Social Science Seminar Series
The Center for International Security and Cooperation

Stanford University

Thursday, October 16, 2014

The Digital Dictator's Dilemma: Internet Regulation and Political Control in Non-Democratic States

Jaclyn Kerr

Doctoral Candidate, Georgetown University
Predoctoral Fellow, Stanford University

Abstract: Over the last two decades, states around the world have struggled with the challenge of understanding the impact of the Internet and networked information and communication technologies (ICTs) within their societies and determining how best to regulate and govern these new technologies. This challenge has likely appeared particularly stark to hybrid and authoritarian regimes where the availability of these technologies has offered fundamental shifts in the forms of expression and association potentially attainable by citizens. But regime responses have differed dramatically, with some embracing the Internet and ICTs, investing in infrastructure, and turning a relatively blind eye to the new forms of discourse and activism they engender, while others have attempted in various ways to severely restrict the political uses of the Internet and related technologies.

This paper uses a mixed-method approach to analyze global patterns of Internet policy adoption across hybrid and authoritarian regimes, and to offer a preliminary model of key causal factors and processes influencing policy choice – particularly the choice whether to adopt restrictive policies that limit Internet use and content or to permit the development of and access to a vibrant uncensored Internet. The roles of political instability, ICT sector development, authoritarian learning and other factors are examined. Large-N analysis identifies global patterns of Internet restrictions, particularly noting policy clustering within regions and amongst states sharing similar cultural values or regime type, and examines how these patterns appear to be changing as Internet penetration increases. The paper also draws examples from the author's case study of Internet policy in the Russian Federation, tracing changes in domestic Internet policy choices and their relation to political instability and control, examining a critical period of policy change in a regime that had previously stood out for its relatively unrestricted Internet.

The Digital Dictator's Dilemma:
Internet Regulation and Political Control in Non-Democratic States

Jaclyn Kerr

Georgetown University

"The Net interprets censorship as damage and routes around it." – Electronic Frontier Foundation (EFF) co-founder John Gilmore, 1993

"The single most significant change in the politics of cyberspace is the coming of age of this simple idea: The code is law. The architectures of cyberspace are as important as the law in defining and defeating the liberties of the Net. Activists concerned with defending liberty, privacy or access must watch the code coming from the Valley - call it West Coast Code - as much as the code coming from Congress - call it East Coast Code." – Legal Scholar Lawrence Lessig, 1999

"Where it was once considered impossible for governments to control cyberspace, there are now a wide variety of technical and nontechnical means at their disposal to shape and limit the online flow of information." – Ronald Deibert and Rafal Rohozinski, 2010

On November 1, 2012, a new Russian Internet law went into effect that is ostensibly aimed at protecting children from websites promoting drug use, suicide, and pedophilia. The law, an amendment to the existing "Act for Information" which had been passed by both houses of parliament and signed by Vladimir Putin in July 2012, established a "blacklist" of banned websites to be managed and updated daily by Russia's Federal Service for Supervision of Telecommunications, Information Technology and Mass Communications, Roskomnadzor. Each blacklisted website was to be either directly shut down or blocked by all Russian ISPs. Major Russian Internet companies and human rights NGOs had protested against the law's passage, and many observers had argued that the law was a thinly veiled pretext for the introduction of Internet censorship and a further crackdown against pro-democracy and oppositional materials online (BBC Online, October 31, 2012). Within its first two weeks of implementation, the law led to the banning of over 180 sites, including a popular Wikipedia-style site "Lurkmore" that includes satirical pages making fun of Vladimir Putin (Elder, November 12 2012).

Over the last two decades, states around the world have struggled with the challenge of understanding the impact of new information and communication technologies within their societies and determining how best to regulate and govern these new technologies. This challenge has likely appeared particularly stark to

hybrid and authoritarian regimes where the availability of these technologies has offered fundamental shifts in the forms of expression and association potentially attainable by citizens. But regime responses have differed dramatically, with some embracing the new Internet and networked information and communication technologies (ICTs), investing in infrastructure, and turning a relatively blind eye to the new forms of discourse and activism they engender, while others have attempted in various ways to severely restrict the political uses of the Internet, mobile phone messaging, and related technologies. While a number of non-democratic states like China, Saudi Arabia, and Iran have long censored or blocked access to certain topics and sites for domestic Internet users, for example, others – including Russia and some other states of the former Soviet Union – have until recently shown less immediate concern about directly restricting online content and speech.

Why have Internet and information technology policy choices differed so dramatically across non-democratic regimes? What factors have influenced state decisions to adopt more- or less- restrictive approaches, and how durable are these choices once taken? What trends in Internet regulation can be observed in the wake of the Arab Spring, Russia's "Snow Revolution" movement, the "Innocence of Muslims" conflagration, and other prominent instances of protest and civic unrest associated with growing Internet use, and what do these patterns portend for the future?

This paper uses a mixed-method approach to analyze global patterns of Internet policy adoption across hybrid and authoritarian regimes, and to offer a preliminary model of key causal factors and processes influencing policy choice. Large-N analysis identifies global patterns of Internet policies, demonstrating that regime-type alone is an important but by itself inadequate indicator of policy choice. While policies regulating or restricting online freedoms of speech, media, access to information, or association often parallel their "offline" equivalents, such "online-offline policy-linkage" is only part of the picture. Even among non-democratic regimes with similar levels of Internet penetration, we see fairly dramatic variation in how these technologies are regulated. Examining factors which could make states of similar non-democratic regime types more or less likely to protect or restrict freedom of the Internet and networked technologies, I argue that regimes approach these policy decisions as a sort of "dictator's dilemma," in which they must balance between the domestic and international reputation-costs and lost economic opportunities related to restricting their Internet and their perception of the potential stability risks they face by allowing it to continue to grow unfettered. Noting patterns of policy clustering within regions and amongst states sharing similar cultural

values, I suggest that several diffusion and learning mechanisms are also playing significant roles in the spread of particular regulatory approaches.

