

# Democratic and Anti-Democratic Regulators of the Internet: A Framework

Michael L. Best<sup>1</sup>  
mikeb@cc.gatech.edu

Keegan W. Wade<sup>2</sup>  
keeganwade@gmail.com

## Abstract

We employ Lessig's framework of regulation to conceptualize the relationship between the Internet and democracy. Lessig defines four classes of regulators, forces that control and define systems such as the Internet. They are markets, architectures, norms, and laws. We propose that a "democratic regulator" is a force that serves to enhance civil or political liberties. And we argue by example that there are democratic (and, indeed, anti-democratic) regulators that control aspects of cyberspace. Expressing the democratic effects of the Internet in this manner may prove useful for future comparisons across existing Internet and democracy theories, especially in the realm of quantitative analyses.

## Introduction

Over the past 15 or so years there has been substantial speculation as to the relationship between the Internet and democracy, with most scholars falling into one of two main camps: the pro-democracy, "cyberoptimist" camp; and the anti-democracy, "cyberpessimist" camp (for a fairly comprehensive list of theories, see Norris, 2000 and Best & Wade, 2006). Of all the theories in the cyberoptimist camp, perhaps the most relevant is Christopher Kedzie's (1997) "dictator's dilemma" which posits that the very presence of the Internet is a boon to democracy. Conversely, exponents of the anti-democracy camp such as Shanthi Kalathil and Tyler Boas (2003) demonstrate that the authoritarian governments can harness the Internet for their own purposes. Despite all the different democratic viewpoints, scholars seem to have come to a consensus that, depending on the context, the Internet can be either a boon to democracy or a tool of oppression.

In order to explore how (or how not) the Internet might affect levels of democratization, we propose to make use of an existing theoretical framework, augmented somewhat to our ends. Lawrence Lessig (1999) has proposed a theoretical framework of "regulability," which has shown itself to be a powerful and important construction for describing methods of control and impact of the Internet. Below, we provide an overview of Lessig's

---

<sup>1</sup> Affiliated with the Berkman Center for Internet and Society, Harvard Law School and the College of Computing, Georgia Tech.

<sup>2</sup> Corresponding author. Technical Consultant with Blackbaud Inc.

argument and then suggest that there might be “democratic regulators” – constraints or affordances on the use of the Internet that might act as agents for (or against) political and civil liberties.

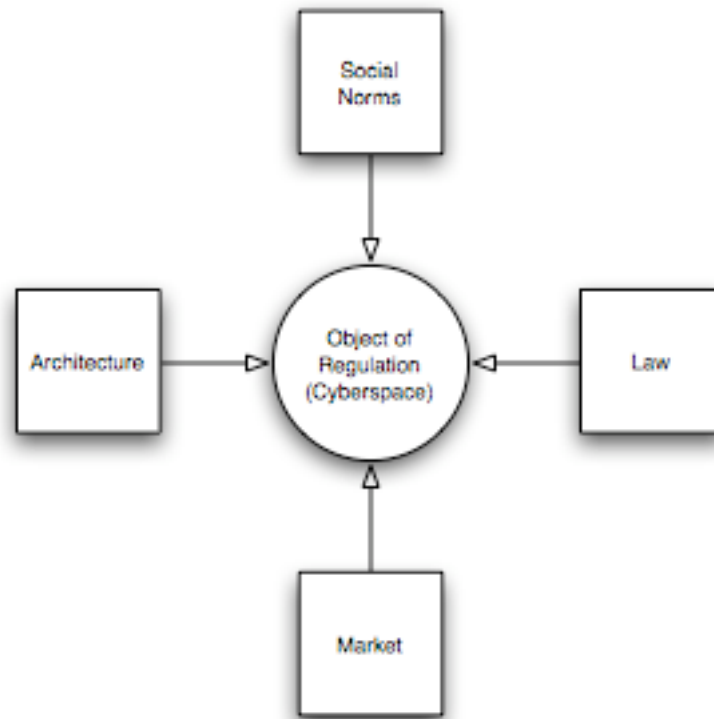
### ***Lessig’s framework of regulation***

Lessig’s framework identifies four forces that regulate or constrain an object (e.g. the Internet). They are: the law, markets, norms, and architecture (Figure 1). Each of these regulators has the following unique properties:

1. Law constrains by defining a command that, if broken, threatens punishment. Law is imposed by a state.
2. Markets regulate through price. The market regulator is immediate—it is characterized by a direct monetary exchange.
3. A social norm regulates through a stigma that a community (not a state) imposes. Deviation from a norm makes you socially abnormal, which can have negative affects, such as alienation from a community.
4. Architecture (or “code”) regulates through the physical burden it imposes. It is imposed immediately and automatically by its very design.

