instance) might have a unique address (e.g. https://www.facebook.com/pages/Falun-Gong/112176658799482?fref=ts) that could be blocked, content from this page could still be visible to any user via "shares" and updates visible on a user's newsfeed, which does not have a unique address (always https://www.facebook.com/).

[23] South Korea implemented a law in 2007 requiring websites with more than 100,000 visitors per day to use resident registration numbers to track what South Koreans posted online. Although the "real name" verification policy was primarily directed at domestically hosted web sites, it also applied to international companies. Google's YouTube division responded by disabling commenting and video uploads from the country, thus forcing Korean users into noncompliance by making them post anonymously using accounts registered outside of the country. The law was overturned in 2012—along with an equally controversial law forbidding South Koreans from disclosing support or opposition of a political party or a candidate on the Web—but ongoing filtering policies and online speech restrictions led Reporters Without Borders (2012a) to label South Korea as a country "under surveillance" in its annual "Enemies of the Internet" report, putting it in the same company as Russia and Egypt.

While intermediary liability is functionally similar to some of the filtering methods described below—such as the installation of filtering software on email servers—intermediary liability should be considered distinct in that (a) it is a policy geared towards private (often foreign) or partially privatized companies, and (b) content removal is usually carried out through human operators or internal screening procedures, not government-issued filtering software.[24] Because intermediary liability transfers some of the regulatory burden from the state to the ISPs and OSPs, it reduces the state's institutional requirements for control. But government agencies will still be charged with identifying prohibited material, and passing on formal requests to filter or remove said content to ISPs and OSPs or the gateway providers through which ISPs lease their bandwidth.

In Thailand, for example, a "Cyber Inspector" unit working within the Ministry of Information and Communication Technology identifies prohibited content related to pornography, gambling, terrorism, separatist movements, and especially the monarchy (OpenNet Initiative, 2012d). Other case studies suggest human censors within an ISP or OSP are often tasked with monitoring and manually removing or shutting down blog posts, discussion forums and message boards that address verboten topics or criticize prominent political figures (Calingaert, 2010).

Measuring enforcement at the source and intermediary liability is best accomplished by analyzing country profiles from Freedom Net, OpenNet Initiative, and Reporters Without Borders and identifying instances of arrests, prosecutions, or state-sanctioned repercussions for hosting, possessing, or distributing prohibited Internet content. Freedom House's *Freedom of the Net* country profiles are especially useful, as their coding methodology specifically looks for several categories of "violations of user rights," including the presence of laws which call for criminal penalties or civil liability for online and ICT

[24] Such filtering is more likely to occur in joint ventures. Skype's Chinese-language client, built in cooperation with China's mobile Internet giant TOM Online, filters users' messages based on a list of banned keywords, and stores conversations where specific keywords had been mentioned (Zuckerman, 2010; Villeneuve, 2008, Oct. 1).

activities, and instances of individuals being detained, prosecuted, or sanctioned by law enforcement agencies for disseminating or accessing prohibited content.

*Filtering.* Filtering represents the first generation of technical Internet control techniques,[25] and remains the most common technique governments use to restrict access to content deemed objectionable for social, political, and security reasons. Network filtering of the Internet by national governments is documented in more than 30 countries worldwide, not all of them authoritarian. Filtering is often implemented when physical control or direct jurisdiction over the targeted site is beyond the reach of authorities. Filtering may be carried out through a firewall—a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts. When a firewall works effectively requests by targeted users to access restricted sites and content are consistently blocked or misdirected. In addition to government-implemented filtering, many privately operated websites—including those domained in the United States—filter their content by the geographic location of their users (Ziccardi, 2012; Deibert, 2010a; Faris & Villenveuve, 2008; ONI, 2013).[26]

Governments may implement filtering mechanisms either directly or through intermediaries at any of the four main network nodes: the Internet infrastructure itself, Internet service providers (ISPs), institutional computer networks, and individual (home) computers. Applying filtering schemes and blocking technologies directly on the Internet infrastructure—or more specifically, the network service providers (NSPs) which provide Internet connections to ISPs and maintain the physical backbone of the Internet,[27] and the Internet Exchange Points (IXPs) which keep domestic Internet traffic within the local infrastructure—is the most effective approach, as it allow regimes to condition Internet access throughout an entire country (Ziccardi, 2012).

[25] The People's Republic of China was one of the first states to adopt filtering systems at the backbone of the country's internet, and this approach has become the standard model for Internet censorship ever since.

[26] For example, streaming video provider Hulu blocks all users outside of the US from accessing its content (Ziccardi, 2012).

[27] Including the high-speed fiber-optic links connecting high-capacity routers that direct network traffic.

Moving down the infrastructure, the second node is that of Internet service providers (ISPs), the companies (or state owned enterprises) that provide users with access to the Internet, usually via a fixed or mobile access line such as dial-up, DSL, 3G, WiMAX, or fiber-optic cable. Government authorities may oblige ISPs to install filtering software or to adhere to specific surveillance schemes. At this infrastructure level, states may also target information exchange intermediaries, such as language translation sites, email providers, and proxy server sites (Ziccardi, 2012; Deibert et al, 2008; Fielder, 2012).[28] A third level is institutional networks, such as libraries, universities, Internet cafés, and even corporate computer networks. Increased control over specific types of institutions is common in many countries.[29] The fourth—and lowest—level at which filtering may be implemented is on home computers on individual laptops, which may come with preinstalled filtering and monitoring software, or may be exposed to such software through malicious attacks and inadvertent downloads (Ziccardi 2012).[30]

The institutional requirements for filtering are moderate. Although filtering does not require a large bureaucracy—especially as much of the technical implementation of blocking requests can be carried out by intermediary providers—it does require expensive hardware and software, and personnel with the technical capabilities to install and optimize both. Many regimes have to acquire filtering technology from Western providers. For example, Wagner (2012) notes that the Ben Ali regime was only able to build and develop its censorship regime with the help of "international consultants, importing international technology and access to international filtering systems" (p. 490). Indeed, corporate tech entities have emerged as critical actors in the Internet control supply chain. The most recent Reporters Without Borders *Enemies of the Internet* report (2013a) highlights the

[28] Although proxy server sites are also one of the primary ways users get around filters.

[29] In the United States, twenty-four states have Internet filtering laws that apply to publicly funded schools or libraries. Some states also require publicly funded institutions to install filtering software on library terminals or school computers (National Conference of State Legislatures, 2013).

[30] The Chinese government issued a directive requiring the installation of a specific filtering software product, Green Dam, on all new personal computers sold in mainland China by 2009. But the directive was soon scaled back, and the project eventually lost funding.

increasingly important role a small number of private-sector "digital mercenaries" play in providing authoritarian regimes with censorship and surveillance technology.[31]

The best measurements of filtering come from the OpenNet Initiative. The organization runs filtering tests directly within countries (often at multiple locations, and during different times of day and week) using specifically designed software which checks content accessibility against a global list (constant for each country) and a local list (different for each country). The global list comprises a wide range of relevant and popular websites mostly in the English language, including sites with content that is perceived to be provocative or objectionable. The local lists are designed individually for each country by regional experts, and include specific content believed to be blocked by existing filtering mechanisms. ONI classifies blocked content into four categories: political (e.g. regime opposition); social (e.g. religious and moral issues); conflict (e.g. secession movements); and access to specific communication tools (e.g. foreign-based social networks).

*Surveillance.* Roberts and Palfrey (2010) describe the Internet as a "surveillance-ready" technology conducive to a wide variety of state-administered information monitoring techniques. It is important to emphasize that monitoring Internet activity is not necessarily that same as "controlling" Internet activity. The knowledge that authorities may be watching user activity may, of course, deter an individual from accessing, viewing, or posting prohibited digital data (or participating in online dialogues).[32] But unlike filtering, the effect of monitoring is indirect, and the change in user behavior may be minimal depending on the perceived punishment.[33] Furthermore, a large percentage of Internet activity occurs "out in the open"—i.e. on publicly accessible websites and social

[31] These companies include the U.K.'s Gamma Group, Germany's Trovicor, Italy's HackingTeam, California-based Blue Coat Systems, and France's Amesys, which sold its EAGLE spyware to Libya while Muammar Gaddafi was still in power, and is now being sued in France by the International Federation for Human Rights (FIDH) for complicity in torture

[32] Or lead them to Virtual Private Network (VPN) connections and other encrypted services such as TOR, a free software for enabling online anonymity.

[33] Furthermore, the value of Internet monitoring for an authoritarian regime may be diminished when and if users are constantly self-censoring as the regime is unlikely to gather useful information—especially if dissidents simply avoid the platform altogether out of distrust.

media platforms.[34] The monitoring or gathering of this sort of information may be part of surveillance operations, but illicit or simply covert surveillance should be thought to refer to the monitoring of Internet activity—including emails, file transfers, and web browsing records—that a user believes to be private.

Authoritarian regimes use surveillance in order to track and control dissidents, spy on journalists and their sources, and generally head off potential destabilization. For instance, China—an industry leader in so many aspects of authoritarian Internet control—uses its human resource heavy "Golden Shield" program to carry out a massive domestic surveillance of ISPs and online chat rooms, scanning carefully for criticism of the Chinese Communist Party, praise of Falun Gong, and other comments and postings that might challenge regime leadership. A great number of liberal democracies have developed their own surveillance systems, including advanced systems for tracking all incoming and outgoing Internet traffic. Furthermore, private firms headquartered within those democratic states—including multinationals Google, Yahoo, and Facebook—have collected their own massive Big Data troves on users, including search queries and social maps, while the multitude of domestic Internet service providers continue to log the browsing behavior of subscribers. This information, in turn, may eventually be turned over to government authorities (Roberts & Palfrey, 2010; Reporters Without Borders, 2013a).

Effective surveillance requires moderate to high institutional requirements, as intelligence gathering is a largely human labor-intensive affair. China's state media, for example, recently revealed that the Chinese government employs more than two million people to monitor web activity—an absolutely staggering number that serves to underscore the extensiveness of the country's surveillance state (BBC, 2013, Oct. 13). Some aspects of surveillance occur simultaneously with some of the control mechanisms

[34] Reams of information can be gathered about many individuals simply by typing their names into Google or skimming through their public Facebook and LinkedIn profiles.

described above, especially through intermediary liability. ISPs in Asia, for example, are increasingly required to monitor users' access and retain information about their web activity and other computer usage. This practice is most prominent in Myanmar, where Internet café owners are required to take screenshots of visited web sites. Some countries tie surveillance to individual user access, requiring Internet users to register with their real names before gaining access to Internet services. Even democratic South Korea briefly implemented a policy that required users in forums and chat-rooms to register their real names before commenting (Deibert, Palfrey, Rohozinski, & Zittrain, 2012, pp. 231-232).

Other aspects of surveillance may occur outside of the normal Internet regulatory apparatus, and under the purview of law enforcement or state security agencies operating with or without Internet or telecommunications agency coordination. The National Security Agency in the United States operates under the jurisdiction of the Department of Defense and reports to the Director of National Intelligence. Much of the NSA's surveillance operations occurred under the rubric of "signals intelligence" (often contracted to SIGINT), which refers to intelligence-gathering by interception of signals, whether between two or more people communicating electronically or from electronic emissions from military and civilian weapons and tracking systems. The NSA's domestic eavesdropping program was originally designed to locate al-Qaeda terrorist cells suspected of still operating in the United States (Clark, 2007; Aid, 2010, pp 243-244). Although the organization possesses only limited legal authority to spy on US citizens, it constructed a surveillance network with the capacity to reach around 75 percent of all US Internet communications (Gorman & Valentino-Devries, 2013, August 20).

Measuring surveillance is difficult since it is, by definition, covert and intentionally difficult to track, and the number of government agencies and personnel performing surveillance activities may not be well known or reported. Freedom House's Freedom of the Net (2013d) coding methodology specifically looks for evidence of state surveillance of Internet and ICT activities, but the coding category includes the important—if ambigu-

ous—caveat "without judicial or other independent oversight." The coding questionnaire also considers the extent to which digital technology providers are required to aid the government in monitoring the communications of their users, but again this sort of information is not always well known, as recent reporting about the NSA in the United States makes clear.

*National information-shaping strategies.* National information-shaping strategies represent a sophisticated and multidimensional approach to Internet control that has emerged most prominently in China and Russia. This technique focuses on successfully competing with potential threats through the proactive manipulation of web content, which renders it more challenging for regular users to distinguish between credible information and government propaganda. Specific actions include employing "Internet Brigades" to post propaganda and disinformation on blogs, participate in Internet polls with an intention to skew the results, disseminate false information about unfolding events, and harass bloggers and social media users supporting opposition candidates. Bahraini authorities, for example, have employed hundreds of Internet "trolls" to scour popular domestic and international websites, and—while posing as ordinary users—attack the credibility of those who post information that reflects poorly on the government. These same Internet brigades may also coordinate in denial-of-service attacks to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. During the 2008 Russia-Georgia war, pro-government Russian hackers launched denial-of-service attacks against a wide range of Georgian ISPs and websites (Deibert & Rohozinski, 2010: pp. 17, 129; Kelly, Cook, & Truong, 2012, p. 2).

Like surveillance, institutional requirements for national information shaping strategies are fairly high. While China appears to be using these strategies in addition to existing control efforts, Deibert & Rohozinski (2010) suggest that Russia is using these sophisticated approaches to control *instead of* filtering and other blunt control techniques because they are difficult to trace back to the government. The absence of overt

state-mandated Internet filtering in the country has actually led some observers to conclude that the Russian Internet represents an open and uncontested space, thus helping the country avoid the Internet pariah label. Another possible—and related—explanation is that these subtle techniques do not inadvertently disrupt Internet activity for "normal" users and business operations, thus making the country a more attractive destination for foreign direct investment.

National information shaping strategies are difficult to verify and thus difficult to measure without in-depth fieldwork. Freedom House's Freedom of the Net (2013) coding methodology looks for instances of cyberattacks against opposition websites, but does not cover sophisticated propaganda techniques.

**Interests.** Interests refer to policy stakeholders (the individuals, groups, organizations, and institutions with a vested interest in a particular policy or its outcome) and the arrangement of stakeholder power in support of the policy, per Wilson (2000). In general policy terms, this arrangement may involve one or more powerful interest group, including governmental and nongovernmental actors, traditionally friendly or competitive groups, broad base coalitions, or well-endowed interests with narrow coalitions. The state may be a power broker (mediator) here, or a major actor itself. Members of the dominant political party or business class may also take a prominent role, and the state may be predisposed to favor these elite interests because of their positional advantages. In authoritarian regimes, such policy coalitions often include key constituencies at the social core of the regime (Morlino, 2008).[35]

Internet policy stakeholders may include Internet service providers, content developers, trademark holders, intergovernmental groups, policy experts, and end users. Pri-

[35] Stakeholder analysis is a useful way to further break down regime power dynamics, and to specifically identify the critical policy actors. Power, in this analysis, can discerned through two dimensions: first, the power dynamic observable in the decision making process, by which (per Dahl) actor A can force actor B to do something B would not otherwise have done; and second—and more broadly—through the observable control of the agenda, especially the extent to which particular issues that might challenge the values or interests of particular actors are kept out of policy making processes (van der Bulck, 2013; Barzilai-Nahon, 2008).

vate actors may play critical policy advisory roles in emerging economies. Eldon (2005), for instance, documents how ICT companies have been influential in Kenya's Internet policy working groups, and helped to guide the country's telecommunications expansion and Internet development. In the late 1990s, Costa Rica's proactive government partnered with private sector actors to attract ICT FDI (most notably Intel) and transform the country's image from "banana republic" to "Silicon Valley South." Israel, India, and other countries have adopted similar approaches to creating FDI-friendly tech hubs (Drori, 2004, pp. 443-444).

As discussed earlier in the paper, Internet policy may fork off into distinct Internet *regulatory* regimes and Internet *control* regimes when there are competing economic and political interests. Zheng (2008, pp. 49-50) identifies just such a dynamic in China, where policy makers face the "difficult double tasks" of promoting information technology development for economic reasons while simultaneously controlling information access and communication channels for political reasons. Although the control regime seems able to maintain the upper hand through its strategic use of coercive measures, there is recent evidence that China's Firewall may be hurting the tech industry by slowing Internet traffic and hindering the use of cloud-computing services (Economist, 2013a; Mozur & Tejada, 2013, Feb. 13; Schuman, 2011, Oct. 26). This architectural flaw will eventually reduce China's global competitiveness in e-commerce, which could cause a shift in the dynamic between the two regimes. Such factional policy cleavages in China and other authoritarian regimes hold special ramifications for democratization efforts, especially when and if this schism roughly parallels the split between regime "soft-liners" and "hard-liners."[36]

[36] O'Donnell and Schmitter (1986) famously argued that that "there is no transition [to democracy] whose beginning is not the consequence—direct or indirect—of important divisions within the authoritarian regime itself" (p. 19). Case studies suggest that Internet policy might be a bellwether of such schisms to the extent that it introduces a Dictator's Dilemma—a variation of Huntington's famous King's Dilemma—wherein economic development gains and subsequent increases in governing regime legitimacy come at ever increasing costs (and decreasing successes) for information control efforts (Wand, 2012). More specifically, new technologies and subsequent institutional changes may erode political advantages and economic rents for entrenched elites, while empowering new political actors and competing interest groups (Fredman, 2012; Acemoglu & Robinson, 2006, p. 15).

A broad coalition stakeholder approach to policy making has been most evident at the global Internet governance level. The main Internet governance bodies—Internet Corporation for Assigned Names and Numbers (ICANN), World Summit on the Information Society (WSIS), and the Working Group on Internet Governance (WGIG)—represent a policy regime-building collaboration between governments and private actors. The extent of these bodies' influence on national Internet control policies is detailed in the *International factors* section ahead.

**International Factors.** Internet policy is inherently global since it applies to a global information infrastructure, a network of networks. When a Chinese Internet policy results in the removal of a blog post critical of the CCP, that policy affects Internet users around the globe trying to access that content. Likewise, content available to the rest of the world may not be available to Chinese users because of that country's extensive firewall. The Internet is thus a global technology experienced under local conditions (Braman, 2011, p. 150).

The most important global Internet administrative body is the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for the coordination of the global Internet's system of unique identifiers and, in particular, ensuring its stable and secure operation.[37] The United States government originally controlled the Domain Name System of the Internet directly. But as the Internet expanded globally and commercially, total US control became untenable. Instead of turning administrative authority over to an international body such as the UN's International Telecommunication Union (ITU), in 1998 the Clinton Administration created ICANN as a not-for-profit organization incorporated under California law, effectively privatizing domain name

[37] More specifically, ICANN's critical tasks include (1) coordinating the allocation and assignment of the three sets of unique identifiers for the Internet, which are (a) domain names (forming a system referred to as "DNS"); (b) Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and (c) protocol port and parameter numbers; (2) coordinating the operation and evolution of the DNS root name server system; and (3) coordinating policy development reasonably and appropriately related to these technical functions (ICANN, 2011).

governance in order to keep that critical aspect of Internet governance out of the hands of world governments and UN bureaucrats (Brito, 2011, March 5).

Government representatives from around the world sit on ICANN's Governmental Advisory Committee, but as the name implies, their role is only advisory and policy decisions are ultimately made by the ICANN board. Governments unsatisfied with their limited influence over this critical aspect of Internet governance have traditionally gone to the ITU to air their grievances.[38] Until recently that organization's policy influence was marginal. However, during a renegotiation of the telecommunication treaty in 2012, a number of countries, including Russia, China, and Saudi Arabia, proposed overarching reforms for the ITU that would have created significant Internet policy obligations for member states (Brito, 2011, March 4; Dourado, 2013, Sept. 8). While representatives of democratic member states fought to keep the worst provisions out of the final treaty, it still contained objectionable provisions, and was bundled with a resolution giving the ITU greater agency in crafting Internet policy. The United States and 54 other countries refused to sign, and in September 2013, two senior US officials—FCC Commissioner Ajit Pai and Republican Rep. Greg Walden—suggested the United States should pull funding from the ITU if the body persisted in its attempts to regulate the Internet (Dourado, 2013).

Several international organizations contribute directly and indirectly to Internet policy. Treaties are the basis of these activities, whether multilateral, plurilateral, or bilateral. Braman (2011) explains how the formation of the World Trade Organization in 1995 was necessitated by the transition to a global information economy. While the General Agreements on Tariffs and Trade had largely focused on goods, the WTO was designed to

---

[38] Dutton and Peltu (2010) note that the ITU's World Summits on the Information Society (WSIS) in 2003 and 2005 were a significant and controversial recognition of the technology's growing global importance, and that a key WSIS characteristic was its commitment to multi-stakeholder global Internet policy-making. Many works have analyzed the significance of the WSIS—the UN's International Telecommunication Union (ITU) body more broadly—for national Internet policy making (See Dutton & Peltu, 2010; Mathiason, 2008; Shahin, 2007).

accommodate information processing and related services (via the General Agreement on Trade in Services), and to treat more systematically the trade dimensions of intellectual property rights (via the Trade Related Aspects of Intellectual Property Rights agreement). Liberalizing telecommunications agreements under the WTO framework may affect the cost of network access to the Internet, and trade agreements covering trade in computing and networking equipment may affect the cost of equipment used to use the Internet.[39]

Multilateral treaties cover a broad purview, and effectively create an additional layer of legal infrastructure between the international and state levels. The most comprehensive of such regional legal entities is, of course, the European Commission. Other regional entities created by multilateral treaties with such features include those of the North American Free Trade Agreement, and the Association of South East Asian Nations (Braman, 2011, pp. 151-152).

**Incidents.** Wilson (2000) notes that the first stage of policy regime change involves external factors ("incidents" here for alliterative purposes) that effectively weaken the policy regime, create conditions favorable to change, or act as a catalyst for change. Other policy literature refers to such factors as "trigger events."[40] As the term suggests, external factors emerge—often unexpectedly—from outside of the set of circumstances and conditions that shaped the existing policy regime. These observable occurrences can be divided into *stressors*, which impose pressure on the regime, or *enablers*, which facilitate change.[41] Stressor and enabler factors may emerge suddenly or incrementally, but in either case they can be identified and analytically isolated as the *cause* of a partic-

[39] China's World Trade Organization accession came only after substantial deregulatory policy compliances. The concessions resulted in a massive foreign investments in Chinese telecoms and an expansion in domestic access and usage. Foreign investors were authorized to form joint ventures, investing up to 50% in Internet services in the whole country, and up to 49% in the mobile sector in major Chinese cities (Daniel, 2005, p. 30). Although the governing regime has maintained tight content controls on the Internet, trade law analysts have speculated that China's website blocking policies are not consistent with its GATS commitments, and could produce a WTO ruling against the country should a case be brought up (Harley, 2010, Jan. 26; Zimmerman, 2013).