To illustrate this framework, consider how these regulators might relate to an individual, we’ll call him “Mr. X”, who is sending out unsolicited commercial emails on a massive scale.

1. The threat of criminal sanctions, for instance under the CAN-SPAM Act, may prevent Mr. X from SPAMing (a *legal* regulation).
2. Mr. X may not have sufficient funds to buy the personal computers, networking equipment, or internet service in order to engage in SPAM (a *market* regulation).
3. The threat that Mr. X’s friends might ostracize him if they find out that he is SPAMer might dissuade him from the practice (a *normative* regulation).
4. Finally, an ISP may employ a physical and virtual security system that prohibits sending of high volume email messages from a single source (an *architectural* regulation).



*Figure 1.* Lessig's framework for regulation.

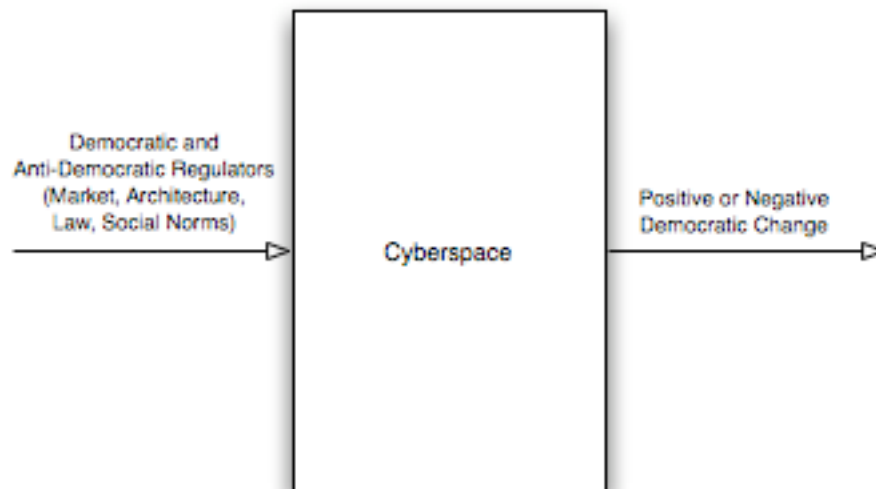
### **Democratic and anti-democratic regulators**

We say that a regulator is democratic if it increases civil rights or political liberties. Civil liberties include the freedom to develop opinions, institutions, and personal autonomy without interference from the state, which implies the freedom of expression and belief; freedom to associate and organize; rule of law; and personal autonomy and individual rights can be considered as civil liberties. Universal Service Obligations are laws that regulate operators. They are democratic because they serve to increase the reach of the network to under-served communities. And this, we believe, increases civil and political liberties.

In addition to defining democratic regulators, we also note the effects that anti-democratic regulators can have. An anti-democratic regulator is the opposite of a democratic regulator—it undermines civil liberties or political rights. If a government were to limit the speed at which their backbone servers operated by imposing bandwidth quotas, this could be classified as an anti-democratic regulator. Slower communication could result in citizens being less able to engage in civil society activities with each other online, causing democracy to suffer. Similarly, if a private ISP privileged certain commercial communications while restricting the communication of civil society this too would be anti-democratic within our framework. Witness the ongoing debate over Net Neutrality

where private ISP's wish to offer such premium services to their best commercial partners.

Again, it is our hope that the notion of democratic regulators might act as an explanatory framework as we try to understand the role of the Internet in the processes of democratization.



*Figure 2.* Democratic and anti-democratic regulators.

For each of Lessig's categories of regulation, prominent democratic or anti-democratic regulators of the Internet can be identified. We avoid trying to map associations between these regulators in different categories, even if such associations exist. This includes feedback associations. If we included these mappings, we would increase the complexity of our analysis enormously. As Lessig says, "The interaction among these four [forms of regulation] is hard to describe." (1999, p. 88). As such, we focus on the direct causal relationships between Internet regulation and democracy.

### ***Architectural regulators: Code***

#### **How it regulates**

We explore two kinds of code regulators: encryption software and filtration software. Encryption works by obfuscating messages so that third parties cannot read them. It can also ensure a message's authenticity and integrity. Some of the more prominent encryption technologies include SSL and PGP, which have been around since the mid-1990s.