[40] Wilson (2000) cites Cobb and Elder (1983) as an example of this usage.

[41] The effect of the phenomena or phenomenon is observable—or measurable—even if the factor itself is not (e.g. a heat wave).

ular *effect* or series of effects[42]—including a disruption of the institutional arrangement executing the policy, an identification of anomalies in the prevailing policy paradigm, a reassessment of the legitimacy of the policy itself, or a challenge to the power dynamic in support of the policy.

One particular type of stressor, the "spillover effect," would seem to be of special relevance to authoritarian Internet policy regimes and media policy regimes more broadly. Spillover effects occur when changes in the governing regime initiate policy level regime shifts. Authoritarian regimes, of course, implement many policy level regimes *explicitly* for the purpose of preventing such changes and assuring regime stability. Thus a shift in governing-level regime—especially from authoritarian to (or towards) democratic—would seem to augur equally dramatic shifts in media and Internet policy.[43]

**Methodology Summary**

The wide range of Internet control regimes can best be classified using a typological approach. The typology outlined in this paper identifies and categorizes the most common and most prominent control regime types. The typology identifies groupings of countries exhibiting densely linked shared characteristics and presents them as "models"—effectively ideal types, and more specifically constructed types to the extent that they are analogous to a measure of central tendency. The typology is decidedly descriptive in that it identifies the compounds of conceptual attributes (the policy regime dimensions) that comprise particular types (Internet control regime models).

The typology draws from and refines Eko's (2001; 2008) Internet regulatory ty-

---

[42] The relationship between cause and effect, in turn, can be explained through a causal mechanism. Wilson (2000) does not articulate this level of causal analysis in presenting his framework, but his case study examples adequately demonstrate this relationship.

[43] Although the Arab Spring and similar uprisings provide anecdotal evidence that ICT-emboldened activists can continue to catch authoritarian regimes off guard, a wealth of evidence suggests authoritarian regimes have utilized ICT to create sophisticated surveillance systems that can enhance and optimize their repressive capabilities. There is evidence that regimes learn from the experience of other countries and act preemptively against particular forms of ICT to stem off civil unrest—for example, in the wake of the "Twitter revolution" in Iran, the service was blocked across mainland China in the days preceding the 20th anniversary of the Tiananmen Square crackdown (Aday et al 2010).

pology which is largely based on a single (albeit multifaceted) dimension of *governmentality*. The six policy regimes dimensions used in this typology are derived from policy regime, public policy, and Internet policy literature. The dimensions are: ideas, Internet penetration, institutional arrangement, interests, international factors, and incidents. The typology categories are identified in Table 3.1, and discussed in further detail in the next chapter.

| | Cuban Model | Chinese Model | Russian Model |
|---|---|---|---|
| *Includes* | Cuba, North Korea, Myanmar | China, Saudi Arabia, Iran | Russia, Kazakhstan, Uzbekistan |
| **Ideas** | Authoritarian governing regimes willing to deviate from global ICT trends in order to maintain political control. | Authoritarian governing regimes actively promoting ICT development while maintaining tight Internet control. | Authoritarian or semi-authoritarian regimes promoting ICT development and using more subtle means of Internet control. |
| **Internet Penetration** | Very low (0 to 30 percent) | Moderate (30 to 60 percent) | Moderate (30 to 60 percent) |
| **Institutional Arrangement** | A "gateway" governmental agency controls — either directly or indirectly — the country's Internet architecture. Access is limited to a small elite portion of the population, while activity is closely monitored and controlled. | A "gateway" governmental agency controls — either directly or indirectly — the country's Internet architecture. High levels of institutional capacity allow for control focus on activity, not access. | A "gateway" governmental agency controls — largely indirectly — the country's Internet architecture. Open access to the Internet and very little filtering, Government competes in informational space with competitors. |
| **Interests** | Limited political pluralism; small political and business elite. | Limited political pluralism; core political elite; growing business class; international investors and companies. | Limited political pluralism; core political elite; growing business class; international investors and companies. |
| **International Factors** | Hermit countries largely cut off from global e-commerce market. | WTO agreements produce liberalized telecom sectors. | Members of the Commonwealth of Independent States (CIS); vocal in global Internet governance issues. |
| **Incidents** | Arab Spring and similar incidents reinforced necessity of tight controls. | WTO accession and similar economic agreements; Foreign direct investment | Color revolutions induced governments to increase Internet control capacity. |

**Table 3.1:** Typology of Internet Control Policy Regimes

| | Developmental Model | United States Model | European Model |
|---|---|---|---|
| *Includes* | Botswana, Costa Rica, India, Malaysia | US only | France, Germany, Italy, Switzerland, Norway |
| **Ideas** | Developing countries with democratic or hybrid governing regimes and liberalizing economies leveraging ICT as a tool for social and economic growth. | Democratic government with a self-regulatory approach to tech sector. Conception of the Internet as a marketplace of ideas. National security backdrop to surveillance efforts. | Democratic governments with co-regulatory approach to tech sector. Policy makers' views on privacy and speech contrast with US. |
| **Internet Penetration** | Low to Moderate (0 to 60 percent) | Very high (80 to 90 percent) | Very high (80 to 90 percent) |
| **Institutional Arrangement** | Varying levels and arrangements of Internet control, but filtering and surveillance are generally less pronounced than in gateway model countries due, in part, to lower levels of institutional capacity and higher levels of democracy. | FCC has jurisdiction over some issues, but no single agency regulates the Internet. NSA provides the US with unprecedented surveillance capacity. NTIA and NIST also exert a degree of control over functional aspects of the technology. | While EU Directives produce policy harmonization on Single Market-related telecommunication, e-commerce, and data privacy issues, a number of important Internet control policies remains firmly in the ambit of national governments. |
| **Interests** | Limited to full political pluralism; growing business class; international investors and companies. | Multinational tech corporations that shape Internet development and maintain giant troves of personal and business data for users across the globe. | The region's tech sector is not especially strong. Data privacy and "information liberation" have become political issues with young voters. |
| **International Factors** | WTO agreements produce liberalized telecommunications sectors. Strong ties with multinational corporations. | US policy makers have been proactive in intellectual property right protection at international level. | Countries have succeeded in applying speech and data laws extraterritorially through a combination of market power and threat of asset seizure. |
| **Incidents** | Varies, but IMF-led stabilization and similar transitions towards market economies common. | Post 9-11 national security initiatives compel ISPs to share users' private Internet communications with government agencies. | Data Retention Directive was adopted by the European Union after 9-11, but has generated resistance by member states. |

# Chapter Three

## Typology Categories

### Cuban, Chinese, and Russian models

Eko identified and defined the gateway model of Internet regulation in a 2001 *Communication Law and Policy* article, and expanded upon the concept in several subsequent works (2008; 2012).[1] The most salient feature of the gateway model is its institutional arrangement, which reflects a command-and-control regulatory posture. Under this model, a governmental agency in control of the country's Internet exchange points (IXPs) or Internet backbone either serves as operator by providing Internet connections to users directly, or as direct regulator by leasing bandwidth to private or partially privatized Internet service providers (ISPs). Through control of the IXPs and ISPs, governments may install hardware and software necessary to filter and monitor web communication. This allows governments to (a) create firewalls that prevent access to portions of the Internet, which are blocked in the name of national security, culture, morality, or some other stated interest, and to (b) monitor Internet communication (including email and other private messages) coming in and out of the country and circulating domestically. By bundling all relevant Internet control mechanisms in one (or a few) Internet agencies, authoritarian governments can create a centralized control structure that is able to make and implement far-reaching policy decisions about the Internet effectively and extremely rapidly. Wagner (2012) refers to this arrangement as "push button autocracy" in an analysis of Tunisia's Internet control policy regime.

Eko (2008) notes that this model is most evident in countries with authoritarian or semi-authoritarian governing regimes. Authoritarian governing regimes are characterized by—among other factors—limited *political pluralism*, which is usually broadly defined

[1] ISPs and IXPs had already been identified as critical mechanisms of control for authoritarian governments (Shapiro, 1999, p. 65; Human Rights Watch, 1999, p. 463), but Eko expanded on this observation by detailing the specific manner in which control of the Internet architecture allowed governments to strategically limit both Internet access and Internet activity.

as interest-group competition within a democratic structure. More specifically, we can say that political pluralism, per Eisenberg's definition (2010, p. 18), comprises two intertwined themes: the distribution of power among groups, and the ability of any one group to direct individual development. The degree of limited pluralism varies among different subtypes of authoritarian regimes, including so-called hybrid regimes,[2] but it can be assumed that under *any* such regime, participation in political power is likely controlled through certain social forces and channeled through different organizational structures, including mass media and Internet policies.

A survey of case studies of Internet policy under different authoritarian regimes—especially those compiled by the OpenNet Initiative and Freedom House[3]—reinforces the applicability of Eko's gateway model:

- In Myanmar, the Ministry of Communications and Information Technology retains control over the country's international connection to the Internet through two main Internet service providers, the state-owned Myanmar Post Telecommunication and the military-linked Yatanarpon Teleport.
- In Saudi Arabia, the Communications and Information Technology Commission's Internet Services Unit is responsible for overseeing Internet services through 25 licensed ISPs and implementing filtering directives.
- In China, access to the Internet is provided by eight state-licensed ISPs, while Internet usage is tightly regulated by the Ministry of Industry and Information Technology (MIIT), which oversees the country's Great Firewall filtering system which blocks foreign content, and its Golden Shield domestic Internet monitoring system.
- In Russia, a substantial portion of the telecom market—including broadband Internet providers—remains under state control, while all ICT is regulated by the

[2] See Gilbert and Mohseni (2011).

[3] All country Internet information ahead is sourced to these profiles, unless otherwise noted.

Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (*Roskomnadzor*), which possesses the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law.

- In Ben Ali-era Tunisia, all Internet traffic was routed through the Tunisian Internet Agency (*Agence Tunisienne d'Internet*, ATI), which provided the regime with a well-staffed institution to directly carry out existing Internet regulatory policy, and to develop and attain additional Internet control mechanisms.

However, beyond the centrality of a government "gateway" agency and the presence of an authoritarian governing regime—the distinguishing characteristics of the model—gateway countries exhibit a great diversity in Internet control mechanisms employed, filtering and censorship (more generally) criteria, and other identified typology dimensions. Three groupings emerge, which I have categorized with titles reflecting the most exemplary cases of the traits described: the Cuban model, Chinese model, and Russian model. These three models are distinct enough along multiple dimensions that I treat them as discrete categories, rather than subsets of a single "gateway" category.

**Cuban model.** Countries within this grouping feature very low Internet penetration rates (0 to 30 percent), and governments willing to deviate from global ICT trends in order to maintain maximum political control. Cuban model governments may neglect to invest in Internet-related telecommunications infrastructure and technologies, refuse to change the legal and administrative investment climates in ways that would attract the kind of capital needed to generate significant Internet growth, or only allow incremental Internet expansion that never exceeds their limited institutional control capacity (Franda, 2002). The Internet can be crudely but effectively controlled under this model because users are reliant upon the government to provide not only Internet service, but also Internet points of access. However, this approach is decidedly *not* conducive to economic growth. Many authoritarian and semi-authoritarian regimes—especially within Central Asia—ini-

tially implemented many of the policies and control mechanisms described ahead, but eventually changed tact when the necessity of the Internet for foreign direct investment and domestic business growth became evident.

Cuban model regimes can neutralize the Internet as a perceived political and social stability threat by confining Internet *access* to a small elite portion of the population—usually military, scientific, and administrative-intelligence circles—while severely controlling the circumstances under which the bulk of the population is able to gain and use the technology. This can be achieved by (a) developing a sanitized national intranet as a substitute for the global Internet, (b) maintaining a weak Internet infrastructure with a limited number of ISPs, and (c) routing individual Internet users into government controlled Internet cafés where access and activity can be carefully monitored. Cuban model regimes may also use filtering technology and enforcement at the source actions to limit Internet *activity* for any and all users.

National intranets were attractive Internet alternatives for authoritarian governments in the late 1990s and early 2000s, since users were limited to a screened network of content that offered little to no political threat to the regime. The global Internet was either cut off entirely in such an arrangement, or extremely filtered. Although Intranets functioned as a short-term solution, their shortcomings were substantial, especially for governments trying to attract foreign direct investment and keep domestic businesses competitive. Hence, in China, plans for a national intranet were eventually overtaken by events—first, a tipping point in global Internet adoption, and second, the liberalization of the Chinese telecommunications sector as part of the country's entry into the World Trade Organization—which made the idea much less feasible (Wingfield & Macavinta, 1997, Jan. 15; Kalathil & Boas, 2003, p. 141). Today, only Cuba and North Korea maintain such systems, although even in these countries there is evidence that citizens are gaining Internet access through other means and otherwise circumventing the intranet arrangement.

Maintaining an underdeveloped Internet infrastructure is a similarly flawed strategy. Even Myanmar—where Internet penetration rates remain in single digits due its antiquated Internet infrastructure—is finely shifting policy and seeking outside investment to make the necessary upgrades in its telecommunications sector. Internet cafés, however, are a popular feature even in high Internet penetration countries, but they are especially critical points of access in low penetration countries where home computers are rare. Internet cafés allow authoritarian regimes to tie Internet activity to individual Internet users, thereby combining two dimensions of control (*access* and *activity*).

Cuban model countries do employ a number of strictly *activity* controls, although these are mostly limited to enforcement at the source actions, limited surveillance, and filtering. Enforcement at the source refers to attempts to regulate prohibited content at the endpoints of the network—i.e. the sources and recipients of objectionable material—and to some extent the intermediaries who host users' digital content. In authoritarian countries, this targeting often comes in the form of coercive actions—including intimidation, arrest, torture, and execution—against reporters, bloggers, activists, and everyday Internet users for violations of media or security laws. Such actions may also occur outside of a formal legal or political framework entirely. Four journalists were slain in Guatemala in 2013, for example, and most observers were rightly skeptical of interior minister Mauricio López Bonilla's claim that the killings were unrelated to their professions (Reporters Without Borders, 2013b).

Surveillance efforts include tracking the Internet activity of dissidents, spying on journalists and their sources, and scanning and filtering private emails. These efforts are generally less sophisticated than in Chinese model countries because of a lack of technical resources. Cuban model countries may simply opt to block a website or service—especially those domained elsewhere—if they lack the capacity to adequately monitor user activity. Filtering is actually fairly effective in countries where Internet access for a relatively small amount of users is limited to a few government operated or closely regulated

ISPs, as the filtering software and hardware can generally handle that amount of traffic. But filtering on a larger scale can be an expensive undertaking.

In addition to initial installation costs, filtering software and hardware must be periodically updated to maintain effectiveness, which requires further (and ongoing) investment. Many regimes have to acquire filtering technology from Western providers, and private-sector "digital mercenaries" have emerged as critical actors in the Internet control supply chain. In addition to technology costs, the agencies implementing the filtering must also build a list of sites and pages to block. This can be an arduous, human resource heavy task if the content to be blocked is a *type* of content, such as pornography, rather than a specific site, such as an opposition political party or human rights organization (Murdoch & Anderson, 2008).

As personal computer and smartphone ownership rates increase, however, Cuban model regimes must develop a more complex and cumbersome set of control mechanisms that require a great deal more institutional capacity to effectively execute. Some governments will forgo this option—either by choice or necessity—and instead pursue a development model whereby direct government control is largely relinquished in favor of economic development and market liberalization. Other governments will simply increase their institutional control capacity, and double down on control efforts. Authoritarian and semi-authoritarian governments transitioning from low to moderate Internet penetration thus face a critical policy junction. In some cases, particular *International factors* or *Incidents* might have a strong influence in that policy decision. The Arab Spring, for instance, caused some Middle Eastern governments to double down on Internet control measures, while others (especially Tunisia) have transitioned to the developmental model.

**Chinese model.** Countries within the Chinese model grouping feature moderate Internet penetration levels (30 to 60 percent), government-led ICT promotion and development, and a high institutional capacity which allows them to effectively manage and control digital information within their jurisdiction.

Examples of this high institutional capacity:

- China's "Great Firewall" global Internet filtering system is optimized for centralized and region-level management. The system is estimated to have cost the government $160 million dollars when it was developed in the late 1990s. In addition, Internet commentators are paid to post online comments in line with CCP interests, and the government employs more than *two million people* to monitor web activity.
- Iran employs a sophisticated centralized filtering system that augments the filtering conducted at the Internet service provider level, and can effectively block a website within a few hours across the entire network in Iran. These filtering efforts are carried out using domestically produced technology for identifying and blocking objectionable web sites, which reduces the country's reliance on Western filtering technologies. The state also counters critical content and online organizing efforts through online regime-funded propaganda, including 400 news websites either directly or indirectly supported by the state.
- Saudi Arabia filters all web traffic through country-level proxy servers which contain massive databases of banned sites. This means that the Internet content that users in Saudi Arabia see is not the original page on a server outside the country, but a copy on the computer servers in Riyadh and Jeddah. Through this system, the government blocks any content that it deems harmful to society or challenging to the royal family or other Gulf Arab States.

Because of such high levels of institutional capacity, Chinese model countries primarily focus on controlling Internet *activity*, not Internet *access*. Activity refers to how the Internet is used by individuals, organizations, and government agencies. Control of the online activity can take different forms: (a) enforcement at the source—i.e. direct state action against the producers, consumers and hosts of prohibited digital content—which is generally a regime's first enforcement option for controlling prohibited content and on-

line activity, (b) filtering and blocking of websites or programs; (c) surveillance of online activity, and finally (d) attempts to manipulate and control social and political discourse through various means of information, propaganda, and entertainment (Eriksson & Giacomello, 2009). Many of these mechanisms are also present in Cuban model countries, but because of their high institutional capacity Chinese model states are able to execute them with a greater degree of technical sophistication and generally handle a much larger amount of Internet traffic.

Enforcement at the source efforts in Chinese model countries are increasingly directed through intermediary liability, which refers to government regulation of and coordination with Internet service providers (ISPs) that provide access *to* the Internet and online service providers (OSPs) that provide services *through* the Internet. Some OSPs like Facebook operate as "walled gardens" where access is controlled by a single company, and posted content largely exists outside of the searchable parameters of the normal Internet and outside of the screening capacity of most filtering programs. These sites are thus very difficult for authoritarian governments to control unless they (a) block the service entirely, or (b) reach an agreement with the OSP to remove prohibited content as necessary. OSPs can and do cooperate with governments to act as censors, removing content deemed unacceptable under the justification of legal compliance. However, such an arrangement is much easier when the OSP is domestically hosted, and China, Russia, and numerous Middle Eastern governments have encouraged the creation of national alternatives to Twitter and Facebook that are easier for the government to monitor and regulate.

The example of Weibo is illustrative of this trend. After the July 2009 riots in Ürümqi, the capital city of the Xinjiang Uyghur Autonomous Region, the Chinese government shutdown many social media services, domestic and international alike. Weibo, a hybrid of Twitter and Facebook, was launched in the wake of this crackdown as a Beijing-approved alternative to existing services, as the parent company Sina had a strong record of keeping content the government deemed sensitive off its 20 million blogs

(Epstein, 2011 March 3; Ramzy, 2011, April 21). Today the service has more than *500 million* registered users (Ong, 2013, Feb. 21). In cooperation with the government, Sina sets strict controls over the posts on its services and is proactive in removing prohibited content. Nearly 30 percent of the total deletions occur within five to thirty minutes of posting, and nearly 90 percent of the deletions happen within the first 24 hours (Zhu, Phipps, Pridgen, Crandall, & Wallach, 2013).

As noted above, filtering and surveillance efforts in Chinese model countries are considerably more sophisticated than in Cuban model countries, owing in large part to greater investment in filtering hardware and software. Although China developed and implemented its Great Firewall relatively early in the Internet development process, for most countries advances in filtering technology are gradual and incremental. Wagner (2012) details how the Tunisian Internet Agency (ATI) under Ben Ali was able to expand its Internet control over several stages as it acquired new hardware and software, and added new tactics to address emerging threats. The first stage began in 1997 when the ATI implemented a web-blocking proxy filtering program. Because all fixed-line Internet traffic passed through infrastructure controlled by the ATI, the regime was able to load the filtering software onto its servers and filter content consistently across Tunisia's ISPs. The second stage, which lasted from 2003 to 2007, began with the implementation of email-inspection and filtering, which augmented the existing web-blocking filtering program, and added a greater element of surveillance to the control operation. In the third stage, from 2007 to 2010, the ATI added deep packet inspection technology to its filtering and surveillance efforts. The government also initiated national information shaping tactics during this period to proactively shape public opinion online through seemingly organic blogs, videos, and social media posts designed to insult dissident bloggers or praise the government. A fourth and final stage began near the end of 2010, when the regime employed hacking attacks and website defacement efforts to stem the tide of the revolution.

Even the most sophisticated filtering and surveillance technology cannot catch every prohibited communication, in part because the technology advances so quickly. Before the Arab Spring, ATI authorities were aware that the existing filtering system lacked the technical capability to filter or intercept social media posts and messages while still allowing access to the sites themselves. Tunisia did not have the capabilities to develop its own censorship hardware and software, and was negotiating with a European tech supplier to add monitoring of social networks to its existing monitoring capabilities when the events of the Jasmine revolution overtook the country (Wagner, 2012; Silver, 2011, Dec. 21).

Furthermore, extensive filtering and surveillance efforts eventually become detrimental to economic growth. This is especially the case in China, where the government is trying to avoid the middle-income trap by steering the economy up the value chain into high-tech industries. High-speed Internet is critical to this economic development plan, but lag-inducing filtering negates any infrastructure gains. Anecdotal evidence suggests the Internet slows down to a near halt in the country when a sensitive event is taking place. Limiting the free flow of information hampers the development of homegrown, innovative businesses tapped into the global tech scene. Finally, filtering interrupts normal business operations by making the web unreliable, while surveillance makes companies wary of sending classified business information into and out of the country. All of this is a detriment to foreign direct investment in the country's tech industry, and puts its domestic businesses at a distinct disadvantage (Schuman, 2011; Mozur & Tejada, 2013).

As detailed in Chapter One, Zheng (2008) argues that the inherent contradictions in the Chinese government's approach to the Internet have produced two distinct Internet policy regimes: an Internet *regulatory* regime which seeks to promote the technology's development, and an Internet *control* regime which seems to limit any destabilizing effects. Such policy cleavages—in China and elsewhere—would seem to hold special ramifications for democratization efforts, especially when and if this schism roughly parallels

the split between regime “soft-liners" and "hard-liners.” O’Donnell and Schmitter (1986) famously argued that “there is no transition [to democracy] whose beginning is not the consequence—direct or indirect—of important divisions within the authoritarian regime itself” (p. 19).

**Russian model.** Countries within the Russian model grouping are all members of the Commonwealth of Independent States (CIS),[4] feature moderate Internet penetration levels (30 to 60 percent), government-led ICT promotion and development, and moderate to high institutional capacity. The distinguishing characteristics of Russian model countries are (a) relatively open access to the Internet, (b) relatively low or nearly non-existent levels of filtering, (c) strategic removal of content (rather than filtering) through state coordination with ISPs and OSPs and functional domain name controls, and (d) sophisticated information-shaping strategies whereby the government competes in informational space with potential adversaries and competitors.

As this paper has detailed, authoritarian governing regimes are closely linked with repressive Internet control regimes. Thus we would expect the countries of the former Soviet Union—Russia and the Commonwealth of Independent States (CIS)—to follow suit, especially as many of their respective political trajectories have bent back towards authoritarianism after briefs periods of political opening. Only two CIS countries, Ukraine and Moldova, rank as *partly free* in Freedom House's most recent (2013) Freedom in the World report. The rest are all decidedly *not free*. Yet a 2010 report from the OpenNet Initiative, “Control and Subversion in Russian Cyberspace” (Deibert & Rohozinski, 2010), notes that although “creeping authoritarianism” is evident throughout the CIS in nearly every facet of social and political life—and especially in the media, where independent press outlets are stifled and journalists regularly intimidated—the Internet remains accessible and relatively free from censorship. ONI’s frequent filtering tests throughout the

[4] Turkmenistan—with it single digit penetration levels and tight government controls over access—is a clear regional exception, and fits cleanly within the Cuban model.

region identified significant filtering in only Uzbekistan and Turkmenistan. For the rest of the region, web content was as freely available as in Western Europe or the United States.

This is not because the governments lack the means to implement greater control—although these countries feature a more liberalized telecommunications market than other authoritarian or semi-authoritarian states, all of the countries within this grouping feature gateway institutional arrangements whereby a government ministry or agency tightly regulates the country's Internet service providers (ISPs), and generally controls the Internet backbone. In Russia, for example, all of the major ISPs are either state owned or include significant state participation (either directly or through a state-controlled entity),[5] and most of the country's existing country-wide cable lines are held by a small number of large operators, including the state-controlled Rostelecom and TransTeleCom—a subsidiary of government-owned Russian Railways—which operates and services the largest fiber-optic communication network in the country. Roskomnadzor—a Russian abbreviation for the *Federal Service in the Sphere of Telecom, Information Technologies, and Mass Communications*, which is located in the Ministry of Communications and Mass Communications—is the key government mass media agency. Its functions include licensing of broadcasters, registration of mass media outlets, and issuances of warnings for failure to comply with the mass media statute. Roskomnadzor possesses the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law. (OpenNet Initiative, 2010a; Freedom House, 2013a; Reporters Without Borders, 2012c).

Given the ample control mechanisms outlined above, why is there not pervasive filtering in Russia or elsewhere in the CIS? Deibert and Rohozinski (2010) argue that in CIS countries, control strategies are designed to shape and affect *when* and *how* information is received by users, rather than denying access outright. This is accomplished

[5] This arrangement in other CIS countries in similar, with former state monopoly telecom providers (e.g. KazakhTelecom, KyrgyzTelecom, Tajiktelecom, etc.) dominating private providers in the market.

through the use of what the authors label second generation controls, which enable state actors to strategically block access to online content through intermediary liability and subtle and covert mechanisms which can be difficult to trace back to the government, and third generation controls, which enable to state to compete with perceived adversaries through counterinformation campaigns that overwhelm, discredit, or demoralize opponents.

According to Deibert and Rohozinski (2010), second generation controls have an overt and a covert track: the former aims to normalize and legalize content controls by specifying the conditions under which access to particular content can be denied (or said content can be remove from servers), while the latter establishes procedures and technical capabilities that allow content controls to be applied immediately and effectively before and during critical moments (e.g. elections or public demonstrations), and to be applied in ways that assure plausible deniability.

Second generation controls identified by Deibert and Rohozinski (2010) include:

- Compelling Internet sites to register with authorities, and using noncompliance as justification for removing ‘‘illegal’’ content.
- Strict criteria pertaining to what is ‘‘acceptable’’ within the national media space, and the strategic de-registration of sites that do not comply from the national domain.[6]
- Expanded use of defamation, slander, and ‘‘veracity’’ laws to deter bloggers and independent media outlets from posting material critical of the government or specific government officials.

[6] In Russia, for example, recent rules promulgated by Nic.ru—the largest Russian domain name-registration company—and reflecting official regulations allow the organization to cancel domain names (and thus access) for websites that incite violence or “extremist” activity, advocate the overthrow of the government, or feature activity in conflict with human dignity or religious beliefs. In addition, all domain name-registration companies within the country are authorized to suspend domain names upon written notification from “agencies conducting an investigation”—a provision would potentially authorize prosecutors, the Federal Security Service (FSB), the police, or the drug enforcement agency (FSKN) to order such a move (Reporters Without Borders, 2012c) .

- Evoking national security concerns—especially at times of civic unrest—as the legal justification for blocking or removing specific Internet content and services.
- Formal and informal requests to ISPs and OSPs to remove material, backed by the threat of serious sanctions.
- Computer network attacks, especially the use of distributed denial-of-service attacks, to overwhelm ISPs and selected sites. Such attacks are difficult to trace back to the government.

Deibert and Rohozinski (2010) provide numerous examples of all of the above. It should be noted that the use of these particular controls—as detailed in both the authors' account and the most recent Freedom on the Net report—varies considerably across the CIS region. Evidence from Belarus, Kazakhstan, and Uzbekistan suggests those countries are more likely to have content blocked or removed, or even cut Internet and mobile phone service altogether when their respective regimes feel threatened by protests and would-be Color Revolutions. Russia—the model's namesake—largely uses enforcement at the source in the form of offline threats and attacks against bloggers and journalists critical of local officials and powerful business interests,[7] coordinated DDoS attacks, and the sort of third generation control mechanisms described ahead. But in all of these countries, there is very little permanent technical filtering.

Deibert and Rohozinski (2010, p. 27) label "third generation" controls as (a) mechanisms for enhancing state control over national cyberspace, and (b) sophisticated techniques for competing in informational space with potential adversaries and competitors. The examples the authors provide of the former do not seem substantially different from second or even first generation controls, although the focus seems to be on increasing surveillance capacity rather than content removal capacity. For instance, the authors note that Russian ISPs are now obliged by law to purchase and install equipment that

[7] Numerous examples are detailed in Russia's Reporters Without Borders profile (2012c), and in Alexanyan, Barash, Etling, Faris, Gasser, Kelly, Palfrey, and Roberts (2012).

would permit local authorities to monitor the Internet activity of specific users. More recent accounts suggest that ISPs are now required to temporarily store *all* Internet traffic—including IP addresses, telephone numbers, and usernames—and make it available to the Federal Security Service (FSB), the internal affairs agency that replaced the KGB (European Digital Rights, 2013, Nov. 6).

Deibert and Rohozinski (2010) have a stronger claim about the second variation of third generation controls—which the authors refers to as "information shaping strategies"—where the focus is less on denying access (either to the Internet itself or to particular online content) than successfully competing with potential threats through data mining, surveillance, and effective counter-information campaigns. The ultimate source of such campaigns is difficult to attribute since they are "designed to render opaque the role of state actors" (p. 28). These techniques include using paid "Internet Brigades" to post prepackaged propaganda and disinformation in online discussions, skew Internet polls, and harass other users in particular forums.[8] The authors provide numerous examples of such information shaping strategies, and similar examples are also well documented in recent *Reporters Without Borders* country profiles of Russia, Uzbekistan, and Kazakhstan. This technique saw a marked increase in the run-up to parliamentary and presidential polls in Russia at the end of 2011. Several thousand Russian Twitter accounts were hacked in order to flood social media with pro-government messages, while a series of distributed denial-of-service attacks paralyzed sites critical of the government before and during the vote. The most recent Freedom House *Freedom of the Net* report (2013e) notes that the phenomenon of paid pro-government commentators has spread over the past two years, and now appears in 22 of the 60 countries surveyed, including China, Bahrain, Malaysia, and Ecuador.

---

[8] However, Alexanyan, Barash, Etling, Faris, Gasser, Kelly, Palfrey, and Roberts' (2012) comprehensive survey of the Internet's impact on Russian politics, media, and society finds that efforts by the government to push propaganda online through blog supporters—paid or otherwise—have not been very successful, as the mere presence of pro-Kremlin voices does not necessarily translate into influence.

Deibert and Rohozinski (2010) speculate that one explanation for sophisticated second and third generation controls throughout the CIS region is the respective governments' extensive prior experiences in dealing with opposition groups. Well before the Arab Spring, for instance, swells of young protesters used the Internet, mobile phones and text messages to launch protests in Ukraine in 2004, Belarus in 2006, and Moldova in 2009 (Barry, 2009, April 7).[9] In part, this was because the Internet was a relatively liberalized sector of the information sphere in the early aughts throughout many of the former Soviet republics. The Internet and social media, then, were external factors that disrupted the existing policy sphere and created pressure on regime actors to adjust policies. In the wake of the Twitter fueled protests, all three countries developed much more robust online surveillance capacities (Kransnoboka & Semetko, 2004; Manaev, Manaeva, & Yuran, 2012; Deibert et al 2008, p. 181).

**Developmental Model**

Eko's (2001, 2008) typology of Internet regulatory regimes includes a "developmentalist" model in which national Internet policy is (a) geared towards using the technology as a catalyst for rapid economic and social development, and (b) reflective of Internet and ICT development blueprints laid out by the World Bank, International Monetary Fund, United Nations special agencies, bilateral aid organizations, and diverse international non-governmental organizations. This policy model is an extension of older UNESCO-led "development communication" policies which instrumentalized mass communication mediums in third world countries as tools for disseminating critical information about agricultural production, health services, education opportunities, and similar social and economic resources.[10] Eko argues that the Internet developmentalist model

[9] Ukraine and Moldova are better described as "flawed democracies" than authoritarian or even hybrid regimes. Neither country is included on Gilbert and Mosheni's (2011) list of hybrid regimes, and both countries are labeled "partly-free" by Freedom House. But the "flawed" qualifier does suggest real civil liberties concerns.

[10] See Schramm (1964) for a full treatment on the role of information in developing countries during the Cold War.

was first articulated in a 1995 World Bank report which encouraged the international aid community to help developing countries in Sub-Saharan Africa become connected to the Internet. The report emphasized that "the information revolution offers Africa a dramatic opportunity to leapfrog into the future, breaking out of decades of stagnation or decline" (Baranshamaje, Boostrom, Brajovic, Cader, Clement-Jones, Hawkins, Knight, Schware, & Sloan, 1995; quoted in Eko, 2001, pp.478-479).[11]

While this international policy backdrop is important, the "developmentalist" label is problematic for several reasons. First, it is unclear if Eko intends this model to be broadly applicable to all developing countries or only those receiving substantial policy guidance from international organizations and donor agencies. The term "developing country" is something of a catch-all term—although it generally refers to countries that have not achieved a significant degree of industrialization relative to their populations, specific criteria for both "developing" and "developed" status vary from organization to organization. For instance, Eastern European countries with transition economies are sometimes grouped with developing countries based on their low or middle levels of per capita income, and sometimes with developed countries based on their high industrialization. The IMF uses a flexible classification system that considers (a) per capita income level, (b) export diversification, and (c) degree of integration into the global financial system. The World Bank classifies countries into four income groups (IMF, 2013; Soubbotina, 2004).

Second, not all developing countries have waited for the explicit prompting of international organizations and donor agencies to launch proactive Internet development policies, while others lacked (and continue to lack) the Internet infrastructure and other vital telecommunications resources necessary to initiate such policies in the first place. Furthermore, there is considerable national Internet policy variation even within the

[11] The USAID commissioned Leland Initiative—also known as the African Global Information Infrastructure—was among the first comprehensive development efforts to build IT infrastructure in Africa as a step toward African economic and social growth (Wheeler, 2011, p. 199).

Sub-Saharan African region Eko analyzes. Nigeria—a regional Internet leader with more than 45 million users and 26 percent penetration—features very few significant controls and no laws restricting online content. Other Sub-Saharan countries fit cleanly within the Cuba or Chinese model, with all service controlled by a state-owned or operated provider—such as the Ethiopian Telecommunications Corporation or Zimbabwe's TelOne—and all access and usage strictly regulated by a government agency. Some landlocked African countries with extremely low penetration levels (0 to 10 percent) effectively lack a functional regulatory framework at all.[12]

The term developmentalism also has some distinctly negative connotations related to its Cold War-era origins: Ting and Feng (1996) define developmentalism as a "set of ideas which emphasize the political primacy of economic development as dynamics of institutions and policies and as the fundamental means of political legitimacy" (p. 21). The authors note that in the case of both Latin America and parts of East Asia, the end product of developmentalism was embedded authoritarian (or semi-authoritarian) governing regimes, as economic success granted legitimate leadership status to political figures with dubious democratic credentials.

I use the label "developmental model" to avoid that connotational baggage and to cast a wider comparative net. The developmental model is observable in developing-level countries with proactive Internet development policies that leverage the technology as a tool for social and economic growth, and serve as an extension of ICT-driven development goals more broadly. The latter may include attracting foreign direct investment, increasingly the value-added output of domestic businesses, and creating technology hubs which facilitate both goals. Developmental model countries have Internet penetrations levels ranging from low (0 to 30 percent) to moderate (30 to 60 percent), and feature democratic governing regimes or even semi-authoritarian governing regimes, to the extent that the latter are willing to allow Internet development to proceed beyond their

[12] Although the few controls that exist place them in the Cuban model by default.

institutional span of *activity* control. Authoritarian regimes at this level of development (and Internet penetration) operate almost exclusively under the Cuba or Chinese model category even when the telecommunications market is partially liberalized, as political stability takes precedence over economic development.[13]

Developmental countries feature varying levels of Internet control, and may even maintain gateway model institutional arrangements through which a government ministry maintains substantial regulatory authority over otherwise private ISPs. However, filtering and surveillance in developmental model countries is simply less pronounced than in authoritarian or semi-authoritarian countries, and the democratic system provides a public check on Internet policy issues. That said, some countries clearly straddle the line between gateway-variation and developmental models.

**ICT and Development.** It is widely recognized that ICT can act as a catalyst for development and enable change across all economic sectors, especially in combination with other growth-promoting policies. Hanna (2003) identifies three different ICT policy goals that occur across economic levels, but are especially pronounced at the developmental stage. First, countries may develop and promote their national ICT infrastructure and industry (both hardware and software) to attract both market seeking and efficiency seeking foreign direct investment (FDI).[14] Second, countries may utilize ICT as a general purpose, value-added technology that can increase the productivity and competitiveness of the local economy—particularly among ICT-intensive industries and services.[15] Third and finally, countries may use ICT development as a part of larger policy strategy for social and community development, often in coordination with nongovernmental organizations and other civil society actors working to increase education opportunities

[13] Political control and economic growth are not mutually exclusive, of course, but as the earlier discussion of China's Internet policy makes clear, substantial Internet control mechanisms tend to be a drag on economic growth over the long term.

[14] Market seeking FDI is especially attractive in developing countries favoring import substitution strategies.

[15] The impact of investment in ICT infrastructure may span beyond targeted industries into all types of information-based and business-support services.

and economic agency. This latter goal is important as a policy backdrop that encourages governments to expand Internet access, but is ultimately of only marginal importance in the larger Internet control regime framework.[16]

ICT is of particular importance to landlocked developing countries (LLDCs), which tend to perform poorly as hosts for FDI. A UN report on FDI in landlocked countries highlights the global service and knowledge economy as a practical development alternative to manufacturing and other export sectors with potential high transaction costs, as geographic distance from ports and other hubs of commerce becomes largely irrelevant. The low-cost labor of some LLDCs is a significant advantage here, but the report notes that LDCs need to be proactive in generating worker skill sets that would attract such investment and enhance local technological capabilities (UNCTAD, 2003).

While Eko (2001, 2008) focuses almost exclusively on Africa—the region where World Bank influence on national Internet / ICT policy is arguably the strongest—the developmental model has been most pronounced (or at least effective) in Latin America and East Asia.

- Colombia has the second highest Internet penetration rate in Latin America (after Uruguay), due in large part to government-led ICT development efforts. Strong government support and tax breaks for foreign investors have accelerated Bogotá's position as a major South American tech hub (Mumford, 2013.)
- Proactive government initiatives in Argentina have increased penetration levels to 60 percent, while the country's investment friendly climate has attracted large, global high-tech corporations such as Motorola, Microsoft, Hewlett-Packard, IBM, Sony, and Google (Essinger, 2012).
- The Malaysian government has prioritized the development of broadband

[16] Cuban model countries, for instance, are unlikely to relax particular controls solely for the purpose of making online education or health care resources more accessible.

Internet infrastructure, and household penetration recently surpassed 60 percent. Tech companies receive ample tax incentives to relocate their operations to MSC Malaysia, the country's designated Special Economic Zone for tech. Startups receive assistance from government grants and private venture capitalists (Do, 2013).

- Internet penetration has increased to 36 percent in the Philippines, and users enjoy nearly unrestricted access to the Internet. The government's five year Philippine Digital Strategy plan include ambitious ICT infrastructure expansion. Like Ireland in Europe, the Philippines is especially attractive to tech investors because its citizens speak English. Tech companies are also able to piggyback on service linkages created by the thriving business-process outsourcing (BPO) sector (Freedom House, 2013b; Do, 2013).

Despite significant gains in Internet and mobile phone penetration across Africa—particularly Sub-Saharan Africa—the region does not have a strong record of success in establishing major tech hubs or generally utilizing the Internet and ICT to create value-added economic sectors, although recent evidence suggests this development gap may finally be closing. Kenya has been an especially prominent target for tech investment as its fiber-optic cables tie the country (and much of East Africa) to Europe and the Middle East, sparking hopes of an information-technology boom. The government hopes to create 120,000 BPO jobs by 2020 through the development of tech hubs and giant call centers built around economies of scale. Kenya, Ghana, South Africa, and other African nations hope to compete with outsourcing companies in India for the lower end of the BPO market (The Economist, 2010). Botswana's ICT development efforts are particularly interesting, as the government of the landlocked country has identified ICT as a critical component of economic diversification efforts. The country's ample diamond revenues are funding the construction of a colossal science and tech park that has been designed to place start-

ups, global corporations, and research and health organizations in a sprawling 57-hectare facility in the capital city of Gaborone (LaBarre 2011).

**Control Mechanisms.** Policymakers within developmental model countries implicitly or explicitly recognize that the long term benefits of ICT and Internet driven economic development outweigh any short term political or social instability that may result from largely unfettered access, and have thus relinquished a command-and-control regulatory approach, liberalized their telecommunications systems, and privatized state-owned telecommunications operators. In Malaysia, for instance, a government pledge to refrain from censorship of the Internet reflected a financial calculation to attract foreign investment, and was statutorily enshrined in the Communications and Multimedia Act of 1998, which regulates the country's telecommunications industry. The pledge was repeated in a bill of IT development guarantees to reassure foreign investors (OpenNet Initiative, 2012c). The regulatory backdrop in developmental countries is usually a mixture of self-regulation and co-regulation, especially with regard to infrastructure expansion and other telecommunications issues. Formal government regulatory intervention into Internet activity and content usually reflects familiar public interest concerns—namely, pornography and other obscene material, fraud and identity theft, and hate speech.

Latin American and African developmental countries feature very low levels of systematic technical filtering for political or security-related content. Prohibited content—especially child pornography—is usually removed or blocked through collaboration with ISPs. Colombia, for example, passed legislation in 2001 to prevent the online circulation of child pornography and to eliminate online content related to child prostitution. The law prohibits ISPs from hosting child pornography and requires them to provide customers with software to block all forms of pornography (OpenNet Initiative, 2013a).

Asian developmental countries tend to feature much higher level of filtering, and may even grant filtering authority to a government agency with regulatory authority over private ISPs in a similar fashion to gateway model countries. In India, for instance, the

Information Technology Act criminalizes the online publication of obscene information and grants the central government power to issue filtering directives through the Department of Information Technology. Indonesia grants similar authority to the Ministry of Communications and Information Technology, which carries out filtering through hardware and software installed by ISPs. Recent testing from the OpenNet Initiative (2012b; 2012c) in both countries revealed filtering on political, social, and security content, including some content with clear public interest. However, both countries' preferred censorship approach has been intermediary liability through content removal requests, including directives to social media platforms to remove content that could offend religious sensibilities, and select enforcement at the source mechanisms, especially for pornographic material (Freedom House, 2012). Despite the presence of these Chinese model-style control mechanisms, both India and Indonesia are democracies, and these control policies have emerged from parliamentary bodies accountable to the public. Nevertheless, such filtering and concentrated government control underscores the extent to which developmental model countries with high institutional capacity may retain a relatively effective span of control over their own Internet infrastructure.

Other developmental countries, however, suffer from a lack of effective control mechanisms due in large part to minimal institutional capacity. This regulatory gap is especially evident in Nigeria where domestic-based advance-fee fraud solicitations and similar scams have earned the country a negative reputation. Although such activities are explicitly illegal, the government simply lacks the resources to crack down on the practice (Eko, 2008). In Mexico and other Latin American countries, drug trade-based violence has extended onto social media platforms, creating a climate of self-censorship and highlighting the necessity of privacy protections (Freedom House, 2012b; Goodman, 2011). In addition, copyright protection is generally weak in developmental countries across the globe, even when international agreements such as the WIPO Copyright Treaty have been ratified.

**The United States Model**

Eko's (2001; 2008) typology of Internet regulatory regimes includes a "neo-mercantilist" model framed around libertarian economic principles. The neo-mercantilist model emerged in the United States, which adopted a hands-off regulatory posture after the technology was privatized and its commercial prospects became evident. This approach was encapsulated in the Clinton-Gore administration's 1997 document "Framework for Global Electronic Commerce," which conceptualized the Internet as a competitive marketplace of ideas, goods, services, and cultural content and advanced a vision and framework for expansion and governance of the Internet that emphasized e-commerce. The document was intended to be a policy blueprint for not only US regulation, but also an appeal to governments around the world to assume a similarly minimalist regulatory posture in order to best facilitate a global e-commerce network (Eko, 2012, pp. 228-229).