Filtration prevents users/citizens from accessing information that would otherwise be available. It is well known that some governments use filtering technologies to block access to politically sensitive web sites (Kalathil & Boas, 2003).

## **Encryption**

Encryption can have a powerful positive effect on the democratization process by allowing, for instance, dissident groups to organize secretly. But, as Lessig points out, cryptography is “Janus-faced... it will stop crimes and it will create new crimes. It will undermine dictatorships and it will drive them to new excesses” (p. 36).

Encryption software such as PGP likely plays a part in keeping the communications of non-governmental organizations (NGOs) and transnational advocacy networks (TANs) private (Goodman & Drozdova, 1999). As such, encryption can prevent abusive governments from filtering NGO and TAN communications for political content. This is democratic because it allows for such organizations to share information on government abuses with the rest of the world, pressuring governments to reform (Selian 2002). There are numerous examples of international organizations that do this, including Amnesty International, Human Rights Watch, and the Environmental Investigation Agency.

## **Filtration software**

Filtration software can have negative implications for civil society since they can make it difficult for citizens to access media concerning political ideas, and can prevent people from associating with certain groups. For example, Zittrain and Edelman (2003) found that the Chinese government actively blocks a myriad of websites associated with politically threatening material, such as civil society and political websites. It does so largely by filtering for server IP addresses and URL keywords. This has the effect of preventing foreign-based civil society organizations and advocates from becoming a political force. For example, the Chinese government prevents the dissemination of Falun Gong information by blocking Falun Gong websites whose servers are located outside of China (Zittrain & Edelman, 2003, p. 9). Decreased access to information concerning organizations such as Falun Gong can keep people from organizing, equating to a loss in civil liberties. Many nations including Singapore, Vietnam, Saudi Arabia, Bahrain, Yemen, and the United Arab Emirates filter Internet content (Kalathil & Boas, 2003; Chalaby, 2000).

Thus, we argue on the one hand that encryption-enabled software can regulate or enable individual use of the Internet in ways that enhance democratic activities (and thus encryption can be a democratic regulator) or, on the other, that enhance the activities of authoritarian regimes (and thus encryption can be an undemocratic regulator). Filtration software, when embedded in the architecture of networks run by authoritarian states, serves as an undemocratic element of code.

## ***Market-based regulators: Internet access price***

### **How it regulates**

We offer examples where Internet access price, a market regulator, can lead to both democratic and anti-democratic effects. Our thinking is based on the assumption that increased Internet access leads to a greater and broader population of Internet users, which in turn can lead to more civil liberties. In line with this reasoning, we also assume that limited access has the opposite effect.

### **Internet access price**

For most nations, access price has been steadily decreasing (ITU, 2004). Increased Internet availability suggests that Internet access is penetrating a wider range of economic strata (as slow as these increases might be). A democratic implication of this is that more citizens gain access to a communications medium that holds the potential to educate, enhance personal autonomy, and even foster communal debate (through email, web forums, etc). The fact that the Internet is a multi-dimensional, non-centralized, and cost effective means of communication only amplifies its capacity to breed civil liberties in this regard (Kedzie, 1997; Boas 2000, pp. 57-58).

Inexpensive Internet communications better allow NGOs and TANs to organize and communicate, both in and out of authoritarian nations. Thus, “NGOs have been able to cut costs and improve the effectiveness and scale of their communications, planning, other logistics, and information gathering, storage, processing, exchange, and protection” (Goodman & Drezdova, 1999, p. 25).

A result of this is that NGOs can better expose and pressure abusive governments. For example, the International Tibet Independence Movement has credited the Internet’s cost-effectiveness for making their operations more efficient (Goodman & Drezdova, 1999). According to the Movement’s president, it greatly helped them organize and prepare for their 1996 “March for Tibet’s Independence”, and even allowed them to stream the march online. Hundreds of thousands of people accessed the website throughout the event.

But access price does not always fall over time for every nation. It is possible that some governments use price controls to keep certain users/citizens away from the Internet. Chalaby suggests that the Chinese government does this (2000) and Kalathil and Boas suggest that the Burmese authorities engage in this too (2003). If true, then access price can prevent citizens from exercising the civil liberties and political rights that they might otherwise gain if they could afford access, such as those listed in the previous paragraph.

Thus, low Internet access prices encourage a broader set of users and are thus democratic market regulators. Conversely, high Internet access prices would discourage use and be an undemocratic market regulator.