While the neo-mercantilist model is reflective of the United States' regulatory policy backdrop, the term's free-market connotations do not adequately reflect several critical and interrelated aspects of control unique to the United States. First, although the Internet regulatory backdrop in the US is largely self-regulatory, some important co-regulatory mechanisms do exist. Second, the presence of so many important Internet giants in Silicon Valley and elsewhere within the US gives the government regulatory authority over not only its own national corner of the Internet, but also the multinational tech corporations that shape Internet development and maintain giant troves of personal and business data for users across the globe. Third, the United States arguably has greater *functional* control of the Internet than any other country through its indirect control of the Domain Name System management body and global data encryption standards. Fourth and finally, recent revelations about National Security Agency (NSA) surveillance operations and cooperation and coordination with Google, Yahoo, and other tech companies suggest a unique convergence of the three control aspects identified above, and raise serious concerns about violations of user rights.

I use the term "United States model" here to avoid the connotational baggage of the term "neo-mercantilist" and to highlight the extent to which the model's control mechanisms are only found within the United States. While other countries do feature relatively *laissez faire* approaches to content and commerce regulation, the US model is narrowly applicable to its namesake due to the presence of the unique control mechanisms described above. The US's default position at the top of the Internet national regulatory hierarchy may shift, however, if the Internet continues to organically balkanize into culture and language-defined walled gardens anchored around national and regional online services providers and mobile apps less dependent upon global telecommunication standards.

**Regulatory backdrop.** No single agency regulates the Internet in the United States. The Federal Communications Commission (FCC), an independent agency of the executive branch, has claimed jurisdiction over some Internet-related issues as an extension of interstate communication, although it does not directly regulate the Internet or Internet service providers (ISPs). Other government agencies, such as the National Telecommunications and Information Administration (NTIA), play advisory or executive roles with respect to telecommunications, economic, and technological policies and regulations. The US Congress is the most important Internet policy maker, as the body creates important national Internet laws and delegates regulatory authority. Government agencies such as the FCC and the NTIA must act within the bounds of congressional legislation (Freedom House, 2013c).

As discussed ahead, government departments and agencies outside of the normal regulatory structure also exert a degree of control—both directly and indirectly—on the Internet and Internet companies. These include (a) the National Security Agency (NSA), which operates under the jurisdiction of the Department of Defense, and has coordinated with Silicon Valley-based tech giants to create a massive surveillance network, (b) the Department of Commerce and the National Telecommunications and Information Admin-

istration (NTIA), which together maintain unilateral oversight over ICANN operations and exercise the ultimate authority over the DNS root zone of the Internet, and (c) the National Institute of Standards and Technology (NIST), a non-regulatory agency of the Department of Commerce which developed an Advanced Encryption Standard (AES) capable of protecting sensitive communications which was widely employed by the US government, the private sector, and users around the globe.

Regulation of the Internet in the United States largely serves to facilitate and reinforce e-commerce and to ensure wide user access to the technology generally. For instance, in order to achieve uniformity to state electronic signature laws—which are critical to e-commerce transactions—the US government enacted the Electronic Signatures in Global and National Commerce, or E-Sign, Act of 2000, which preempted all existing state law and insured the security, reliability, privacy, and authentication of online transactions (Eko, 2001; Blythe, 2005). Although the United States has been an influential model for such regulation at the national and international level, policy makers within developed economies have been remarkably consistent in their efforts to promote and facilitate e-commerce, as the technology is widely perceived to reduce information asymmetries, lower transaction costs within national markets, and provide opportunities for business and consumers to access previously inaccessible markets (Deffains & Winn, 2012, p. 347).[17]

While the United States is one of the most connected countries in the world with penetration rates above 80 percent, the US has fallen behind countries like Switzerland, the Netherlands, Denmark, and South Korea in terms of Internet speed, cost, and broadband availability. The Universal Service Fund was established as part of the Telecommunications Act of 1996, and was designed to provide telephone service to underserved areas of the country. The fund uses fees applied to telephone bills to subsidize telecom

[17] National law reforms based on the UN's Model Law on Electronic Commerce appear to have satisfied business demands to remove legal obstacles to the use of e-commerce technologies, and future legal or political challenges are unlikely (Eko 2008).

providers that operate in underserved areas and would not survive in the marketplace without such support (Warf, 2013; Freedom House, 2013).

Approximately 4,000 ISPs operate in the United States, although fifteen of them control nearly 80 percent of the market, and four—AT&T, Comcast, Time Warner, and Verizon—control around 50 percent and own the majority of network cables and other infrastructure. The most important regulatory issue for ISPs over the last decade has been the principle of "network neutrality," according to which network providers must treat all data on the Internet equally, not discriminating or charging differentially by user, content, site, platform, application, or modes of communication. Supporters of the principle argue that without it, ISPs would be able to block (or change more for) Internet applications such as Netflix that require greater bandwidth usage, thereby imposing a tiered service model that would remove competition and create a segmented Internet not unlike cable television. In December 2010, the FCC issued a compromise ruling on the issue that instructs fixed-line service providers not to block access to, or unreasonably discriminate against, lawful websites, applications, devices, or services. The rules for wireless broadband providers are much more limited, however, and would not keep ISPs from charging more for faster access (Freedom House, 2013c; Lessig & McChesney, 2006, June 6).

US policy makers' conception of the Internet as a marketplace of ideas is important as it suggests a normative standard that—except in very limited circumstances explored ahead—the government may not regulate online "speech" on the basis of its subject matter or viewpoint. Litigation in the US concerning governmental efforts to regulate speech on the Internet has established that online communications including emails, shared files, and published content are to be accorded the full measure of First Amendment protection.[18] This high standard of free speech continues to distinguish the United States Internet control regime from other national models in the West. Internet

[18] That said, regulation of speech is uncontroversially constitutional with respect to threats, bribery, defamatory statements, fighting words, fraud, copyright violation, plagiarism, and other forms of speech that courts have decided the First Amendment, properly understood, does not protect (Levmore & Nussbaum, 2010).

regulation based on the ambiguous notion of public interest is used to block or shut down sites for hate speech in France and Germany and blasphemous content in Italy (Levmore & Nussbaum, 2010; Warf, 2013, p. 65).[19] Although there have been pushes for tighter content controls in the United States, legislative attempts at creating a mandatory filtering or screening system have failed to produce a comprehensive solution (OpenNet Initiative, 2010b).

Eko (2001) and Frydman, Hennebel, and Lewkowicz (2012) clarify that Internet regulation in the United States is not exclusively self-regulatory, as some co-regulatory mechanisms exist in three important areas: minors' protection and the fight against child pornography, security issues related to the fight against terrorism, and the protection of copyrighted materials. In these areas, the authors argue that various legal patterns illustrate an "invisible handshake" (Birnhack & Elkin, 2003) between the state and private actors, especially ISPs, which are enlisted in the implementation of the law.[20] Nevertheless, the authors emphasize that these co-regulation mechanisms are issue-specific exceptions against a broader self-regulatory policy backdrop, whereas in Europe co-regulation is the general and leading model of regulation of Internet content.

The US approach to online child pornography is fairly standard. Sexual content involving children is illegal in most jurisdictions, and international cooperation in creating a global legislative framework to prosecute individuals involved in its production and dissemination reflects a willingness by policy making actors to separate the regulation of this particular type of content from broader censorship issues (Taylor & Quayle, 2003).[21]

---

[19] For further details on the Italian authorities' crackdown on anti-Catholic websites domained in the United States, see Associated Press (2002).

[20] "Invisible handshake" is a term coined by Okun (1980) to refer to implicit contracts between employers and employees characterized by a mutual expectation of longevity. These agreements are enforceable only through the threat that if one party reneges, he or she will lose the benefit of the trust on which the relationship was founded.

[21] The United Nations Convention on the Rights of the Child provides the legal basis for the suppression of child pornography on the Internet. In this convention, member countries of the United Nations agreed to undertake the necessary actions to protect children from all forms of sexual exploitation and sexual abuse (United Nations General Assembly, 1989; Eko 2001).

US policy related to the issue is co-regulatory to the extent that it shares the burden of regulation with private actors. The 1998 Protection of Children from Sexual Predators Act and 2000 Children's Internet Protection Act compel ISPs and other Internet players to act as law enforcement intermediaries by providing user information to the government or by restricting access to controversial material (Frydman, Hennebel, & Lewkowicz, 2012).

National security initiatives in the United States compel ISPs and OSPs to share users' private Internet communications with government agencies in particular circumstances. According to the Patriot Act—amended by the 2002 Cyber Security Enhancement Act (CSEA)—law enforcement authorities may urge ISPs to disclose user communications relating to emergency security matters (Frydman, Hennebel, & Lewkowicz, 2012). Moreover, the CSEA (a) permits the voluntary disclosures of content and information on customer records to a law enforcement agency if the ISP "believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency," and (b) allows any government employee to conduct surveillance at the invitation of the ISP (Birnhack & Elkin-Koren 2003: 103-105).

Leaked documents from former National Security Agency (NSA) contractor Edward Snowden reveal that the agency has been compelling at least nine large US companies, including Google, Facebook, Microsoft, and Apple, to disclose content and metadata relating to e-mails, web chats, videos, images, and documents in order to collect "foreign intelligence information." Although the PRISM program under which such data collection occurs is targeted at persons abroad, the NSA is able to retain and use information "incidentally" collected about US persons (Freedom House, 2013c). Companies are legally required by the Foreign Intelligence Surveillance Act to hand over whatever information the government asks for under the law. But, as revealed in reporting from the *New York Times*, they are not required to make it easier for the government to get that

information—which is why Twitter declined to make as much information available as did Google, Facebook, and others (Miller, 2013, June 7).

Finally, US policy makers—acting at the behest of key stakeholders—have been relatively proactive in attempting to ensure online intellectual property right protection, in part through holding ISPs liable for illegal downloads and enlisting them in enforcement efforts. Like child pornography enforcement, national policy on the issue reflects international efforts at policy harmonization. The World Intellectual Property Organization (WIPO), a specialized agency of the United Nations, has led a multilateral approach to intellectual property through a series of treaties which made international copyright law applicable to the Internet (Delta & Matsuura, 2008). Intellectual property may refer to copyrights, patents or trademarks, as well as author's rights and moral rights (Eko, 2012, p. 280). According to the 1998 Digital Millennium Copyright Act (DMCA), an ISP that is unaware that it is hosting infringing material and does not take advantage of the infringing activity cannot be held liable. However, when a copyright owner notifies the provider about the infringement, the ISP must remove or disable access to the material within ten days to avoid liability for damages (Frydman, Hennebel, & Lewkowicz, 2012).

**Key interests.** Many of the largest and most important Internet and information technology companies in the world are headquartered in the United States. This includes Silicon Valley-based Google, Facebook, Apple, Twitter, eBay, Yahoo, HP, Intel, and Oracle, and Washington-based Microsoft and Amazon. The relationship between the tech sector and the US government is a complicated one, but each side has ample incentives to maintain a mutually beneficial "partnership," however uneasy. The tech sector is a critical component of the US economy. US tech companies—especially Apple and Google—routinely dominate global rankings of corporate brand leaders, and function as soft power intermediaries by winning over the "hearts and minds" of middle class consumers in emerging markets. The "brand gap" between these companies and their global competitors reflects positively on the US's entrepreneurial culture and business-friendly

regulatory environment. Apple—a brand associated with forward thinking products and a minimalist approach to design—is in many ways a symbol of the US's dynamism and strength in innovation, technology, and marketing (Interbrand, 2013; Chin & Collazo, 2012, Nov. 3).

The US government, in turn, has been an important—if underrecognized—benefactor to many tech companies. During the Cold War, the Department of Defense poured money into developing technologies at America's elite engineering schools, including Stanford, which used the money to fund the research and business ventures that created Silicon Valley.[22] While it is well known that the US Defense Advanced Research Projects Agency bankrolled the Internet, fewer people are aware of the extent to which CIA and military funded research facilitated the growth of GPS technology (which has critical to the success of smartphones), or that Apple and Intel's success came after both companies received early financing from the US Small Business Investment Company program created by Congress (Kim, 2013, Aug. 1; Mazzucato, 2013). In addition, the US government has backed US tech companies in important domestic and international court cases. A recent US International Trade Commission order, upheld by President Barack Obama's administration, blocks Samsung from importing or selling certain hardware found to infringe on Apple patents, while the US government, together with Google and Facebook, have undertaken a lobbying offensive against proposed EU data privacy laws (Decker, 2013, Oct. 8; Der Spiegel, 2012, Oct. 7).

Recent revelations stemming from former National Security Agency (NSA) contractor Edward Snowden suggest that the relationship between the government and these tech companies has been both more cooperative and more contentious than previously disclosed. The PRISM program operated by the NSA allows the government to scour the Internet usage of foreign nationals overseas who use any of nine US-based service

[22] The "Silicon Valley" description stems from the silicon chips used by Fairchild, Intel and other local semi-conductor manufacturers.

providers, including Apple, Facebook, Microsoft, Google, Yahoo, YouTube, Skype, AOL and the lesser known company PalTalk, which hosted a lot of traffic during the Arab Spring and the ongoing Syrian civil war. While these companies are legally required by the Foreign Intelligence Surveillance Act to hand over whatever information the government asks for under the law, they are not required to make it easier for the government to get that information. Although Twitter declined to comply with government requests for greater access to user information, other companies were more compliant and worked with government officials to develop better methods for efficiently and securely sharing the personal data of foreign users in response to lawful government requests (Miller, 2013, June 7).

**Functionality control.** Eriksson and Giacomello (2009) describe functionality as the technical quality of Internet usage, the most pertinent features of which—for the purposes of national and international-level control—are the technical protocols of Internet communication, including the Domain Name System (DNS), and the data encryption algorithms necessary for secure digital communication and data protection.[23] Because the United States government was involved in the early development of the Internet, many parts of the Domain Name System were originally performed by either US government agencies or pursuant to contracts by US government agencies. But as the Internet expanded globally and commercially, total US control became untenable. Instead of turning administrative authority over to an international body such as the UN's International Telecommunication Union (ITU), in 1998 the Clinton Administration created the Internet Corporation for Assigned Names and Numbers (ICANN) as a not-for-profit organization incorporated under California law, effectively privatizing several critical administrative functions—including DNS management, IP address space allocations, protocol parameter assignment, and root server system management functions—in order to keep that critical

[23] Eriksson and Giacomello (2009) do not specifically identify encryption as a functional control, but including it here is a reasonable inference given its centrality in digital communication.

aspect of Internet governance out of the hands of world governments and UN bureaucrats. The Department of Commerce and the National Telecommunications and Information Administration (NTIA) oversee ICANN, and exercise the ultimate authority over the DNS root zone of the Internet (Feld, 2003; Brito, 2011, March 5).[24]

ICANN is not the Internet's sole administrative body. Two other groups— the Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C)—develop the standards for how information is shared and displayed through the Internet and on the web. The groups have substantial consultative and technical power but very little national oversight—in no small part because their efforts rarely if ever pose a threat to national interests. And while the Internet couldn't work without regional IP registries, they are effectively nodes in the system carrying out functions dictated by ICANN.[25] The US has reaffirmed its delegation of the DNS management to ICANN while insisting it could intervene in case of an emergency. A 2009 "Affirmation of Commitments" between the US government and ICANN permitted the corporation more independence, but preserved the government's power to take over the root server in an emergency (Kravets, 2013, Oct. 14; Meyer, 2013, Oct. 16).

Governments like China, India, and Russia have long distrusted ICANN, and lobbied for DNS management to be turned over to an organization such as the ITU. But criticism of the United States' role in the system became more pervasive in the wake of the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). The House and Senate proposals, respectively, were introduced in 2011 to stop the theft of intellectual property through foreign-based websites. Both bills were variants of strategies introduces in the 2010 Combating Online Infringement and Counterfeits Act (COICA), which was directed primarily at domestic websites. Both SOPA and PIPA would have required ISPs to stop

[24] The extent to which ICANN can be said to "control" the Internet is often overstated. Penenberg (2005) notes that while ICANN's function is important, most online traffic exists outside the traditional domain-name system in peer-to-peer file sharing and instant messaging.

[25] ICANN assigns not only top-level domains—the dot-suffixes like .com and .edu—but also country codes like China's .cn and the United Kingdom's .uk.

referring requests for websites hosting infringing content to their assigned IP addresses, and would have required search engines to stop linking to these sites as well.

Critics raised numerous concerns about both bills, not least of which that they would undermine the integrity of the Domain Name System and the development of Domain Name System Security Extensions (DNSSEC), a set of security protocols that fix fundamental vulnerabilities in the DNS. Provisions related to DNS redirection were eventually pulled from SOPA, and both bills were eventually tabled after intense voter pressure and online activism (Herman, 2013; Masnick, 2011, Dec. 9). In 2012, however, the US government admitted to seizing at least 750 dot-com domains registered *outside of the US* for allegedly breaching federal copyright and trademark laws. This was followed by the Snowden leaks in 2013, which revealed the extent of the NSA's global surveillance machine and further undermined trust and confidence in the US government's ability to objectively administer technical features of Internet governance, even indirectly (Kravets, 2012, March 6; Kravets, 2013, Oct. 13; Meyer, 2013).

Encryption standardization is another critical aspect of both functionality (as the code through which digital information is securely transmitted) and activity (as the ends to which encryption is a means). While some countries—usually authoritarian—set their own national encryption standards to better control the information environment,[26] most countries rely upon standards endorsed by the International Organization for Standardization (ISO), an international standards body composed of representatives from standards organizations from several countries. The National Institute of Standards and Technology (NIST), a non-regulatory agency of the Department of Commerce, is charged with recommending cybersecurity standards in the United States, and is a key player in the ISO. A recent *New York Times* report revealed that the NSA used its influence as the world's most experienced code maker to covertly introduce a "back door" into a 2006 standard

[26] In Tunisia under Ben Ali, for instance, ISPs were prohibited from transmitting encrypted information approval.

adopted by NIST and later by the International Organization for Standardization, which counts 163 countries as members (Perlroth, Larson, & Shane, 2013, Sept. 5).

While the compromised portion of the algorithm was relatively simple to replace, NIST publicly discouraged tech companies from using that cryptographic approach. Other revelations suggest the compromise was part of a broader, multi-pronged effort by the NSA to break widely used Internet encryption technologies. According to the *Times*, cryptographers "have long had mixed feelings about [NIST's] close relationship with the [NSA]," but the back door revelations "confirmed their worst fears and eroded their confidence in [NIST] standards entirely" (Perlroth, 2013, Sept. 10).

**Surveillance.** Government-led Internet surveillance in the United States and other countries will generally occur outside of the normal Internet regulatory apparatus, and often under the purview of law enforcement or state security agencies. The NSA operates under the jurisdiction of the Department of Defense and reports to the Director of National Intelligence. Much of the NSA's surveillance operations occurred under the rubric of "signals intelligence" (often contracted to SIGINT). The NSA's domestic eavesdropping program was originally designed to locate al-Qaeda terrorist cells suspected of still operating in the United States, and the organization possesses only limited legal authority to spy on US citizens. Nevertheless, it has constructed a surveillance network with the capacity to reach around 75 percent of all US Internet communications (Gorman & Valentino-Devries, 2013, August 20).

Such a large number clearly constitutes a substantial degree of "control" over the Internet in terms of both activity and functionality. However, the extent to which such control is legal or necessary is difficult to ascertain. In December 2013, two federal judges reached polar opposite conclusions about the legality of the NSA's data collection programs. Judge William H. Pauley III in New York endorsed arguments made by senior government officials that such data collection was a necessary tool for effective counter-terrorism efforts, and ruled that bulk data collection was lawful. Two weeks prior, Judge

Richard J. Leon in Washington ruled that the government had failed to make the case that the program was necessary, and further data collection was probably unconstitutional (Liptak & Schmidt, 2013, Dec. 28, p. A1). Freedom House's Freedom on the Net coding system for surveillance includes the important—if ambiguous—caveat "without judicial or other independent oversight," and although the organization details concerns about the NSA's efforts in its most recent report on the United States (2013c), it still ranks the country as *Free*.

The FBI has followed the NSA's lead in expanding its wiretapping capabilities. The 1994 Communications Assistance for Law Enforcement Act (CALEA) forces telephone companies to provide backdoors to government so that law enforcement agencies can spy on users after obtaining court approval. CALEA was expanded in 2006 to reach Internet technologies like peer-to-peer voice-over-Internet protocol services. A recent proposal by the FBI would allow law enforcement agencies to listen in on any conversation online, regardless of the technology used, by mandating engineers build "backdoors" into communications software. Companies would be ordered to comply, and judges could impose fines if they did not (Savage, 2013, May 7).

**European Model**

Eko's (2001; 2008) typology of Internet regulatory regimes includes a "Euro-Communitarian" model reflective of a "Euro-governmentality" and the hierarchical relationship between the European Union and member states. This regulatory model represents a market-based system of governance characterized by the formulation and transfer of directives, in specific issue areas of Internet communication, from the European Union to its member states for purposes of policy harmonization.[27] However, it should be emphasized that while such directives have binding force in relation to the result to be achieved for each member state, they do not explicitly dictate the forms and methods for

[27] The EU uses directives to bring different national laws into line with each other, and they are particularly common in matters affecting the operation of the single market (e.g. product safety standards).

achieving that result. Directives can thus be distinguished from EU regulations, which are self-executing and do not require any implementing measures. Directives may oblige national legislatures to amend national law only to the extent necessary for the functioning of the Single Market.

Important aspects of Internet control policy—including the definition and designation of "illegal" online content and specific telecommunication data retention policies—vary between EU member states, and enforcement on these issues will continue to reflect each country's institutional capacity. Furthermore, the EU does not have its own intelligence or surveillance agency. Each member state maintains its own security and intelligence agencies, which vary considerably in their surveillance and data gathering capabilities. Freedom House, the OpenNet Initiative, and Reporters Without Borders all analyze EU member states' Internet policies individually, and that approach is unlikely to change in the years ahead. Moreover, Switzerland, Norway, and several smaller countries are not part of the EU, but their co-regulatory approach to the Internet is quite similar. As such, I use the category label "European model" to reflect the regional and hierarchical aspects of this model without giving EU directed policy harmonization undue descriptive weight.

Europe is the region with the highest Internet penetration rate in the world (75 percent), but the continent features a wide spectrum of Internet penetration levels ranging from exceptionally high (Iceland at 96 percent) to relatively low (Moldova at 43 percent). In 2013, the average penetration rate across the continent (including Russia) was 75 percent. However, rates of usage vary widely, and are typically much higher in Northern and Western Europe than in Eastern and Southern parts. This digital divide reflects long-standing socio-economic differentials (Warf, 2012, p. 27; ITU, 2013).