### ***Law-based regulators: State laws***

#### **How it regulates**

Laws can affect the Internet in ways that both hinder and encourage democracy. Free speech laws such as the America's First Amendment enable NGOs and TANs (including dissident exiles) to harness the power of the Internet to pressure for reform. Other kinds of laws can do the opposite, and clamp down on certain forms of free speech such as political dissent.

#### **State laws**

There are a host of NGOs and TANs around the world that depend on freedom of speech laws to pursue their political causes. This is important in the context of civil liberties and political rights because these groups have considerable power in exposing illegitimate government practices, possibly forcing them to grant their citizens political rights and civil liberties. The example of the Tibet Independence Movement from the previous section also serves as a good example here.

That said, various governments around the world—Malaysia, Turkey, China, and others—have criminalized politically dissident online speech—and this hurts civil liberties in those nations (Chalaby, 2000). For example, in China, a man named Lin Hai received a two year jail sentence for distributing Chinese email addresses to exiled dissidents (Chalaby, 2000). Even if these kinds of laws cannot be enforced in full, governments can still make occasional examples of dissenters, intimidating others.

### ***Socially normative regulators: Self-censorship rough consensus, working code***

#### **How it regulates**

We briefly explore two social norms that regulate the Internet: self-censorship, and the norms of the Internet Engineering Task Force (IETF).

#### **Self-censorship**

Self-censorship effectively restrains citizens from experiencing civil liberties they would otherwise enjoy on the Internet. Although subjective and variable, individual self-

censorship has similar democratic effects to filter-based censorship, in that it limits citizens' personal autonomy and freedom of association. Kalathil and Boas note that self-censorship on the Internet is apparent in a number of authoritarian nations, including Burma, China, Egypt, Saudi Arabia, Singapore, and Vietnam (2003).

## **IETF**

Founded in 1986, the IETF supplies the standards and protocols that form the Internet's architecture (Harris & Hoffman, 2004). Oversight by the IETF ensures that changes in the Internet's architecture are based on the criteria of technological efficacy, which can prevent governments from arbitrarily changing the Internet to suit their needs. This norm is embodied in their credo "rough consensus, working code" (Huizer, 1996).

While it is difficult to see how civil liberties or political rights can be gained as a result of the "rough consensus" IETF norm, we can confidently say that it keeps governments from removing them. For example, it keeps governments like the United States' from implementing backdoors in the Internet to accommodate wiretapping (McCullagh, 1999). The IETF discards changes such as these on the basis that they do not enhance the efficiency of the Internet.

## **The Value of this Framework**

There are presently several theories concerning how the Internet affects democracy, such as Kedzie's dictator's dilemma theory (1997), Steel and Stein's amplification theory (2002), Rosenau and Johnson's postinternational theory (2002), and others. Expressing these theories in the common language of regulators (as per our framework) simplifies the process of conducting comparisons between them. This is because all regulators operate at the same conceptual plane. To show how this might work, we provide an example involving two theories: Kedzie's dictator's dilemma (1997), a democracy-enhancing theory of the Internet, and the political disengagement theory (see Scheufele & Nisbett, 2002), an anti-democratic theory of the Internet. We suggest how each of these theories might be translated in terms of regulators, and then propose how these regulators might be operationalized if we ever wanted to get an idea of their causal weights. Quantifying regulators for regression analysis may help to determine which theory is the most credible in a particular setting.

## **The Dictator's Dilemma**

The dictator's dilemma occurs when commercial and financial pressures arising from globalization force dictators into relinquishing their monopoly over digital communications. It is a dilemma for the dictator because losing control of media can translate into weakened political influence, and increased political autonomy for citizens.

Internet content, specifically, can be difficult for governments to control due to the low cost at which large amounts of content may be transmitted, and the Internet's inherent capacity for multidirectional communications. Both of these characteristics make digital information more difficult for governments to filter, and provide civil activists with a powerful new resource by which to pursue their political ends.

The dictator's dilemma can be thus expressed in terms of regulators: When a dictator bows to financial pressures and begins to pursue more information technology-friendly policies, several regulatory mechanisms may bring about increased democratic activity in his country. For instance, if the dictator's government were to support the implementation of improved backbone services to increase the speed of business communications, this could be classified as an architecture-based democratic regulator as it potentially results in more opportunities for online citizens to engage in civil activities. The government may also decide to implement laws that promote ISP competition, which can have the effect of lowering Internet access prices for citizens, making online activities more affordable for a greater proportion of the population. This could be classified as a *market-based democratic regulator* since lower access price equates to more civil activists being able to afford access to the Internet. These regulators are illustrated in Figure 3 below.

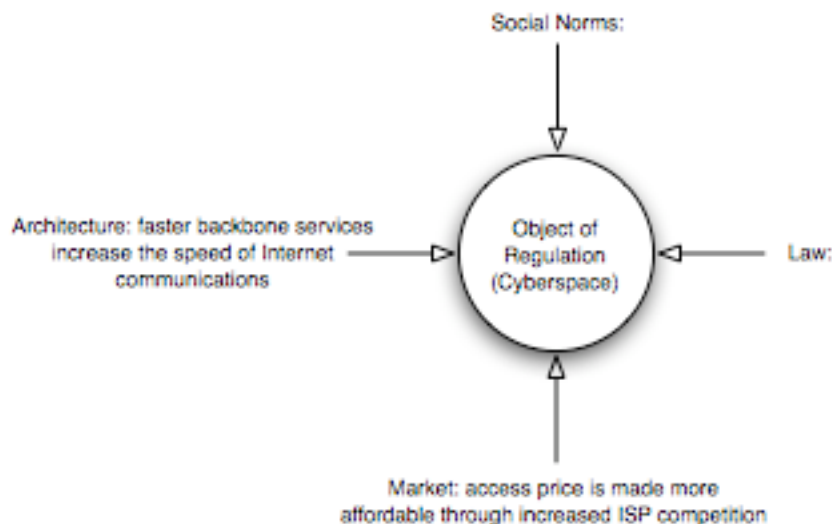


Figure 3. The dictator's dilemma as expressed in terms of regulators

## The Theory of Political Disengagement

The idea behind the theory of political disengagement is that even if people do have unrestricted access to the Internet, they may not use it for political ends anyway. One example is how the Internet may actually prevent people from keeping up to date with politics: Tewksbury and Althaus (1999) suggest that because online news is often

formatted in a way such that one story looks like it is equally important to every other story, Internet news-seekers attend less to political stories that are traditionally covered on the front page of newspapers. Indeed, Internet news-seekers are in no way obliged to view political matters at all if they don't want. Consequentially, these people become disconnected with politics, and democracy suffers.

This example illustrates *architectural regulation*, since the format of Internet news is responsible for discouraging Internet news-seekers from reading articles related to politics. It is anti-democratic since it potentially results in people becoming disengaged in politics, and prevents them from participating in those forms of civil activities (such as debates) that depend on individuals being politically informed. Figure 4 illustrates this regulator.

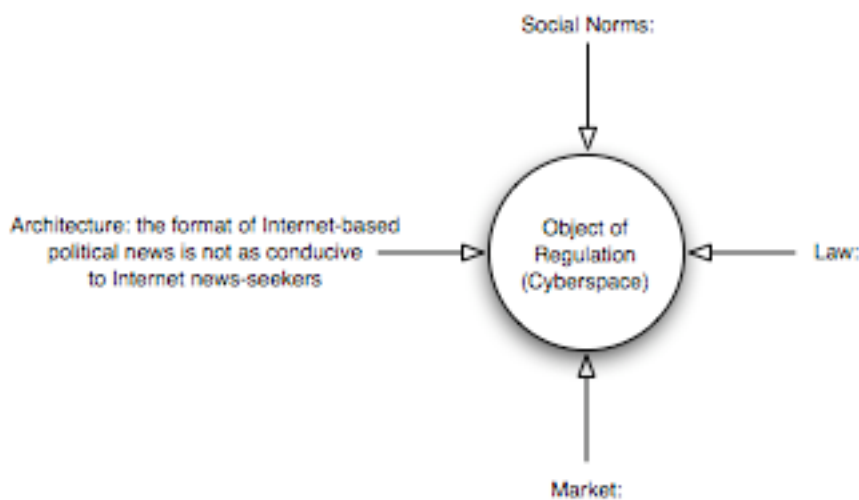


Figure 4. The theory of political disengagement as expressed in terms of regulators

### Comparing Between These Two Theories

By expressing these theories in terms of regulators, we have gained a new way to evaluate their relative worth. In our examples, the dictator's dilemma theory had two democracy-causing Internet regulators, and the theory of political engagement had one, although we cannot base the overall democratic influence of the Internet solely on the number of democratic and anti-democratic regulators at hand. Indeed, one of these regulators could well have more influence than the other two combined. Therefore, it would be prudent to estimate the relative weight of each regulator as it affects democracy, before arriving at any conclusions.