**Regional Policy**. European Commission policy papers from the early 1990s echo many of the same themes as the United States' preferred Internet development approach: business leadership balanced with government efforts to expand accessibility. The Com-

mission's 1994 "Europe and the Global Information Society" report—which came to be known as the "Bangemann Report" after the German Commission chair—touted the ability of a liberalized and Europe-wide market to deliver the benefits of an "information society" in terms of economic growth, new services, and employment opportunities. At that time, most European governments were still in direct control of their national telecommunications sector and remained wedded to traditional interventionist policies in regard to industrial and technological affairs. The report set the tone for a series of liberalizing directives issued in the area of telecommunication terminals, services, and infrastructure (Ducatel, Webster, & Herrmann, 2000; Savin, 2013, pp. 25-26).[28]

Two focal points of EU intervention in the field of Internet regulation began to crystallize: one centered around the Single Market and the other around consumers, citizens, and public interest concerns (Savin, 2013, pp 3-4). The Electronic Commerce Directive (ECD), adopted in 2000, reflected the former and harmonized rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts, and limitations of liability of intermediary service providers. Furthermore, the proper functioning of the Internal Market in electronic commerce was ensured by the Internal Market clause, which meant that information society services were (and are), in principle, *subject to the law of the member state in which the service provider is established*. In turn, the member state in which the information society service is received cannot restrict incoming services (European Commission, 2000).

The EU adopted a new regulatory framework in 2002 meant to (a) cover the Single Market and competition issues, and to (b) improve the development of new infrastructures and technologies. The framework reflects the convergence between fixed and

[28] On the heels of the report, a series of national-level information society strategies were produced. These included the French *Information Autoroutes Report* in 1994, the UK *Information Society Initiative* and German *Path to the Information Society* in 1996, the Irish *Information Society Steering Committee* in 1997, and the Danish *Information Society* in 2000 (Ducatel, Webster, & Herrmann, 2000).

mobile telecommunications and between broadcasting, telecommunications, and information technology more broadly, and effectively puts all telecommunication services under a single regulatory framework (Savin, 2013, pp. 25-26). The European Union has also adopted a series of telecommunication policies designed to promote Internet access, particularly the diffusion of broadband. In 2005, the European Commission launched i2010, an information society initiative intended to enhance Internet access across the continent. This goal was explicitly articulated in the Lisbon Strategy of 2010, which was implemented with the broader aim of accelerating the continent's shift into a competitive, knowledge driven economy (Warf, 2013, p. 28).

Other directives from the Commission reflected a recognition that the impact of the Internet extended beyond e-commerce into the everyday activities of private citizens. In October 1996, the Commission produced a report titled “Illegal and Harmful Content on the Internet” and a Green Paper on “The Protection of Minors and Human Dignity in Audiovisual Services” in response. Based on these documents, “a common framework for self-regulation (of the Internet) at the European level” was drafted, which culminated in an Action Plan on Promoting Safe Use of the Internet, which was adopted in 1999 (OpenNet Initiative, 2007b). The Action Plan emphasized the need to take steps in five broad areas in order to curb illegal and harmful content on the Internet:

1. Promoting voluntary industry self-regulation and content monitoring schemes, including the use of hotlines for the public to report illegal or harmful content;
2. Encouraging Internet service providers to provide filtering tools and rating systems that enable parents or teachers to regulate the access of Internet content by children in their care, while allowing adults access to legal content;
3. Raising awareness about services offered by ICT firms to allow users to control access to content;
4. Exploring the legal implications of promoting the safer use of the Internet; and
5. Encouraging international cooperation in the area of regulation.

Although originally planned as a three-year program, the Action Plan was extended in 2002, and its objectives were widened to cover new and emerging communication technologies. While the 2002 Action Plan largely left implementation to individual states, the 2005 Safer Internet Program aimed to give the EU broader powers and new tools to achieve these goals itself (Deibert, 2010, pp. 279-281).[29]

Both the Action Plan and the Electronic Commerce Directive established the EU's preferred co-regulatory approach to Internet content regulation. The term "co-regulatory" gives a sense of the joint responsibilities of market actors and the state. Frydman, Hennebel, & Lewkowicz (2012) note that the text of the ECD provides a "regime of liability limitations" less favorable to ISPs than the immunity clause in the United States' Communications Decency Act. The language also allows for a degree of state intervention—a position, the authors note, consistent with the European view that "freedom of speech should be subject to certain restrictions, liabilities, and penalties that justify the intervention of public authorities" (pp 138-140).

Although the adjectives "illegal" and "harmful" are often grouped together in reference to online content, there is a critical distinction between them, as the former refers to content criminalized by national laws, while the latter refers to content considered offensive or inappropriate by some people. Harmful content includes legal content which may offend some Internet users or content which may be thought to harm some but not all users, such as pornography that is accessible by children (Akdeniz, 2001, p. 304). Under the Safer Internet Program, the exact definition and categorization of illegal content is intended to vary between member states, especially with regard to hate speech and sexually explicit content. Nazi memorabilia, for example, remains illegal in France and Germany but not in Italy. There is no explicit obligation at the EU-level mandating either governments or ICT firms to filter or remove any particular form of online content

[29] Among other things, the 2005 program included EU-level funding for hotlines for citizens to report offending content, sponsored education efforts on consumer and data protection, and authorized new studies into filtering technology for illegal content (Deibert, 2010).

(Deibert, 2010). Child pornography, however, was and is illegal across all jurisdictions in Europe, and such content matter remains one of the primary impetuses for policy intervention at both the EU and national level.[30]

Commission directives have aimed to not only target particular kinds of content, but to protect user privacy as well. The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence," subject to certain restrictions, and the European Court of Human Rights has given this article a very broad interpretation in its jurisprudence (Sauter, 2011, p. 294). As a result, the EU features some of the world's broadest and most stringent data privacy laws. The EU Data Protection Directive (DPD) implemented in 1998 regulates any "data controller"—that is, anyone who "processes" data they collect. The Directive imposes three relatively stringent requirements on such individuals or companies: First, they must tell consumers *why* they are collecting personal data and receive consent "unambiguously" before proceeding; second, data must be used only for the purposes stated during collection and not redirected to other purposes; third and finally, the data collected must have a reasonable relationship to the purposes for which it is collected. In addition to these basic requirements, the Directive adds extra protection for "special categories," namely, "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (EU Directive, 1995; Goldsmith & Wu, 2006, pp. 174-175).[31]

---

[30] The early results of the Action Plan initiated hotline system—known as the International Association of Internet Hotlines (INHOPE)—were promising: between March 2003 and February 2004, the hotlines processed more than 250,000 reports, more than one third of which were related to child pornography, child trafficking, and sex tourism (INHOPE, 2004). The program subsequently expanded to 38 countries worldwide, including some outside of the EU. In 2012, INHOPE's 150 analysts processed 1,059,758 reports of illegal content. 96 percent of identified illegal content was reported to law enforcement within a day, and 88 percent of it was removed from the Internet within a week (INHOPE, 2012).

[31] The 2002 Electronic Communications Sector Directive (the "E-Privacy Directive") and its 2009 amendment further clarify this protection by requiring anyone who places cookies—small pieces of data that web

Goldsmith and Wu (2006) note that what makes the DPD particularly controversial is its aggressive geographic score. Article 4 of the Directive applies not only to companies established in Europe but also to any company that makes use of data processing "equipment" or "means" in Europe, and to any company that may be reached "by virtue of international public law." This means that EU countries can directly apply their national data protection legislations to non-EU based websites whenever they would make use of equipment located on the territory of the said countries (although not when the equipment is used "solely for the transit purposes"), and this language has been interpreted by European officials to reach nearly any company that collects information from European citizens (EU Directive, 1995; Goldsmith & Wu, 2006, pp. 175-177).

In July of 2002, the EU Internet Task Force began an investigation of Microsoft's Passport system—the predecessor to Windows Live ID, which was intended to function as a single sign-on service for all web commerce—to see if it complied with the 1998 DPD. As issue was whether Microsoft was collecting more data than it needed for the purposes of its program. The EU had considerable leverage in its challenge of the American-based software giant as the European market accounted for about a third of Microsoft's sales. Capitulation was a foregone conclusion, and by January 2003 Microsoft and the EU had an agreement. Microsoft would "substantially modify" its Passport service to conform to EU privacy laws, including granting more user control over how data is shared (Goldsmith & Wu, 2006, pp. 175-177; Bennett, 2008, pp. 158-159).

In 2012, the European Commissioner for Justice, Fundamental Rights, and Citizenship, announced a sweeping new "right to be forgotten" privacy proposal which would require companies like Facebook and Google to remove (a) content that a user posts about themselves and later regrets or simply wishes to see removed, even if said

---

servers pass to a user's web browser while the user is browsing that website— to provide a "clear and precise" statement of what information was placed on the "terminal equipment." The Directive also requires data controllers to ensure that the method for informing subjects must be "user-friendly.," and that users are provided with meaningful opportunities to refuse those files from being mechanically stored (Tsesis, 2013).

content (especially photos or comments revealing personal information) have already been widely distributed, and (b) content that another users posts about someone else that the second party finds objectionable. The onus would then falls on the original user to prove that the said content falls within the exception for journalistic, artistic, or literary content. Under the language of the proposal, Facebook and Google could be held liable for up to two percent of their global income if they fail to remove content when requested. The right was designed to address a real problem familiar enough to anyone with a digital footprint on social media networks, but its approach is so broad that *New Republic* editor Jeffrey Rosen (2012) referred to it as “the biggest threat to Internet free speech in the coming decade," and warned that unless the right was scaled back and more precisely defined, it could "transform Google, Yahoo, and other hosts of third party content into censors-in-chief for the European Union, rather than neutral platforms.”

The "right to be forgotten" has been rebranded as the “right to erasure” in the imminent EU Data Protection reform. Article 17 of this new EU General Data Protection Regulation represents a lesser obligation for content hosts than the original proposal, but still gives data subjects the right to request that data controllers delete any personal data relating to them, and ensure there is no further dissemination of such data (Baker, 2013, Oct. 21). The reform is also intended to establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws, and thus creating a single supervisory authority instead of a far-more-cumbersome twenty-eight. But the proposed reform suffered a major setback in December 2013, after the European Council's legal service chief questioned whether this "one-stop shop" measure was lawful, opining that it might breach European citizens' human rights (Fiveash, 2013, Dec. 9).

Goldsmith and Wu (2006, p. 176) note that the combination of Europe's enormous market power, its concern for its citizens privacy, and the impracticality of tech companies implementing privacy policy changes in one region only has effectively transformed European Union directives into global law. This is due to a simple economy-of-scale

assessment. The California emissions standards is an illustrative example of this effect: when California sets new emission standards for cars, it is more cost effective for automotive manufacturers to build cars to the California standard for the entire United States rather than producing two sets of the same vehicles. This is known as the "California Effect," and the influence of European Union directives on tech policy issues is evidence of a similar "EU effect" operating on a larger scale.

**National policy.** While EU Directives produce policy harmonization on Single Market-related telecommunication, e-commerce, data privacy issues, a number of important Internet control policies remains firmly in the ambit of national governments. Perhaps most critically, national policy makers dictate the definition and designation of "illegal" and "harmful" online content and decide what measures should be taken to filter or otherwise censor it. National courts have also pushed back against the 2006 EU Data Retention Directive (DRD), thus staking out a degree of policy autonomy in this controversial area. Finally, EU member states maintain their own state security and intelligence agencies, which vary considerably in their surveillance and data gathering capabilities.

While European countries generally maintain relatively liberal free speech policies, several governments do attempt to restrict certain types of online content. These efforts stand in sharp contrast to the American conception of free expression. Most of these restrictions relate to intellectual property and certain types of pornography—especially child pornography, but also sexual content labeled as "extreme"—rather than overt attempts to stifle political dissent. More controversially, however, some European nations have in place laws prohibiting incitement to racial hatred, the espousal of neo-Nazi views and ideologies, Holocaust-denial, and the display, possession, or sale of neo-Nazi memorabilia. The source of the proscribed content is generally irrelevant; the laws apply as long as said content is made available to citizens of the respective European country.[32]

[32] French criminal law, for example, applies where criminal offences are committed on the territory of the French Republic (Article 113-2 of the Penal Code) and where a primary offence committed in another country is aided and abetted in France (Article 113-5).

This, of course, means that European courts can attempt to impose their restrictive speech laws on US-domained websites that are acting within their rights under the laws of the United States. Understandably, this leads to complicated and controversial disputes, including one of the most well-known and widely cited challenges to the conception of an unregulable Internet: LICRA vs. Yahoo (Paulson, 2003).

In 2000, a French judge ruled that US-based Yahoo! Inc. had to prevent French users from accessing a Yahoo hosted site auctioning Nazi memorabilia or pay a hefty fine. Yahoo CEO Jerry Yang defiantly stated that the company would not "change the content of our sites in the United States just because someone in France is asking us to do so," and the company's lawyers appealed on the grounds that such geographic based filtering was technically impossible (Goldsmith & Wu, 2006, pp. 5-7). Several American and European experts, however, testified that IP-identification technology could effectively filter the content for 90 percent of French users, and the judge upheld the decision. Yahoo finally removed the Nazi-related content from the French version of its portal, although only after the French court threatened to seize the company's French assets, including income from a sizeable subsidiary (Breindl, 2013). Goldsmith and Wu (2006), and others have noted that the Yahoo! decision seemed to undermine the illusion of a borderless Internet. In the French conception, the Internet must honor national borders and national laws. The decision represented "a direct attempt by a foreign nation to apply its law extraterritorially to restrict the expression of US-based online speakers who are protected by the First Amendment" (Corn-Revere, 2003, p. 223).

Several incidents in the early aughts exemplified the friction between European speech restrictions and the relatively unrestricted online content streaming from websites domained in the United States and elsewhere outside of Europe. In 2002, Italian police closed down five US-based websites featuring *blasphemous* content, which remains illegal not only in Italy but in several countries across Europe, including Denmark, Germany, Greece, Malta and Poland. The websites in question were created in Italy and hosted by

Internet providers in Washington, D.C., and California. Police used the suspects' computer to remove the offense material from the US-domained websites and replace it with crest of the special police unit involved in the case. The crackdown followed a Vatican position paper calling for restrictions on the Internet's "radical libertarianism " (Associated Press, 2002, July 10; Corn-Revere, 2003, p. 224).

In 2001, *Der Spiegel* reported that the German Interior Minister Otto Schily was contemplating perpetrating denial-of-service attacks to disable neo-Nazi websites domained in the United States. Such attacks would be legal, according to Schily, because they represent "the defense of our system of laws against illegal attacks by those who consciously exploit the international medium of the Internet." Schily later backed off that idea, and instead pressed US Attorney General John Ashcroft to exert pressure on an American Internet service provider to remove the offending content (Kettmann, 2002, Jan. 10; Greene, 2001, April 9; Patalong, 2001). In 2002, a German district government obliged 56 ISPs to restrict access to four websites domained in the United States which contained right-wing extremist material.[33] Furthermore, according to a study published by the Berkman Center for Internet and Society in 2002, a number of websites with neo-Nazi and other objectionable material were completely or partly excluded by the German version of the search engine Google. YouTube has also removed content to comply with the demands of German law (Deibert, 2010c; Zittrain & Edelman, 2002).

While European governments have attempted to impose speech restrictions universally, European national courts have emerged as an important defender of user privacy domestically. The EU Data Retention Directive (DRD) was proposed following the terrorist attacks of September 11th attacks as part of a flurry of anti-terror measures in the EU. The Directive obliges all ISPs and telecommunications service providers operating in Europe to collect and retain a subscriber's incoming and outgoing phone numbers,

[33] Because of the federal structure of Germany's political system, Internet content removal and filtering can be initiated at the regional level.

IP addresses, location data, and other key telecom and Internet traffic data for a period of six months to two years for later access by law enforcement. Many EU member state transposed the Directive into national legislation, including Austria, Bulgaria, Denmark, Estonia, France, Italy, Latvia, Liechtenstein, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Norway, and the United Kingdom. Countries outside the European Union such as Serbia and Iceland have also adopted data retention laws (Ermert, 2013, July 05; EFF, ND).

But the DRD was met with considerable resistance in several member states. While mass protests did not kill the legislation, national Constitutional Courts have issued decisions striking down national data retention laws for violating human rights. Nations contesting the Directive include Cyprus, Czech Republic, Germany, Greece, and Romania. The DRD was adopted in Romania, but declared unconstitutional in 2009. In February 2011, Cyprus declared their national data retention law unconstitutional. The Courts in Bulgaria declared mandatory data retention laws unconstitutional and the German law adopting the Directive was declared unconstitutional in March 2010 (Ermert, 2013, July 05; EFF, ND). In December 2013, the Advocate General of the European Court of Justice opined that the directive is incompatible with Article 7 of the Charter of Fundamental Rights. The case combined challenges from Austria and Ireland that wanted proof that massive data collection is proportionate, necessary, and efficient. While the opinion is not binding on the European Court of Justice, in the majority of cases advocate general opinions are followed (Robinson, 2013, Dec. 12; Ermert, 2013, Dec. 13).

**Surveillance.** The European Union has never established a EU-level intelligence agency, although there have been recent calls to create one as a "counterweight" to the US's National Security Agency (Whittaker, 2013, Nov. 5). However, the EU does possess some intelligence assets. The European Police Office, or Europol, is essentially an analytical intelligence agency, while the EU Intelligence Analysis Centre (INTCEN) is a small foreign intelligence analytical unit that reports to the External Action Service,

the EU's embryonic diplomatic corps. Both agencies handle data categorized as signals intelligence—including Internet communication—however, neither Europol nor INTCEN maintain their own intelligence collection facilities (Jeffreys-Jones, 2013, pp. 222-223; Jeffreys-Jones, 2013, March 19). INTCEN's staff is very small—a mere 70 people, including temporary agents—and the agency depends upon the security and intelligence services of member states (European Parliament, 2012). The European Union Agency for Network and Information Security (ENISA) works to prevent and address network security and information security problems, and releases an annual "Threat Landscape" report that identifies the top cyber-threats. Its operations are, however, better categorized as information analysis than intelligence gathering.

Many of the national intelligence services are quite sophisticated. Recent reporting from *The Guardian* (Borger, 2013, Nov. 2; MacAskill, Borger, Hopkins, Davies, Ball, 2013, June 22)—largely drawn from Britain intelligence agency documents leaked by former NSA contractor Edward Snowden—suggests that the German, French, Spanish, and Swedish intelligence services have all developed methods of mass surveillance of Internet and phone traffic over the past five years in close partnership with Britain's GCHQ signals intelligence agency, which has also collaborated with the NSA. Like much of the NSA's eavesdropping, this bulk monitoring is carried out through direct taps into fiber optic cables and through covert relationships with telecommunications companies. The communications GCHQ has been able to capture include phone call recordings, email messages, Facebook posts, and users' Internet browsing history for both targeted suspects and entirely innocent people. All of GCHQ's communication surveillance activities have been deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets.

*The Guardian's* analysis of the Snowden documents emphasizes that "GCHQ has become Europe's intelligence hub in the [I]nternet age, and not just because of its success in creating a legally permissive environment for its operations. Britain's location as the

European gateway for many transatlantic cables, and its privileged relationship with the NSA has made GCHQ an essential partner for European agencies" (Borger, 2013, Nov. 2, p. 1). The leaked documents suggest that the French and Spanish agencies had comparable capabilities, largely owing to their relationships with unidentified telecommunications providers. Swedish and Dutch agencies appeared to have more limited capabilities, owing in part to legal restrictions, although the GCHQ has provided legislative guidance to both countries.

A recent joint study by the German think tank *Neue Verantwortung* and the US-based New America Foundation found that the legal foundations, focus, and government oversight of the NSA, GCHQ, and *Bundesnachrichtendienst* (BND), Germany's intelligence service, are all quite similar. The report finds that the underlying laws supporting the programs have the same structure, although the "interpretation of how these laws are applied may diverge (Heumann & Scott, 2013, p. 2).

The authors criticize the weakness of legal controls for intelligence services, which they argue are far too limited:

> In all three countries the intelligence agencies enjoy great discretion and independence when it comes to the collection of foreign intelligence. Legal restrictions and oversight mechanisms are only concerned with the protection of the rights of each country's own citizens. And, in most cases, these restrictions come into place mainly after the interception and collection of telecommunications traffic has already occurred (Heumann & Scott, 2013, p. 2).

All three countries, they conclude, lack robust systems for judicial review to protect citizens from undue surveillance. The authors note that of the three countries, Great Britain has the weakest oversight mechanisms as it lacks institutionalized review of surveillance programs from both the legislative and judicial branches of government (Heumann &

Scott, 2013; Biermann, 2013, Oct. 4).

**Key Interests.** The presence of large Internet and ICT companies within a country should confer a greater degree of Internet control to the extent that said companies are regulated by domestic laws and cooperate with government intelligence agencies.[34] But while Europe features enormous market power that it has leveraged into substantial influence in tech privacy policies, the region's tech sector is not especially strong—especially when compared to the United States. Only four European companies—SAP (Germany), Accenture (Ireland), Atos (France), and Ericsson (Sweden)—are included in Booze & Company's most recent ranking of the world's top 20 ICT companies (Acker, Geerdes, Frone, & Schroder, 2013). And none of the world's top 10 dot-com Internet companies on the *Forbes Global 2000* list are European (DeCarlo, S. (2013).

The tech sector gap between Europe and the United States is becoming more pronounced for several reasons. First, Silicon Valley is uniquely appealing to Euro-born tech entrepreneurs because of it deep talent, linkages with nearby tech players, and ample venture capital funding. Second, Europe features strict labor laws which are acutely problematic in the tech sector, with features high job mobility and fast growing competitors. Third and finally, fewer European graduates are entering the job market with engineering, science, or technology degrees, and tech companies have had to look elsewhere for top talent (Palmer, 2011, June 8; Alderman, 2014, Jan. 3).

This imbalance is unfortunate given the World Wide Web's European roots. While the modern Internet is generally perceived as an American invention, British computer scientist Tim Berners-Lee invented the Web's hyperlink system while working for the European Organization for Nuclear Research (CERN) in Geneva. Not only did Berners-Lee lay the foundations for the Web, he founded the World Wide Web Consortium (W3C) in

[34] This is not true in all instances, of course. Many hedge funds are domained in the Cayman Islands, and few if any observers would argue that the national government there exude much influence over global finance. But states with even a moderate institutional capacity are generally able to leverage the presence of large tech companies into at least a degree of Internet control.

1994 to set standards and specifications for the Web's growth. France also contributed to the technology's growth through Minitel, a popular and influential pre-World Wide Web online service developed at the behest of the French government in the late 1970s (Jones, 2003; Schofield, 2013, June 27).[35]

One tech field Europe excels at is piracy. The Pirate Bay—one the largest and most notorious piracy sites (hence the name)—was founded in Sweden in 2003. The Pirate Bay and other Swedish file sharing sites are part of a strong and influential anti-copyright movement in the country whose values are perhaps best expressed by the country's "Pirate" political party. Pirate Parties have also emerged in Austria, France, and Great Britain (Miegel & Olsson, 2008; Putzier, 2013).