One way to do this is to operationalize the regulators as independent variables in a regression analysis. Although this task would be difficult to carry out on a global scale (due to a dearth of data), it may be more accomplishable in regional settings where specific instances of regulators can be quantified without too much trouble. In the above

examples above, a time-series regression model could be computed with a Freedom House or Polity variable acting as the dependent variable, along with the following independent variables (which represent the regulators):

- **Access price:** measured in dollars per hour of Internet access
- **Quality of backbone:** measured in bandwidth
- **Disengagement:** a survey-generated index indicating how politically connected Internet news-seekers are versus news-seekers of other media

The resulting regression's standardized beta coefficients would indicate the relative weight of each of these regulators, and the R squared score would be representative of the overall democratic compass of the Internet in the country at hand.

## Conclusion

In this essay, we employed Lessig's framework of regulation to examine possible ways that the Internet may affect processes of democratization. Lessig defines four classes of regulators, forces that control and define systems such as the Internet. They are markets, architectures, norms, and laws. We argue that *democratic regulator's* represent such a force that serves to enhance civil or political liberties. As we have seen, there are democratic (and, indeed, anti-democratic) regulators which control aspects of cyberspace. By expressing Internet and democratic theories in terms of democratic regulators, our framework simplifies the process of calculating the relative worth of these conceptual frameworks by providing a common level of analysis for comparison. By operationalizing regulators as independent variables, we may improve the comprehensiveness and accuracy of how we evaluate the Internet's democratic influence in various empirical settings.

## References

- Best, L. M., Wade, K. W. (2006). The internet and democracy: Global catalyst or democratic dud? In preparation.
- Boas, T. C. (2000). The dictator's dilemma? The internet and U.S. policy toward Cuba. *The Washington Quarterly*, 23(3).
- Chalaby, J. K. (2000). New media, new freedoms, new threats. *Gazette*, 62(1).
- Freedom House, Inc. (2004). *Freedom in the world 2004: Survey methodology*. Retrieved June 5, 2005, from <http://www.freedomhouse.org/research/freeworld/2004/methodology.htm>
- Goodman, S., & Drozdova, E. (1999). On liberty in cyberspace: Impact of the internet on human rights. *Stanford Journal of International Relations*, 1(2).

- Harris, S., & Hoffman, P. (2004). *Tao of the ietf* (Request for Comment (RFC)): The Internet Society.
- Huizer, E. (1996). *Ietf-isoc relationship* (Request for Comment (RFC)): The Internet Society.
- ITU. (2004). World Telecommunication Indicators. Geneva: ITU.
- Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes*. Washington: Carnegie Endowment for International Peace.
- Kedzie, C. R. (1997). Communication and democracy: Coincident revolutions and the emergent dictator's dilemma. from <http://www.rand.org/publications/RGSD/RGSD127/>
- Keohane, R., & Nye, J. (1998). Power and interdependence in the information age. *Foreign Affairs*(September/October).
- Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.
- Mathews, J. (1997). Power shift. *Foreign Affairs*(January/February).
- McCullagh, D. (1999). IETF says 'no way' to net taps. *Wired*.
- Norris, P. (2000, September 2). Democratic divide? The impact of the internet on parliaments worldwide. *American Political Science Association Panel*.
- Rosenau, J., & Johnson, D. (2002). Information technologies and turbulence in world politics. In J. E. Allison (Ed.), *Technology, development, and democracy*. Albany: State University of New York Press.
- Scheufele, D. A., & Nisbet, M. C. (2002). Being a citizen online: New opportunities and dead ends. *The Harvard International Journal of Press/Politics*, 7(3), 55-75.
- Selian, A. N. (2002). ICTs in support of human rights, democracy and good governance. International Telecommunications Union.
- Steele, C., & Stein, A. (2002). Communications revolutions and international politics. In J. E. Allison (Ed.), *Technology, development, and democracy*. Albany: State University of New York Press.
- Tewksbury, D., & Althaus, S. (1999). *Differences in knowledge acquisition among readers of the paper and online versions of a national newspaper*. Paper presented at the Annual Meeting of International Communication Association, San Francisco.

Zittrain, J., & Edelman, B. (2003). Empirical analysis of internet filtering in china. 2004, from <http://cyber.law.harvard.edu/filtering/china/>