The 2004 EU Directive on the civil enforcement of intellectual property rights (known as the "(IPR) Enforcement Directive") required EU member states to apply effective remedies and penalties against those engaged in copyright infringement. But the directive was substantially changed due to widespread criticism of its seemingly draconian approach, and the national laws that followed proved to be largely fangless (Whittaker, 2013, April 15). An International Chamber of Commerce report claimed that Europeans downloaded €10 billion worth of pirated music, film, television shows and software from the Internet in 2008 (Tera Consultants, 2010).

More recent national Internet control policies across Europe represent a crackdown on illegal downloading. Perhaps most notable among these is HADOPI, a French anti-piracy law introduced during 2009 by the then president Nicolas Sarkozy that would have disconnected users suspected of copyright infringement from the Internet after multiple violations. France's highest court, the Constitutional Council, subsequently declared the main part of the bill unconstitutional on the grounds that it violated the 1789

[35] Subscribers and terminal users could use the service to search the telephone directory, make train reservations, check stock prices, and chat with one another well before America Online and other companies brought the World Wide Web to American homes. At one point, nine million Minitel sets were installed in households around the country, reaching an estimated 25 million users.

Declaration of the Rights of Man and of the Citizen. The Council later approved a revised version of the law, but after public outrage HADOPI was finally revoked in July 2013 as the government conceded that the punitive penalties imposed on copyright infringers was disproportionate to the crime. The law was replaced with a system of automatic fines, and the government shifted its focus from individual users to “commercial piracy" and "sites that profit from pirated material" (Reporters Without Borders, 2012e; Datoo, 2013, July 9).

The Anti-Counterfeiting Trade Agreement (ACTA), a multinational treaty for the purpose of establishing international standards for intellectual property rights enforcement, would have allowed the EU and other global law enforcement agencies to impose new criminal sanctions on users who violate copyright and patent laws, but the agreement died in the European Parliament in 2012 following Parliament rapporteur David Martin’s statement that “[t]he intended benefits of this international agreement are far outweighed by the potential threats to civil liberties” (BBC, 2012, April 16).

# Chapter Four

# Conclusion

## Research Summary

The introduction to this paper detailed how the mechanisms through which governments attempt to control the Internet may be developed and implemented by different institutions and agencies, or fall outside of a formal regulatory structure entirely. As such, the totality of the institutions and practices of national Internet control is better conceptualized not as a regulatory regime, but as a control regime. This broader definition captures the different methodological and descriptive approaches used in prominent "Internet Freedom" reports and in Internet policy literature more generally, and thus allows for a more effective comparative approach. This paper then sets out to answer the following research question: *What are the different Internet control regimes at the national level and how are they different*? I argue that the wide range of Internet control regimes can be best classified using a typological approach.

The Internet control regime typology I construct in this paper is not intended to exhaustively capture and exclusively categorize every country's respective Internet control regime configuration. Rather, it classifies the most common *and* most prominent control regime types. The typology identifies groupings of countries exhibiting densely linked shared characteristics and presents them as "models"—effectively ideal types, or more specifically constructed types to the extent that they are analogous to a measure of central tendency. The typology should be considered a refinement of Eko's (2001; 2008) typology of Internet regulatory regimes. While Eko's work is a very useful starting point, his analysis is (a) focused on regulation, not control, and (b) largely centered on *governmentality*, a concept that by itself does not adequately or consistently capture important policy regime variations. The six dimensions used in this typology are derived from public policy, Internet policy, and policy regime literature, and are intended to capture all of the relevant aspects of Internet control. In using a multidimensional, descriptive

approach, my proposed typology more accurately identifies the compounds of conceptual attributes that comprise particular types.

By detailing the typology dimensions and explaining their applicability to Internet control policy, the paper addresses several corollary questions raised by the main research question. The answers reinforce the notion that Internet control regime variables are densely linked. First, *what does "control" of the Internet constitute and what are the technical mechanisms through which it can be achieved?* Per Eriksson and Giacomello (2009), control of the Internet occurs across three dimensions: (1) access to the Internet, (2) functionality of the Internet, and (3) activity on the Internet. The mechanisms for control vary by dimension, but effective control across all three dimensions—especially activity—is contingent upon institutional ability. Second, *what are the variations in the strategic and administrative aspects of Internet control?* The strategic aspects generally reflect (a) governing regime type, especially as it reflects upon the degree of political pluralism allowed, and (b) particular normative factors related to policy makers' conception of the "public interest." Administrative aspects reflect policy goals and institutional ability, and are thus closely linked with the level of control. Third, w*hy do different governments adopt particular control regimes?* This typology does not purport to explain why governments choose different control regimes, but the analyzed country profiles suggest that the characteristics identified above—especially governing regime type, normative factors, and institutional ability—are key factors in that decision. Fourth and finally, w*hat are the results, limitations, and unintended consequences of control efforts?* All three factors vary considerably across model types and from country-to-country. But the friction Zheng (2007) identifies between China's contradictory Internet regulatory and control policies is evident in many cases—especially with regard to state surveillance, which often occurs outside of a regulatory framework.

The typology identifies six main Internet control regimes: Cuban model, Chinese model, Russian model, developmental model, United States model, and European mod-

el. The first three models capture authoritarian governing regimes which maintain tight "command-and-control" of their countries' respective Internet architectures through a central "gateway" agency which regulates access. But these control models are very different beyond these few shared characteristics: Cuban model countries feature very low Internet penetration levels and focus their limited control resources on regulating Internet *access* through national intranets and closely monitored Internet cafés; Chinese model countries feature moderate levels of Internet penetration, and focus their ample control resources on regulating Internet *activity* through extensive filtering and surveillance systems; and Russian model countries feature relatively high levels of Internet penetration, and only *indirectly* control the Internet through sophisticated propaganda and strategically timed cyberattacks.

The developmental model applies to developing-level countries with proactive Internet policies that leverage the technology as a tool for social and economic growth. Developmental model countries feature democratic governing regimes or even semi-authoritarian governing regimes with relatively few restrictions on Internet activity. These countries feature varying levels of Internet control, and may even maintain gateway model institutional arrangements through which a government ministry maintains substantial regulatory authority over otherwise private ISPs. Filtering and surveillance in developmental model countries is, however, less pronounced than in authoritarian countries, and democratic institutions provide a public check on Internet policy issues. Some developmental countries suffer from a lack of effective control mechanisms due to minimal institutional capacity.

The United States model of Internet control narrowly applies to the United States only. While at least a few other countries feature a relatively self-regulatory approach to Internet regulation, the US also features several unique functional control mechanisms through its indirect control of the Domain Name System management body and global data encryption standards. In addition, the presence of so many global Internet giants

within the US grants the government regulatory authority over not only its own national corner of the Internet, but also the multinational tech corporations that shape Internet development and maintain giant troves of personal and business data for users across the globe The NSA's collaboration with these companies has given the agency incomparable surveillance capabilities.

The European model applies to many countries within the European continent, where co-regulation is the general and leading model of regulation. Although much regional Internet content analysis focus on the role of the European Union in harmonizing member states' respective Internet regulatory policies through directives, other important aspects of Internet control—including the definition and designation of "illegal" online content, telecommunication data retention policy, and the institutional capacity to carry out enforcement—vary significantly from member from member. Moreover, Switzerland, Norway, and several smaller European countries are not part of the EU, but their regulatory approach to the Internet is quite similar. EU member and non-member states all maintain their own security and intelligence agencies, which vary considerably in their surveillance and data gathering capabilities.

**Research Significance, Limitations, and Analysis**

The Internet control policy regime concept allows for a more effective comparative approach as particular mechanisms of control commonly identified in Internet policy country profiles from Freedom House, Reporters Without Borders, the OpenNet Initiative, and other organizations are clearly operating outside of a formal regulatory framework. This is especially true of national information shaping strategies and enforcement at the source actions under authoritarian regimes, and surveillance efforts under both democratic and authoritarian regimes. In addition, important aspects of functionality are not always considered in comparative accounts. The significance of the US's indirect control of ICANN, for instance, can be overstated, but the degree to which Russia, China, Iran, and other authoritarian countries have lobbied to put root authority under the fold of

a UN body should underscore the continued importance of the Domain Name System.

With the exception of the United States model, the identified control regime models capture clusters of countries sharing densely linked attributes. Some countries do not fit cleanly within the typology categories, however. These include Australia, New Zealand, Canada, and several Pacific Asian countries—especially South Korea and Taiwan—which feature unique control arrangements that mix attributes from other models, yet are not similar enough to one another across dimensions to justify a separate model. Filtering efforts in South Korea, for example, target content related to conflict and security (particularly regarding North Korea), and should be considered within the context of particular geopolitical factors that would be represented in the International factors dimension. A proposed mandatory filtering system in Australia, on the other hand, would have targeted sexually explicit content—a reflection of the country's socially conservative culture that would be captured in the Ideas dimension. In a sense, these outliers could be categorized as European model countries—minus, of course, the harmonizing influence of the European Union—as they all feature co-regulatory approaches to filtering and content regulation. But, again, these countries vary significantly on other dimensions, and no one country represents a *prominent* enough model of control to justify another model category.

The Internet control regime typology outlined in this paper reflects a policy dynamic that could shift rapidly in the years ahead. ICANN board member Wolfgang Kleinwächter (2013, Dec. 21) anticipates a "worst case" scenario in the near future in which the Internet may become increasingly fragmented and nationalized. A number of governments already employing Chinese model control regimes are developing the legal and technical abilities to more rigorously regulate their national Internet segments, which could eventually be walled off from the "world wide" Internet entirely à la the Intranets still used by Cuban model countries. Browsing outside of national domains may require special passwords handed out by governmental authorities on an annual basis. This could produce a greater number of control regime categories, as national regimes could become

more distinct as they become more influential as gatekeepers.

This scenario seems far-fetched, but a more organic balkanization is already occurring on culturally defined corners of the Internet. Taneja and Wu (2013) identify a set of 37 “culturally defined markets”—collections of popular websites that seem to be visited predominantly by people who share languages or cultures. Language, while a powerful factor in explaining this clustering, is not the sole factor: the fourth largest cluster is predominately French language sites, but also includes a substantial number of Arabic language websites domained in Northern Africa, suggesting a distinct Francophone cultural corner of the web. Likewise, there is a clear cluster of Indian sites mostly in English, but distinct from the North American / UK / Australian cluster. An exception to the geo-linguistic clusters is football (soccer) sites, which appear to have a truly transnational audience. The authors’ findings suggest that culture is a more powerful force towards Internet balkanization than government regulation (Zuckerman, June 2). Such natural clusters, however, actually make it easier for governments to control the parts of the Internet most significant to them: the Chinese language cluster, for instance, is of far greater concern to CCP authorities than any other segment of the Internet, and as more Chinese users gravitate to this cluster—especially via Beijing-approved apps such as Weibo—the government’s Internet surveillance efforts become that much easier. Likewise, Russian authorities are likely less concerned with scathing criticism of Putin published in prominent English-language dailies than they are with the everyday communications occurring across "Runet," the Russian language portion of the Internet.

**Opportunities for Further Research**

Recent revelations about the extent of the NSA’s capabilities underscore the importance of integrating state surveillance into Internet policy analysis. The impact of surveillance on user behavior is generally indirect, and the change in user behavior may be minimal depending on the perceived punishment. But the ability to intercept email, read ostensibly private social media posts, and access user browsing records is clearly a form

of control, whether done with proper oversight within a well-defined legal framework or not. A typology of state Internet surveillance regimes could explore distinctions between surveillance techniques, institutional arrangements, and legal frameworks (or the lack thereof) in more detail. Such a typology would be especially useful for democratization analysis. Although the Arab Spring and similar uprisings provide anecdotal evidence that ICT-emboldened activists can continue to catch regimes off guard, a wealth of evidence suggests authoritarian regimes have utilized ICT to create sophisticated surveillance systems that can enhance and optimize their repressive capabilities.

## References

Acemoglu, D., & Robinson, J. A. (2006). Economic backwardness in political perspective. *American Political Science Review*, *100(1),* 115-131.

Acker, O. Geerdes, H. Frone, F. Schroder, G. (2013). *Builders of the digital ecosystem: The 2013 Booz & Company Global ICT 50 Study*. Booz & Company. Retrieved from http://www.booz.com/media/file/BoozCo_Builders-of-the-Digital-Ecosystem.pdf

Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2010). Blogs and bullets: New media in contentious politics. *Peaceworks, (65).* Retrieved from http://www.usip.org/sites/default/files/resources/pw65.pdf

Aday, S., Farrell, H., Lynch, M., Sides, J., & Freelon, D. (2012). Blogs and Bullets II: New Media and Conflict after the Arab Spring. *Peaceworks, (80).* Retrieved from http://www.usip.org/sites/default/files/PW80.pdf

Aid, M. (2010). The troubled inheritance: the National Security Administration and the Obama Administration. In Johnson, L. K. (Ed.). *The Oxford handbook of national security intelligence* (pp. 242-257). Oxford University Press.

Akdeniz, Y. (2001). Internet content regulation: UK government and the control of Internet content. *Computer Law & Security Review*, *17(5),* 303-317.

Alderman, L. (2014, Jan. 3). Unemployed in Europe stymied by lack of technology skills. *The New York Times*. Retrieved from http://www.nytimes.com/2014/01/04/business/international/unemployed-in-europe-hobbled-by-lack-of-technology-skills.html

Alexanyan, K., Barash, V., Etling, B., Faris, R., Gasser, U., Kelly, J., Palfrey, J., & Roberts, H. (2012). *Exploring Russian Cyberspace: Digitally-mediated collective action and the networked public sphere*. Berkman Center Research Publication.

Associated Press. (2002, July 10). Italian police shut down U.S.-based porn sites. *USA Today.* Retrieved from http://usatoday30.usatoday.com/life/cyber/

tech/2002/07/10/italy-porn.htm

Bahrain Center for Human Rights. (2011). *Bahrain: After destruction of the actual protesting site at "the Pearl", the government shifts to eliminate virtual protests*. Bahrain Center for Human Rights. Retrieved from http://www.bahrainrights.org/en/node/4101

Bailey, K. D. (1994). *Typologies and taxonomies: an introduction to classification techniques* (Vol. 102). Sage.

Baker, L. (2013, Oct. 21). Europe pushes ahead with stricter data privacy rules. *Reuters*. Retrieved from http://uk.reuters.com/article/2013/10/21/uk-eu-data-idUKBRE99K0LF20131021

Baranshamaje, E., Boostrom, E., Brajovic, V., Cader, M., Clement-Jones, R., Hawkins, R., Knight, P., Schware, R., & Sloan, H. (1995). *Increasing Internet connectivity in sub-Saharan Africa: Issues, options, and the World Bank Group role.* The World Bank. Retrieved from http://repository.uneca.org/handle/10855/15401

Barbrook, R., & Cameron, A. (1996). The Californian Ideology. *Science as Culture, 6(1),* 44-72.

Barry, E. (2009, April 7) Protests in Moldova explode, with help of Twitter. *The New York Times*.

Barzilai-Nahon, K. (2008). Toward a theory of network gatekeeping: A framework for exploring information control. *Journal of the American Society for Information Science and Technology*, 59(9), 1493-1512.

Bauer, S., Clark, D., Lehr, W. (2010). *Understanding broadband speed measurements.* Boston, MA: Massachusetts Institute of Technology. Retrieved from http://mitas.csail.mit.edu/papers/Bauer_Clark_Lehr_Broadband_Speed_Measurements.pdf

BBC. (2012, April 16). Euro MP David Martin dismisses anti-counterfeiting treaty. *BBC*. Retrieved from http://www.bbc.co.uk/news/technology-17728045

BBC. (2013, Oct. 4). China employs two million microblog monitors state media say.

*BBC*. Retrieved from http://www.bbc.co.uk/news/world-asia-china-24396957

Biermann, K. (2013, Oct. 4). Germany intelligence service is as bad as the NSA. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2013/oct/04/german-intelligency-service-nsa-internet-laws

Bennett, A. A. (2005). Integrating comparative and within-case analysis: Typological theory. In George, A. L., & Bennet, A. A. (Eds.) *Case studies and theory development in the social sciences.* MIT Press.

Bennett, A., & Elman, C. (2006). Qualitative research: Recent developments in case study methods. *Annual Review of Political Science*, 9, 455-476.

Bennett, C. C. J. (2008). *The privacy advocates*. Cambridge, MA: MIT Press.

Best, M. L., & Wade, K. W. (2009). The Internet and Democracy: Global catalyst or democratic dud?. *Bulletin of science, technology & society*, *29(4),* 255-271.

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Harvard University Press.

Berberoglu, B. (1992). *The political economy of development: Development theory and the prospects for change in the third world.* SUNY Press.

Bidgoli, H. (2006). *Handbook of Information Security, Information Warfare, Social, Legal, and International Issues and Security Foundations* (Vol. 2). Wiley.

Birnhack, M. D., & Elkin, N. (2008). The Invisible Handshake: The Reemergence of the State in the Digital Environment. *Tel Aviv University Legal Working Paper Series, 54.*

Borger, J. (2013, Nov. 2). GCHQ and European spy agencies worked together on mass surveillance. *The Guardian* (p. 1). Retrieved from http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

Braman, S. (2011). Internet policy. In Consalvo, M., & Ess, C. (Eds.). *The handbook of Internet studies* (pp. 137-167). John Wiley & Sons.

Blythe, S. E. (2005). Digital signature law of the United Nations, European Union,

United Kingdom and United States: Promotion of growth in E-commerce with enhanced security. *Rich. JL & Tech*., *11,* 6-8.

Brito, J. (2011, March 5). ICANN vs. the World. *Time.* Retrieved from http://techland.time.com/2011/03/05/icann-vs-the-world/

Brosseau, E., Marzouki, M., & Meadel, C. (2012) *Governance, regulation and powers on the Internet*. Cambridge University Press

BBC (2013, March 26). The astonishing speed of Chinese censorship. *BBC News*.

Boas, T. C. (2006) Weaving the authoritarian web: The control of Internet use in nondemocratic regimes. In Zysman, J., & Newman, A. (Eds.), *How revolutionary was the digital revolution? National responses, market transitions, and global technology* (pp. 361-378). Stanford, CA: Stanford.

Braun, D., & Busch, A. (Eds.). (1999). *Public policy and political ideas*. Cheltenham, UK: Edward Elgar Publishing.

Breindl, Y. (2013). *Internet content regulation in liberal democracies*. Göttingen Centre for Digital Humanities. University of Göttingen: Germany.

van den Bulck, H. (2013). Tracing media policy decisions (pp 17-34). In Price, M. E., Verhulst, S. G., & Morgan, L. (Eds.). *The Routledge Handbook of Media Law*. Routledge.

Cairncross, F. (2000). *The death of distance* (2nd Ed.) Cambridge, MA: Harvard Business School Press.

Callanan, C., & Dries-Ziekenheiner, H. (2012). *Safety on the Line: Exposing the myth of mobile communication security*. Washington, D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line.pdf

Calingaert, D. (2010). Authoritarianism vs. the Internet. *Policy Review*, *160(63),* 63-75.

Capano, G. (1999). Replacing the policy paradigm: higher education reforms in Italy and the United Kingdom, 1979–1997. In Braun, D. & Busch, A. (Eds.) Public policy

and political ideas (pp. 81-81). Cheltenham, UK: Edward Elgar.

Caramani, D. (Ed.). (2008). *Comparative politics.* Oxford University Press.

Cave, J., Simmons, S., & Marsden, C. (2008). *Options for and Effectiveness of Internet Self-and Co-Regulation*. European Commission.

CERIAS. (2013). Broadband vs. Dialup Internet Connection. West Lafayette, Indiana: The Center for Education and Research in Information Assurance and Security, Purdue University. Retrieved from http://www.cerias.purdue.edu/site/education/k-12/cerias_resources/files/infosec_newsletters/06broadband.php

Chin, C. & Collazo, J. B. (2012, Nov. 3). 'Brand US' key to pivot in Asia. *Asia Times*. Retrieved from http://www.atimes.com/atimes/Asian_Economy/NK03Dk01.html

Christians, C. G., Glasser, T. L., McQuail, D., Nordenstreng, K., & White, R. A. (2009). Normative theories of the media: Journalism in democratic societies. University of Illinois Press.

Cobb, R.W., & Elder, C. (1983). *Participation in American politics: The dynamics of agenda building.* Baltimore: Johns Hopkins University Press.

Cohen-Vogel, L. & McLendon, M. (2009). New approaches to understanding federal involvement in education. In D. Plank, G. Sykes, and B. Schneider (Eds.), *Handbook of education policy research: A handbook for the American Educational Research Association.* Mahwah, NJ: Lawrence Erlbaum.

Collier, D. LaPorte, J. & Seawright, J. (2008). Typologies: Forming concepts and creating categorical variables. In Box-Steffensmeier, J. M., Brady, H. E., & Collier, D. (Eds.). *The Oxford handbook of political methodology*. Oxford Handbooks Online.

Cooper, G. S. (2008). Tangled Web We Weave: Enforcing International Speech Restrictions in an Online World, A. Pitt. J. Tech. *L. & Pol'y*, 8, i.

Corn-Revere, R. (2003). Caught in the seamless Web: Does the Internet's global reach justify less freedom of speech?. In Thierer, A. D., & Crews, C. W. (Eds.). *Who*

*rules the net?: Internet governance and jurisdiction.* Washington, D.C.: Cato Institute.

Clark, J. R. (2007). *Intelligence and National Security: A Reference Handbook*. Greenwood Publishing Group.

Clark Estes, A. (2012, 12 October) Twitter Censors Users for the First Time. *The Atlantic*.

Daniel, R. (2005). The WTO and telecommunications services in China: three years on. *Info-The journal of policy, regulation and strategy for telecommunications, 7(2),* 25-48.

Datoo, S. (2013, July 9). France drops controversial 'Hadopi law' after spending millions. *The Guardian. Retrieved* from http://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy

DeCarlo, S. (2013). The World's Biggest Companies. *Forbes*. Retrieved from http://www.forbes.com/sites/scottdecarlo/2013/04/17/the-worlds-biggest-companies-2/

Decker, S. (2013, Oct. 8). Apple victory over Samsung Seen Leading to Customs Fight. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2013-10-09/apple-victory-over-samsung-seen-leading-to-customs-fight.html

Deffains, B. & Winn, J.K. (2012). The effects of electronic commerce technologies on business contracting behaviors. In Brousseau, E., Marzouki, M., & Méadel, C. (Eds.). *Governance, regulation and powers on the Internet* (pp. 344-366). Cambridge University Press.

Deibert, R, J. (1997). *Parchment, printing, and hypermedia: Communication and world order transformation*. New York City: Columbia University.

Deibert, R. J. (Ed.). (2008). *Access denied: The practice and policy of global internet filtering*. Cambridge, MA: MIT Press.

Deibert, R. J. (Ed.) (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace.* Cambridge, MA: MIT Press.

Deibert, R. J. (2012) International mechanisms of cyberspace control. In Diamond, L., &

Plattner, M. F. (Eds.). *Liberation technology: Social media and the struggle for democracy* (pp. 33-46). Baltimore: Johns Hopkins University Press.

Deibert, R. J., & Rohozinski, R. (2010a). Liberation vs. control: The future of cyberspace. *Journal of Democracy*, *21(4),* 43-57.

Deibert, R. J., & Rohozinski, R. (2010b). Control and subversion in Russian cyberspace. In Deibert, R. (Ed.). *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 15-34). Cambridge, MA: MIT Press.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations, 18(3),* 339-361.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2012). *Access contested: security, identity, and resistance in Asian cyberspace.* Cambridge, MA: MIT Press.

Der Spiegel. (2012, Oct. 17). 'The Right to be forgotten': US lobbyists face off with EU on data privacy proposal. Der Spiegel. Retrieved from http://www.spiegel.de/international/business/us-government-and-internet-giants-battle-eu-over-data-privacy-proposal-a-861773.html

Do, A. (2013, May 27). Startup scenes across Asia: Let's look 11 of Asia's top tech cities. *Tech In Asia*. Retrieved from http://www.techinasia.com/startup-scenes-asia-lets-11-asias-top-tech-cities

Dourado, E. (2013, Sep. 18). Protecting the open Internet may require defunding the ITU. Here's how to do it. *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/18/protecting-the-open-internet-may-require-defunding-the-itu-heres-how-to-do-it/

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

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

Drori, G. S. (2004). The Internet as a global social Problem. In Ritzer, G. (Ed.). *Handbook of social problems: A comparative international perspective.* Sage.

Ducatel, K., Webster, J., & Herrmann, W. (Eds.). (2000*). The Information Society in Europe: Work and Like in an Age of Globalization*. Rowman & Littlefield Pub Incorporated.

Dutton, W. H. Peltu, M. (2010) The new politics of the Internet: Multi-stakeholder policy-making and Internet technocracy. In Chadwick, A., & Howard, P. N. (Eds*.). Routledge handbook of Internet politics* (pp. 384-400). Taylor & Francis.

Dutton, W. (2013). *The Oxford handbook of Internet studies*. Oxford University Press.

The Economist. (2010, March 25) The world economy calls: Will improved communications attract call centres to Africa?. *The Economist.*

The Economist. (2013a, April 6). The machinery of control: Cat and mouse. *The Economist*, 5.

The Economist. (2013b, April 6). A curse disguised as a blessing? Assessing the effects. *The Economist*, 14.

The Economist. (2013c, April 6). China's Internet: A giant cage. *The Economist*, 3.

Economou, P. (2008, March 27-28). Harnessing ICT for FDI and Development*. Report for OECD Global Forum on International Investment III.* Paris, France.

Eisenberg, A. I. (2010). Reconstructing political pluralism. In Schumaker, P. (Ed.). *The Political Theory Reader*. Wiley.

Edquist, H., & Henrekson, M. (2006). *Technological breakthroughs and productivity growth* (Vol. 24, pp. 1-53). Bradford, UK: Emerald Group Publishing Limited.

EFF. (ND). *Mandatory Data Retention: European Union.* San Francisco, CA: Electronic Freedom Foundation. Retrieved from https://www.eff.org/issues/mandatory-data-retention/eu

Eko, L. (2001). Many spiders, one worldwide web: Towards a typology of Internet regulation. *Communication Law & Policy*, *6(3),* 445-484.

Eko, L. (2008). Internet Law and Regulation. In Donsbach, W. (Ed.). *The International Encyclopedia of Communication*. Hoboken, New Jersey: Blackwell Publishing. Blackwell Reference Online. Retrieved from http://www.communicationency-clopedia.com/subscriber/tocnode.html?id=g9781405131995_yr2013_chunk_g978140513199514_ss70-1

Eko, L. (2012). *New media, old regimes: Case studies in comparative communication law and policy*. Lexington Books.

Eisner, M. A. (2000). A Primer on Regulation. In Eisner, M.A., Worsham, J. & Ringq-uist, E. J. (Eds.). *Contemporary regulatory policy* (pp. 3-18). Lynne Rienner Publishers.

Eldon, M. (2005). Mainstreaming ICTs: Private sector sway. In Etta, F. E., & Elder, L. (Eds.). *At the crossroads: ICT policy making in East Africa.* IDRC.

Elman, C. (2005). Explanatory typologies in qualitative studies of international politics. *International organization, 59(2),* 293-326.

Epstein, G. (2011, March 3). Sina Weibo. *Forbes*. Retrieved from http://www.forbes.com/global/2011/0314/features-charles-chao-twitter-fanfou-china-sina-weibo.html

Eriksson, J., & Giacomello, G. (2009). Who controls the Internet? Beyond the obstinacy or obsolescence of the State. *International Studies Review*, *11(1),* 205-230.

Ermert, M. (2013, July 5). EU Data Retention Directive finally before European Court of Justice. *Internet Policy Review*. Retried from http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162

Ermert, M. (2013, Dec. 13). Advocate General: EU Data Retention Directive unconsti-tutional. Internet Policy Review. Retried from http://policyreview.info/articles/news/advocate-general-eu-data-retention-directive-unconstitutional/225

Essinger, J. (2012, Apr. 23). Latin America creates rival to Silicon Valley. *World Fi-nance.* Retrieved from http://www.worldfinance.com/inward-investment/ameri-

cas/latin-america-creates-rival-to-silicon-valley

Etoh, M., Powell, G. (2005). Evolution of Mobile Networks and Services. In Etoh, M. (Ed.). *Next generation mobile systems: 3G and beyond*. John Wiley.

European Commission. (2000). *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* (Directive on Electronic Commerce). OJ L, 178, 17.

European Digital Rights. (2013, Nov. 6). The Russian govt seeks to increase its control over the Internet. *European Digital Rights.*

EU Directive. (1995*). 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. OJ L 281, 23.11.1995, pp. 31–50.

European Parliament. (2012). Answer given by High Representative/Vice-President Ashton on behalf of the Commission. European Parliament. Retrieved from http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2012-006017&language=EN

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. In Deibert, R. (Ed.). (2008). *Access denied: The practice and policy of global Internet filtering* (pp. 5-28). MIT Press.

Farrell, H. (2012). The consequences of the internet for politics. *Annual Review of Political Science*, 15, 35-52.

Feld, H. (2003). Structured to Fail: ICANN and the "Privatization" Experiment. In Thierer, A. D., & Crews, C. W. (Eds.). *Who rules the net?: Internet governance and jurisdiction* (pp. 333-362). Washington, D.C.: Cato Institute.

Fielder, J. D. (2012). *Dissent in digital: the Internet and dissent in authoritarian states*. (Doctoral Thesis). University of Iowa.

Fiveash, K. (2013, Dec. 9). EU legal eagle: Data protection reforms 'very bad outcomes' for citizens. *The Register*. Retrieved from http://www.theregister.co.uk/2013/12/09/eu_data_protection_reforms_hits_legal_roadblock/

Franda, M. F. (2002*). Launching into cyberspace: Internet development and politics in five world regions*. Boulder, CO: Lynne Rienner.

Fredman, R. (2012). *The Dictator's Dilemma and the Politics of Telecommunications in Cuba: A Case Study*. (Master's Thesis.) The Fletcher School, Tufts University.

Freedman, D. (2008). *The Politics of Media Policy*. Boston, MA: Polity.

Freedom House. (2006). *Freedom of the Press 2006: A Global Survey of Media Independence*. Washington D.C.: Freedom House.

Freedom House. (2011a). *Thailand: Freedom on the Net 2011*. Washington D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/freedom-net/2011/thailand

Freedom House. (2011b). *Tunisia: Freedom on the Net 2011*. Washington D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/freedom-net/2011/tunisia

Freedom House. (2012). *India: Freedom on the Net 2012*. Washington D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/freedom-net/2012/india

Freedom House. (2012a). *Tunisia: Freedom on the Net 2012*. Washington D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/freedom-net/2012/tunisia

Freedom House. (2012b). *Mexico: Freedom on the Net 2012*. Washington, D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/freedom-net/2012/mexico

Freedom House. (2013a). Russia: Freedom on the Net Report 2013. Washington, D.C.: Freedom House. Retrieved from http://www.freedomhouse.org/report/free-

dom-net/2013/russia

Freedom House. (2013b). Philippines: Freedom on the Net. Washington, D.C.: Freedom House. Retrieved form http://www.freedomhouse.org/report/freedom-net/2013/philippines

Freedom House. (2013c). United States: Freedom on the Net. Washington, D.C.: Freedom House. Retrieved form http://www.freedomhouse.org/report/freedom-net/2013/unitedstates

Freedom House. (2013d). 2013 methodology and checklist of questions. Washington, D.C.: Freedom House. Retrieved from http://freedomhouse.org/report/2013-methodology-and-checklist-questions

Freedom House. (2013e). Freedom on the Net: Full Report. Washington, D.C.: Freedom House. Retrieved from http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf

Frydman, B., Hennebel, L., & Lewkowicz, G. (2012). Co-regulation and the rule of law. In Brousseau, E., Marzouki, M., & Méadel, C. (Eds.). *Governance, regulation and powers on the Internet* (pp. 133-150). Cambridge University Press.

Gellman, B. & Soltani, A. (2013, Oct. 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post.* Retrieved from http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

Gelsthorpe, L. (2010) Copyright infringement: A criminological perspective. In Bently, L., Davis, J., & Ginsburg, J. C. (Eds.). Copyright and piracy: An interdisciplinary critique. Cambridge University Press.

Gerring, J. (2011). Social science methodology: a unified framework. Cambridge University Press.

Giacomello, G. (2004). *National governments and control of the Internet: a digital chal-*

*lenge*. Routledge.

Gilbert, L., & Mohseni, P. (2011). Beyond authoritarianism: The conceptualization of hybrid regimes. *Studies in Comparative International Development, 46(3),* 270-297.

Gladwell, M. (2011, February 2). Does Egypt need Twitter? *The New Yorker*.

Gladwell, M. (2010, October 4). Small change: Why the revolution will not be tweeted. *The New Yorker*.

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

Gorman, S., & Valentino-Devries, J. (2013, August 20). New details show broader NSA surveillance reach. *The Wall Street Journal*.

Greene, T. (2001, April 9). Germany may strike Nazi sites with DoS attacks. *The Register*. Retrieved from http://www.theregister.co.uk/2001/04/09/germany_may_strike_nazi_sites/

Gross, M. J. (2012, May). World War 3.0. *Vanity Fair.* Retrieved from http://www.vanityfair.com/culture/2012/05/internet-regulation-war-sopa-pipa-defcon-hacking#

Gunther, R., Montero, J. R., & Wert, J. I. (2000). The media and politics in Spain: From dictatorship to democracy. In Gunther, R., & Mughan, A. (Eds.). *Democracy and the media: a comparative perspective* (pp. 28-84). Cambridge University Press.

Hagestad II, W. (2012). *21st century Chinese cyberwarfare*. IT Governance Ltd.

Hall, P. A. (1986). *Governing the economy: The politics of state intervention in Britain and France*. Oxford: Oxford University Press

Hallin, D. C. & Mancini, P. (2004*). Comparing media systems: Three models of media and politics*. Cambridge University Press.

Hanna, N. K. (2003). Why National Strategies are needed for ICT-enabled Development. *World Bank Staff Paper*. Washington, DC: World Bank.

Hardy, J. (2008). *Western media systems*. Routledge.

Hardy, J. (2012). Comparing media systems. In Esser, F., & Hanitzsch, T. (Eds.). *Handbook of comparative communication research* (pp. 185-206). Routledge.

Harley, B. (2010, Jan. 26) Could the WTO bring down the Great Firewall of China?. *The Columbia Science and Technology Law Review blog.* Retrieved from http://www.stlr.org/2010/01/could-the-wto-bring-down-the-great-firewall-of-china/

Hargittai, E. (1999). Weaving the Western Web: explaining differences in Internet connectivity among OECD countries. *Telecommunications Policy*, *23(10),* 701-718.

Heacock, R. (2008). Sub-Saharan Africa. In Deibert, R. J. (Ed.). *Access denied: The practice and policy of global internet filtering* (pp. 213-225). The MIT Press.

Herman, B. D. (2013). *The fight over digital rights: The politics of copyright and technology.* Cambridge University Press.

Herman, E. S., & Chomsky, N. (2008). *Manufacturing consent: The political economy of the mass media*. Random House.

Heumann, S. & Scott, B. (2013, Sept.). Law and policy in Internet surveillance programs: United States, Great Britain and Germany. *Impulse*. Stiftung Neue Verantwortung / New America Foundation. Retrieved from http://www.stiftung-nv.de/law_and_policy_in_internet_surveillance_programs

Higgins, A., & Azhar, A. (1996, Feb. 5th) China begins to erect second Great Wall in Cyberspace. *The Guardian*. Infotrac Newsstand.

Hitt, M. A., Ireland, R. D., & Hoskisson, R. E. (2012). Strategic management cases: Competitiveness and Globalization. Stamford, CT: Cengage Learning.

Holmes, R. (2013, Aug. 9) From inside walled gardens, social networks are suffocating the Internet as we know it. *FastCompany*. Retrieved from http://www.fastcompany.com/3015418/from-inside-walled-gardens-social-networks-are-suffocating-the-internet-as-we-know-it

Howard, P. N., & Hussain, M. M. (2011). The role of digital media. *Journal of Democracy*, *22(3),* 35-48.

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). *The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?*. Brookings Institution.

ICANN. (2011). Bylaws for Internet Corporation for Assigned Names and Numbers | As amended 18 March 2011. Los Angeles, CA: Internet Corporation for Assigned Names and Numbers. Retrieved from http://www.icann.org/en/about/governance/bylaws/bylaws-18mar11-en.htm

Inglehart, R., & Norris, P. (2003). The true clash of civilizations. *Foreign policy*, *(135),* 63–69.

IMF. (2013). *World Economic Outlook: Frequently Asked Questions.* International Monetary Fund. Retrieved from http://www.imf.org/external/pubs/ft/weo/faq.htm#q4b

INHOPE. (2004). *Inhope Internet Hotline Providers Second Report*. Amsterdam, the Netherlands: International Association of Internet Hotlines.

INHOPE. (2012). *Facts, figures and trends*. Amsterdam, the Netherlands: International Association of Internet Hotlines. Retrieved from http://inhope.pressdoc.com/42774-inhope-2012-facts-figures-and-trends

Interbrand. (2013). *Interbrand releases 14th annual best global brands report.* Interbrand (Press Release). Retrieved from http://www.interbrand.com/en/news-room/press-releases/2013-09-30-d355afc.aspx

ITU. (2010). ITU sees 5 billion mobile subscriptions globally in 2010. Geneva, Switzerland: International Telecommunication Union. Retrieved from http://www.itu.int/newsroom/press_releases/2010/06.html

ITU. (2013) ICT facts and figures. Geneva, Switzerland: International Telecommunication Union. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

Jakubowicz, K., & Sükösd, M. (Eds.). (2008). *Finding the right place on the map: Central and Eastern European media change in a global perspective*. Chicago, IL: Intellect Books.

John, P. (1998). *Analysing public policy*. London: Continuum International Publishing Group.

John, P. (1999). Ideas and interests; agendas and implementation: An evolutionary explanation of policy change in British local government finance. *The British Journal of Politics & International Relations, 1(1),* 39-62.

Jeffreys-Jones, R. (2013). *In Spies We Trust: The Story of Western Intelligence*. Oxford University Press.

Jeffreys-Jones, R. (2013, March 19). The case for a European intelligence service with full British participation. *Oxford University Press Blog*. Retrieved from http://blog.oup.com/2013/03/european-intelligence-service/

Jenson, J. (1989). Paradigms and political discourse: Protective legislation in France and the United States before 1914. *Canadian Journal of Political Science*, *22(2).*

Johnson, D. R., & Post, D. (1995). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review, 48,* 1367.

Jones, S. (Ed.). (2003). *Encyclopedia of new media: An essential reference to communication and technology*. Sage.

Kalathil, S. & Boas, T. C. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace: Washington, DC.

Kelly, S. Cook, S. Truong, M. (Eds.) (2012). *Freedom on the Net 2012*. Freedom House. Retrieved from http://www.freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf

Kedzie, C. (1997). *Communication and democracy: Coincident revolutions and the emergent dictators.* Santa Monica, CA: RAND.

Kettmann, S. (2002, Jan. 10). Nebraska Neo-Nazi irks German Pol. *Wired*. Retrieved from http://www.wired.com/politics/law/news/2002/01/49566

Kicker, R. (Ed.). (2010). *The Council of Europe: Pioneer and Guarantor for Human*

*Rights and Democracy*. Council of Europe.

Kim, J., Rojas, P., Huey, J., Connors, K., & Wang, S. (2008). Latin America. In Deibert, R. J. (Ed.). *Access denied: The practice and policy of global Internet filtering* (pp. 197-206). The MIT Press.

Kim, Q. (2013, Aug. 1). Tracking the relationship of the government and Silicon Valley. *Marketplace*. Retrieved from http://www.marketplace.org/topics/tech/tracking-relationship-government-and-silicon-valley

Kleinsteuber, H. J. (2004). The Internet between regulation and governance. In Möller, C. (Ed.). *The Media Freedom Internet Cookbook* (pp. 61-100). Organization for Security and Cooperation for Europe.

Kleinwächter, Wo. (2013, Dec. 21). Internet governance outlook 2014: Good news, bad news, no news?. *CircleID.* Retrieved from http://www.circleid.com/posts/20131231_internet_governance_outlook_2014_good_news_bad_news_no_news/

Kransnoboka, N. & Semetko, H. (2004) Murder, journalism and the web: how the Gongadze case launched the Internet news era in Ukraine. In Oates, S., Owen, D., & Gibson, R. K. (Eds.) *The Internet and politics: citizens, voters and activists*. New York City, NY: Routledge.

Kravets, D. (2012, March 6). Uncle Sam: If it ends in .com, it's .seizable. *Wired*. Retrieved from http://www.wired.com/threatlevel/2012/03/feds-seize-foreign-sites/

Kravets, D. (2013, Oct. 14). NSA leaks prompt rethinking of U.S. control over the Internet's infrastructure. Wired. Retrieved from http://www.wired.com/threatlevel/2013/10/global-net-infrastructure.

Küng, L., Picard, R. G., & Towse, R. (Eds.). (2008). *The Internet and the mass media*. Sage.

Lee, Timothy B. (2012, December 8). Authoritarian regimes push for larger ITU rule in DNS system. *Ars Technica*. Retrieved from http://arstechnica.com/tech-poli-

cy/2012/12/authoritarian-regimes-push-for-larger-itu-role-in-dns-system/

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

Lessig, L. (2006). *Code: Version 2.0.* New York: Basic Books.

Lessig, L. & McChesney, R.W. (2006, June 8). No tolls on the Internet. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/07/AR2006060702108.html

Levmore, S., & Nussbaum, M. C. (Eds.). (2010). *The offensive Internet: Speech, privacy, and reputation*. Harvard University Press.

Liphart, A. (1977). *Democracy in plural societies: A comparative exploration.* Yale University Press.

Little, D. (1991). *Varieties of Social Explanation: An Introduction to the Philosophy of Social Science*. Boulder, Colorado: Westview Press, Inc.

Little, D. (1996). Causal explanation in the social sciences. *The Southern journal of philosophy, 34(S1),* 31-56.

Lipset, S. M. (1959). Some Social Requisites of Democracy: Economic Development and Political Legitimacy. *American Political Science Review,* 53(1), 69-105.

Liptak, A. & Schmidt, M.S. (2013, Dec. 28). Judge upholds N.S.A.'s bulk collection of data on calls. *The New York Times* (p. A1). Retrieved from http://www.nytimes.com/2013/12/28/us/nsa-phone-surveillance-is-lawful-federal-judge-rules.html

MacAskill, E. Borger, J. Hopkins, N. Davies, N. & Ball, J. (2013, June 22). GCHQ taps fibre-optic cables for secret access to world's communications. *The Guardian* (p. 1). Retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?guni=Article:in%20body%20link

Mathiason, J. (2008). *Internet Governance: The new frontier of global institutions*. Routledge.

Manaev, O., Manaeva, N., & Yuran, D. (2012). Islands in the stream: Reflections on media development in Belarus. Gross, P., & Jakubowicz, K. (Eds.) *Media Trans-*

*formations in the Post-communist World: Eastern Europe's Tortured Path to Change.* Rowman & Littlefield.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.

Marsden, C. T. (2004). Co- and self-regulation in European media and Internet sectors: The results of Oxford University's study www.selfregulation.info. In Moller, C., & Amourous, A. (Eds.) The *Media Freedom Internet Cookbook*. Vienna: OSCE.

Marsden, C. T. (2011a). *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*. Cambridge University Press.

Marsden, C.T. (2011b*). Internet Co-Regulation and Constitutionalism: Towards a More Nuanced View*. Available at SSRN: http://ssrn.com/abstract=1973328 or http://dx.doi.org/10.2139/ssrn.1973328

Masnick, M. (2011, Dec. 9). SOPA supporter: If you use DNSSEC you can ignore SOPA / PIPA. Techdirt. Retrieved from http://www.techdirt.com/articles/20111208/04204617007/sopa-supporter-if-you-use-dnssec-you-can-ignore-sopapipa.shtml

May, P. J., Jochim, A., & Sapotichne, J. (2009). *Policy regimes and governance: Constructing homeland security*. Ohio State University: 10th Public Management Research Association Conference. Retrieved from http://pmranet.org/

Mazzucato, M. (2013). It's a Myth That Entrepreneurs Drive New Technology. Slate. Retrieved from http://www.slate.com/articles/health_and_science/new_scientist/2013/09/entrepreneurs_or_the_state_innovation_comes_from_public_investment.html

McDonnell, T. A. (2013). *The economics of broadband in Ireland: Country endowments, telecommunications capital stock, and household adoption decisions*. (Doctoral dissertation), National University of Ireland.

McLaughlin, W. S. (2003). The use of the Internet for political action by non-state dissident actors in the Middle East. *First Monday*, *8(11).* Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/1096/1016

McQuail, D. (1983) *Mass communication theory: An introduction*. Sage.

McQuail, D. (2010*). McQuail's mass communication theory*. Sage.

McQuail, D., & Siune, K. (Eds.). (1998). *Media policy: Convergence, concentration & commerce*. Sage.

Mearsheimer, J. J. (2001). *The tragedy of great power politics.* WW Norton & Company.

Meyer, R. (2013, Oct. 16). What does it mean for the U.S. to 'lose control of the Internet?'. *The Atlantic*. Retrieved from http://www.theatlantic.com/technology/archive/2013/10/what-does-it-mean-for-the-us-to-lose-control-of-the-internet/280619/

Miegel, F., & Olsson, T. (2008). From pirates to politicians: The story of the Swedish file sharers who became a political party. *Democracy, journalism and technology: New developments in an enlarged Europe*, *203-16.*

Miller, C.C. (2013, June 7). Tech Companies Concede to Surveillance Program. *The New York Times*. Retrieved from http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=1&hp&_r=0

Milner, H. V. (2006). The digital divide: The role of political institutions in technology diffusion. *Comparative Political Studies*, *39(2),* 176-199.

Morlino, L. (2008). Hybrid regimes or regimes in transition?. *Rivista italiana di scienza politica*, *38(2),* 169-190.

Morozov, E. (2009). How dictators watch us on the web. *Prospect Magazine*, 18(11). Retrieved from http://www.prospectmagazine.co.uk/magazine/how-dictators-watch-us-on-the-web/

Morozov, E. (2012) *The net delusion: The dark side of internet freedom.* New York: Pub-

licAffairs.

Mozur, P., & Tejada, C. (2013, Feb. 13) China's 'wall' hits business. *The Wall Street Journal.*

Mumford, M. (2013, Sept. 24). Bogotá Is Becoming South America's Premier Tech Hub. Mashable. Retrieved from http://mashable.com/2013/09/24/bogota-tech/

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In Deibert, R. (Ed.). *Access denied: The practice and policy of global internet filtering* (pp. 57-72). Cambridge: MIT Press.

National Conference of State Legislatures. (2013). *Children and the Internet: Laws relating to filtering, blocking and usage policies in schools and libraries*. Washington, D.C.: National Conference of State Legislatures.

Negroponte, N. (1996*). Being digital*. Random House.

The New York Times. (2000, Nov. 19). The Ruin of Myanmar. *The New York Times*.

Norris, P. (2003). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge, UK: Cambridge University Press.

Norris, P. (2009). Comparative political communications: Common frameworks or babelian confusion?. *Government and Opposition*, *44(3),* 321-340.

O'Donnell, G., Schmitter, P. C., & Whitehead, L. (1986). *Transitions from authoritarian rule: Tentative conclusions about uncertain democracies*. Baltimore: John Hopkins University Press.

O'Sullivan, K. P. V., & Flannery, D. (2011). *A Discussion on the resilience of command and control regulation within regulatory behaviour theories*. Available at SSRN 1927500.

Ong, J. (2013, Feb. 21). China's Sina Weibo grew 73% in 2012, passing 500 million registered accounts. *The Next Web*. Retrieved form http://thenextweb.com/asia/2013/02/21/chinas-sina-weibo-grew-73-in-2012-passing-500-million-registered-accounts/

OpenNet Initiative. (2005) Internet Filtering in China in 2004-2005: A Country Study. OpenNet Initiative. Retrieved from https://opennet.net/studies/china

OpenNet Initiative. (2007a) North Korea. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/north-korea

OpenNet Initiative. (2007b) Internet filtering in Europe, 2006-2007. OpenNet Initiative. Retrieved from https://opennet.net/studies/europe2007

OpenNet Initiative. (2009). Tunisia. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/tunisia

OpenNet Initiative. (2010a). Russia. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/russia

OpenNet Initiative. (2010b). United States and Canada. OpenNet Initiative. Retrieved from https://opennet.net/sites/opennet.net/files/ONI_UnitedStatesandCanada_2010.pdf

OpenNet Initiative. (2010c). Germany. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/germany

OpenNet Initiative. (2012a). Burma (Myanmar). OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/myanmar-burma

OpenNet Initiative. (2012b). India. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/india

OpenNet Initiative. (2012c). Indonesia. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/indonesia

OpenNet Initiative. (2012d). Thailand. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/thailand

OpenNet Initiative. (2012e). Malaysia. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/malaysia

OpenNet Initiative. (2013a). Colombia. OpenNet Initiative. Retrieved from https://opennet.net/research/profiles/colombia

Open Technology Fund. (2013). Internet Access and Openness: Myanmar 2012. Open Technology Fund / Radio Free Asia (February). Retrieved from https://www.opentechfund.org/files/reports/otf_myanmar_access_openness_public.pdf

OECD. (2002). Measuring the Information Economy. OECD Working Paper, Paris. Retrieved from http://www.oecd.org/sti/ieconomy/2771153.pdf

OECD (2010a). Key ICT Indicators. Organization for Economic Co-operation and Development. Retrieved from http://www.oecd.org/sti/ieconomy/oecdkeyictindicators.htm

OECD (2010b). OECD Broadband Subscriptions Criteria. Organization for Economic Co-operation and Development. Retrieved from http://www.oecd.org/sti/broadband/oecdbroadbandsubscribercriteria2010.htm

Okun, A. M. (1980). The invisible handshake and the inflationary process. *Challenge*, 22(6), 5-12.

Palfrey, J. (2010). Four phases of Internet regulation. *Social Research: An International Quarterly*, *77(3),* 981-996.

Palmer, B. (2011, June 8). Good at wine, bad at computers: Why does Europe suck at technological innovation?. *Slate*. Retrieved from http://www.slate.com/articles/news_and_politics/explainer/2011/06/good_at_wine_bad_at_computers.html

Patalong, F. (2001). Otto Schily: Mit Hackermethoden gegen Neonazis. Der Spiegel. Retrieved from http://www.spiegel.de/netzwelt/web/otto-schily-mit-hackermethoden-gegen-neonazis-a-126921.html

Paulson, K. A. (2003). The War on Internet Speech Can Europe and the United States Find Middle Ground?. *Michigan Bar Journal*, *82(3),* 21-23.

Perlroth, N. (2013, Sept. 10). Government announces steps to restore confidence on encryption standards. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/?_r=0

Perlroth, N., Larson, J., & Shane, S. (2013, Sept. 5). N.S.A. able to foil basic safeguards of privacy on web. *The New York Times*. Retrieved from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0&gwh=D4AC1BA96CF502B969ADE3DA04BC86EA&gwt=pay

Penenberg, A.L. (2005). Who controls the Internet?: Why it doesn't matter if the United States is in charge. *Slate*. Retrieved from http://www.slate.com/articles/technology/technology/2005/11/who_controls_the_internet.html

Peng, H.A. (2005). Self-regulation after WGIG. In Drake, W. J. (Ed.). *Reforming Internet governance: Perspectives from the working group on internet governance (WGIG)* (Vol. 12). United Nations Publications.

Peterson, T., Schramm, W., & Siebert, F. S. (1956). *Four theories of the press*. Illinois: University of Illinois Press.

Price, M. E., Verhulst, S. G., & Morgan, L. (Eds.). (2013). *Routledge Handbook of Media Law*. New York: Routledge.

Psychogiopoulou, E. & Anagnostou, D. (2012). Recasting the Contours of Media Policy in a Political Context: An Introduction. In Psychogiopoulou, E. (Ed.). *Understanding Media Policies: A European Perspective* (n.p.). New York: Palgrave Macmillan.

Putzier, K. (2013). Europe's pirate parties are facing rough seas. *World Policy Blog*. Retrieved from http://www.worldpolicy.org/blog/2013/07/31/europes-pirate-parties-are-facing-rough-seas

Ragin, C. C. (2000). Fuzzy-set social science. University of Chicago Press.

Ramstad, E. (2012, Aug. 25) South Korea court knocks down online real-name rule. *The Wall Street Journal.*

Ramzy, A. (2011, Apr. 21). Charles Chao. *Time*. Retrieved from http://content.time.com/time/specials/packages/article/0,28804,2066367_2066369_2066392,00.html

Reporters Without Borders. (2011) *World report: Tunisia.* Reporters Without Borders.

Retrieved from http://en.rsf.org/report-tunisia,164.html

Reporters Without Borders. (2012a) *Internet Enemies Report 2012*. Reporters Without Borders. Retrieved from http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf

Reporters Without Borders. (2012b). Enemies of the Internet: China. Reporters Without Borders. Retrieved from http://en.rsf.org/china-china-12-03-2012,42077.html

Reporters Without Borders. (2012c). Countries Under Surveillance: Russia. Reporters Without Borders. Retrieved from http://en.rsf.org/russia-russia-12-03-2012,42075.html

Reporters Without Borders. (2012d). *Countries Under Surveillance: Thailand.* Reporters Without Borders. Retrieved from http://en.rsf.org/surveillance-thailand,39775.html

Reporters Without Borders. (2012e). Countries Under Surveillance: France. Reporters Without Borders. http://en.rsf.org/surveillance-france,39715.html

Reporters Without Borders. (2013a) *Internet Enemies Report 2013*. Reporters Without Borders. Retrieved from http://surveillance.rsf.org/en/

Reporters Without Borders. (2013b). Another Journalist Shot Dead in Guatemala, fourth this year. Reporters Without Borders. Retrieved from http://en.rsf.org/guatemala-another-journalist-shot-dead-in-20-08-2013,45078.html

Roberts, H., & Palfrey, J. (2010). The EU Data Retention Directive in an era of Internet surveillance. In Deibert, R. J. *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 35-53). Cambridge, MA: MIT Press.

Robinson, F. (2013, Dec. 12). EU Court Opinion: Data Retention Directive incompatible with fundamental rights. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/BT-CO-20131212-702616.html

Rogerson, K.S., & Milton, D. (2010). Internet diffusion and the digital divide: the role of policy-making and political institutions. In Chadwick, A., & Howard, P. N. (Eds.). *Routledge handbook of Internet politics* (pp. 415-424). Taylor & Francis.

Rosen, J. (2011). The 'Twitter can't topple dictators' article. *Press Think*. Retrieved from http://pressthink.org/2011/02/the-twitter-cant-topple-dictators-article/

Rosen, J. (2012). The right to be forgotten. *Stanford Law Review Online, 64,* 88. Retrieved from http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten

Rosenthal, E. (1998, December 19). *Chinese Reminded: No Opposition Allowed.* The New York Times, p. 5.

Roudakova, N. (2011). Comparing processes: Media, "transitions," and historical change. In Hallin, D. C., & Mancini, P. (Eds.), *Comparing media systems beyond the western world*. Cambridge University Press.

Salhi, H. (2009). The state still governs. In Eriksson, J., & Giacomello, G., (Eds.), Who controls the Internet? Beyond the obstinacy or obsolescence of the state. *International Studies Review, 11(1),* 210-214.

Safire, W. (2007) *The right word in the right place at the right time.* New York: Simon & Schuster.

Sauter, M. (2012). *3G, 4G and beyond: Bringing networks, devices and the web together*. John Wiley & Sons.

Sauter, V. L. (2011). *Decision support systems for business intelligence.* Wiley.

Savage, C. (2013, May 7). U.S. weighs wide overhaul of wiretap laws. *The New York Times*. Retrieved from http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?ref=charliesavage&_r=0

Schulte, S. R. (2013). *Cached: Decoding the Internet in Global Popular Culture*. NYU Press.

Schofield, H. (2013, June 27). Minitel: The rise and fall of the France-wide web. BBC. Retrieved from http://www.bbc.co.uk/news/magazine-18610692.

Shields, R. (Ed.). (1996). Cultures of the Internet: Virtual spaces, real histories, living bodies. Sage.

Schramm, W. L. (1964). *Mass media and national development: The role of information in the developing countries* (No. 25). Stanford University Press.

Schuman, M. (2011, Oct. 26). Can China's economy thrive with a censored Internet? Time. Retrieved from http://business.time.com/2011/10/26/can-chinas-economy-thrive-with-a-censored-internet/

Savin, A. (2013). *EU Internet Law*. Northampton, MA: Edward Elgar Publishing.

Shahin, J. (2007). The reassertion of the state: governance and the information revolution. In Krishna-Hensel, S. F., & Mauer, V. (Eds). *The resurgence of the state: Trend and processes in cyberspace governance* (9-34). UK: Ashgate Publishing.

Smith, M., & Menn, J. (2012, December 8). Russia, China alliance wants greater government voice in Internet oversight. *Reuters*.

Solum, B. (2009). Models of Internet Governance. In Bygrave, L. A., & Bing, J. (Eds.). *Internet Governance: Infrastructure and Institutions* (pp. 48-91). Oxford University Press.

Soubbotina, T. P. (2004). Glossary. In *Beyond economic growth: An Introduction to Sustainable Development*. World Bank Publications. Retrieved from http://www.worldbank.org/depweb/english/beyond/global/glossary.html

Steiner, P. (1993). On the Internet, nobody knows you're a dog. *The New Yorker*, 69(20), 61.

Stone, C. (1989). *Regime politics: Governing Atlanta, 1946–1988*. Lawrence: University Press of Kansas.

Taneja, H. & Wu, A. X. (2013). *How does the Great Firewall of China affect online sser behavior? Isolated 'Internets' as culturally defined markets on the WWW*. Cornell University Library. Retrieved from arXiv:1305.3311.

Taylor, M., & Quayle, E. (2003). *Child pornography: An Internet crime*. Psychology Press.

Tera Consultants. (2010*). Building a digital economy: the importance of saving jobs in*

*the EU's creative industries*. International Chamber of Commerce/BASCAP.

Thomas, D., Waters, R., & Fontanella-Kahn, J. (2012, August 27). The Internet: Command and Control. *Financial Times*.

Tsesis, A. (2013). The Right to Erasure: Regulating the Indefinite Retention of Data. *Wake Forest Law Review, 48,* 2014. Retrieved from SSRN: http://ssrn.com/abstract=2361669

Twitter. (2012, Jan. 26) Tweets still must flow. Twitter blog. San Francisco, CA: Twitter. Retrieved from https://blog.twitter.com/2012/tweets-still-must-flow

UNCTAD. (2003). *FDI in Landlocked Countries at a Glance. United Nations Conference on Trade and Development.* Geneva, Switzerland. Retrieved from http://unctad.org/en/docs/iteiia20035_en.pdf

Van Cuilenburg, J., & McQuail, D. (2003). Media policy paradigm shifts towards a new communications policy paradigm. *European journal of communication*, *18(2),* 181-207.

Villeneuve, N. (2008, Oct. 1) Breaching trust: An analysis of surveillance and security practices on China's TOM-Skype platform. *Information Warfare Monitor/ONI Asia*.

Verhulst, S. M., & Monroe, P. (2013). Introduction. In Price, M. E., Verhulst, S. G., & Morgan, L. (Eds.). The Routledge Handbook of Media Law (1-14). New York: Routledge.

Silver, V. (2011, Dec. 12). Post-revolt Tunisia can alter e-mail with 'Big Brother' software. *Bloomberg*.

Ting, G. & Feng, C. (1996). The rise of developmentalism across the Taiwan Strait. In Yü, B., & Chung, T. (Eds.). *Dynamics and dilemma: Mainland, Taiwan and Hong Kong in a changing world*. New York: Nova Publishers.

Voltmer, K. (2012). How far can media systems travel. In Hallin, D.C., Mancini, P. (Eds.). Comparing media systems beyond the western world (pp. 222-245). Cam-

bridge.

d'Udekem-Gevers, M., & Poullet, Y. (2001). Internet content Regulation: Concerns from a European user empowerment perspective about Internet content regulation. *Computer Law & Security Review*, *17(6),* 371-378.

Wagner, B. (2011). "I have understood you": The co-evolution of expression and control on the Internet, television and mobile phones during the Jasmine Revolution in Tunisia. *International Journal of Communication*, *5,* 1295–1302.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy*, *36(6),* 484-492.

Wand, I. (2012). *States and societies in the digital arena: ICT, state capacity, and political change in Asia.* (Master's Thesis.) Vancouver, Canada: The University of British Columbia, Vancouver. Retrieved from https://circle.ubc.ca/bitstream/handle/2429/43234/ubc_2012_fall_wand_itay.pdf?sequence=1

Warf, B., & Vincent, P. (2007). Multiple geographies of the Arab Internet. *Area*, *39(1),* 83-96.

Warf, B. (2013). *Global geographies of the Internet.* Springer.

West, D. M. (2005). *Digital government: Technology and public sector performance*. Princeton University Press.

Wilson, C. (2000). Policy regimes and policy change. *Journal of Public Policy*, *20(03),* 247-274.

Wingfield, N. & Macavinta, C. (1997, Jan. 15). China's national intranet. *CNET News*. Retrieved from http://news.cnet.com/2100-1023-262013.html

Wheeler, D. (2011). Does the Internet empower? A look at the Internet and international development. In Consalvo, M., & Ess, C. (Eds.) *The handbook of Internet studies* (pp 188-211). John Wiley & Sons.

Whittaker, Z. (2013, April 15). EU anti-piracy law overhaul under attack; ISPs warn

against site blocking, censorship. *ZDNet*. Retrieved from http://www.zdnet.com/eu-anti-piracy-law-overhaul-under-attack-isps-warn-against-site-blocking-censorship-7000014023/

Whittaker, Z. (2013, Nov. 5). EU justice chief: Europe should have its own spy agency to counter NSA snooping. *ZDNet*. Retrieved from hhttp://www.zdnet.com/eu-justice-chief-europe-should-have-its-own-spy-agency-to-counter-nsa-snooping-7000022818/

World Bank. (N.D.). ICT Glossary Guide: 100 ICT Concepts. The World Bank. Retrieved from http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:21035032~menuPK:282850~pagePK:210058~piPK:210062~theSitePK:282823~isCURL:Y,00.html#I

World Bank. (2012.) World Bank Development Indicators E-book. World Bank. Retrieved from http://data.worldbank.org/sites/default/files/wdi-2012-ebook.pdf

Yang, G. (2009). *The power of the Internet in China: Citizen activism online*. Columbia University Press.

Yang, G. (2013). Social dynamics in the evolution of China's Internet Content Control Regime. In Price, M. E., Verhulst, S. G., & Morgan, L. (Eds.). *The Routledge Handbook of Media Law* (pp. 285-302). Routledge.

Zheng, Y. (2008). *Technological empowerment: The Internet, state, and society in China*. Stanford University Press.

Ziccardi, G. (2012). *Resistance, liberation technology and human rights in the digital age* (Vol. 7). Berlin: Springer Verlag.

Zittrain, J. (2003). Internet points of control. *Boston College Law Review, 43(1).*

Zittrain, J. & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In Deibert, R. (Ed.) *Access denied: The policy of global Internet filtering* (pp. 29-57). Cambridge, MA: MIT Press.

Zhu, T., Phipps, D., Pridgen, A., Crandall, J. R., & Wallach, D. S. (2013). The Velocity of censorship: High-fidelity detection of microblog post deletions. Washington D.C.: 22nd USENIX Security Symposium. Retrieved from http://arxiv.org/abs/1303.0597

Zuckerman, E. (2010). Intermediary Censorship. In Deibert, R. J. (Ed.) *Access controlled: The shaping of power, rights, and rule in cyberspace* (pp. 71-85). Cambridge, MA: MIT Press.

Zuckerman, E. (2013, June 2). We Chat: Learning from the Chinese Internet. *My heart's in Accra blog*. Retrieved from http://www.ethanzuckerman.com/blog/2013/06/02/wechat-learning-from-the-chinese-internet/

# Appendix

## Freedom on the Net vs. Freedom in the World Scores

| | Freedom on the Net | Freedom in the World |
|---|---|---|
| Angola | 34 | 5.5 |
| Argentina | 27 | 2 |
| Armenia | 29 | 4.5 |
| Australia | 18 | 1 |
| Azerbaijan | 52 | 5.5 |
| Bahrain | 72 | 6 |
| Bangladesh | 49 | 3.5 |
| Belarus | 67 | 6.5 |
| Brazil | 32 | 2 |
| Burma | 62 | 5.5 |
| Cambodia | 47 | 5.5 |
| China | 86 | 6.5 |
| Cuba | 86 | 6.5 |
| Ecuador | 37 | 3 |
| Egypt | 60 | 5 |
| Estonia | 9 | 1 |
| Ethiopia | 79 | 6 |
| France | 20 | 1 |
| Georgia | 26 | 3 |
| Germany | 17 | 1 |
| Hungary | 23 | 1.5 |
| Iceland | 6 | 1 |
| India | 47 | 2.5 |
| Indonesia | 41 | 2.5 |
| Iran | 91 | 6 |
| Italy | 23 | 1.5 |
| Japan | 22 | 1.5 |
| Jordan | 45 | 5.5 |
| Kazakhstan | 59 | 6.5 |
| Kenya | 28 | 4 |
| Kyrgyzstan | 35 | 5 |
| Lebanon | 45 | 4.5 |
| Libya | 45 | 4.5 |
| Malawi | 42 | 3.5 |

| | | |
|---|---|---|
| Malaysia | 44 | 4 |
| Mexico | 38 | 3 |
| Morocco | 42 | 4.5 |
| Nigeria | 31 | 4.5 |
| Pakistan | 67 | 4.5 |
| Philippines | 25 | 3 |
| Russia | 54 | 5.5 |
| Rwanda | 48 | 6 |
| Saudi Arabia | 70 | 7 |
| South Africa | 26 | 2 |
| South Korea | 32 | 1.5 |
| Sri Lanka | 58 | 4.5 |
| Sudan | 63 | 7 |
| Syria | 85 | 7 |
| Thailand | 60 | 4 |
| Tunisia | 41 | 3.5 |
| Turkey | 49 | 3.5 |
| UAE | 66 | 6 |
| Uganda | 34 | 4.5 |
| Ukraine | 28 | 3.5 |
| United King-dom | 24 | 1 |
| United States | 17 | 1 |
| Uzbekistan | 78 | 7 |
| Venezuela | 53 | 5 |
| Vietnam | 75 | 6 |
| Zimbabwe | 54 | 6 |

Result Details & Calculation

X Values
$\sum = 2723$
Mean = 45.38
$\sum(X - M_x)^2 = SS_x = 25726.18$

*Y Values*
$\sum = 245.5$
Mean = 4.09
$\sum(Y - M_y)^2 = SS_y = 216.75$

*X and Y Combined*
$N = 60$
$\sum(X - M_x)(Y - M_y) = 2002.39$

*R Calculation*
$r = \sum((X - M_y)(Y - M_x)) / \sqrt{((SS_x)(SS_y))}$

$r = 2002.39166666667 / \sqrt{((25726.18)(216.75))} = 0.85$

Meta Numerics (cross-check)
$r = 0.85$

Key

*X*: X Values
*Y*: Y Values
$M_x$: Mean of X Values
$M_y$: Mean of Y Values
$X - M_x$ & $Y - M_y$: Deviation scores
$(X - M_x)^2$ & $(Y - M_y)^2$: Deviation Squared
$(X - M_x)(Y - M_y)$: Product of Deviation Scores

Chart