The paper is divided into four sections. The following section on "Authoritarian Internet Regulation" further develops the puzzle in hand, examining the history of growing Internet regulation since the early web and the attitudes of Internet observers concerning the future prospects. Internet regulation and governance promise to be complicated and widely contested issues in years to come. I suggest that one useful theoretical prism from which to observe the diverse approaches states have taken to the Internet is from the perspective of theories of norm adoption and diffusion, viewing policy choice as a "dictator's dilemma" that is likely to be influenced by both domestic factors and international and regional pressures and norms.

The subsequent section, "Theoretical Argument: Internet Policy as Norm Adoption," provides an overview of my theoretical argument. Drawing on political science literature on regime type, norm adoption, and policy diffusion as well as the more specific literature on Internet regulation previously discussed, I examine possible domestic and international factors likely to influence regime Internet policy decisions, and develop a preliminary typology and set of related causal hypotheses by which to predict patterns of policy choice. Next, in the "Empirical Findings and Analysis" section, I use OpenNet Initiative (ONI) Internet filtering data to examine global variation in Internet policy, and its relation to regime type, Internet penetration rates, domestic political stability, regional norms, and other possibly relevant factors, discussing what theoretical insights can be drawn from the data. I examine patterns of policy clustering and longitudinal change within regions and cases as possible indications of underlying processes.

The paper concludes with a discussion of potential long-term trends in the future of Internet policy and governance, particularly focusing on the implications for the future of hybrid regimes.

AUTHORITARIAN INTERNET REGULATION

In his July 2010 article in Journal of Democracy, Larry Diamond described the Internet and other information and communication (ICT) technologies as "liberation technologies," which he defined as technologies "that can expand political, social, and economic freedom." In addition to their potential role in "mobilizing against authoritarian rule," Diamond suggested that the Internet and ICTs also play important roles in "widening the public sphere," creating conditions of greater "transparency and accountability" and in so doing "documenting and deterring abuses of human rights and democratic procedures," and even in helping

alleviate conditions of "poverty and ill health" amongst large populations (Diamond 2010). In a response to Diamond's discussion of "liberation technologies," in their October 2010 article "Liberation vs Control: The Future of Cyberspace," Ronald Diebert and Rafal Rohozinski discussed the conflicting and often confusing trajectories of cyberspace as a place both of "liberation" and of "control." They highlighted that such social complexity is a characteristic of all "technological systems" – especially in the area of communications and the era of globalization. A mix of many "actors, cultures, interests, and ideas" interact to generate rapid innovation through "dynamic density" and shape cyberspace as a continuously changing "ecosystem of physical infrastructure, software, regulations, and ideas" (Diebert and Rohozinski 2010). This ecosystem is by no means guaranteed to play the same "liberating" role or sustain the same user rights in all times and settings.

The debate over the role of the Internet as a technology of "liberation" or "control" highlights a gradual change in perception of the nature and potential governability of the Internet. While Lawrence Lessig's seminal 1999 book, *Code and Other Laws of Cyberspace*, helped first draw the attention of legal and technical communities in the United States to the Internet's potential vulnerability to new forms of regulation and technical restrictions, as early as 2006, Jack Goldsmith and Tim Wu began arguing that it was also not safe to assume the Internet's continued global uniformity: As states seek to assert control over this new and influential technology within their territories, the future nature of the Internet and rights of Internet users might differ dramatically by country (Lessig 1999; Goldsmith and Wu 2006). An increasing number of observers also point to the growing role of private IT companies in influencing Internet regulation (Ethan Zuckerman 2007, Rebecca MacKinnon 2012). Even within the context of Western democracies, legal scholars and activists now point to a changing and potentially less free Internet. Jonathan Zittrain has argued forcefully that, though there are many legitimate concerns such as security leading to changes in Internet regulation at all levels, there is a fundamental risk of the loss of the Internet's "generativity" – a quality that has permitted it to play such a novel and empowering role in society (Zittrain 2008).

Today a growing number of observers stress the extent to which the "liberation" argument must be leavened with a fair consideration of the varieties of levels, forms, and agents of control now present to regulate the use of cyberspace. Contrary to the early web idealists who believed the Internet could not be regulated, contemporary Internet scholars point to a growing list of "[ever-more] sophisticated cyberspace controls" (Deibert and Rohozinski 2010). Plotting the course from the early laissez-faire days of the 1990s

"'dot-com' boom," Deibert and Rohozinski have explained how "growing recognition of serious risks in cyberspace" – ranging from malicious software and cyber warfare to copyright and intellectual property infringement concerns – has "led to a wave of securitization efforts" that have in-turn given greater legitimacy to "government intervention in cyberspace more generally—including in countries whose regimes may be more interested in self-preservation than in property protections." While "more than forty countries, including many democracies, now engage in Internet-content filtering," the authors explain that many "next-generation controls" go beyond filtering, aiming more at "inculcating norms, inducing compliant behavior, and imposing rules of the road" (Deibert and Rohozinski 2010, 49). As Daniel Drezner, Evgeny Morozov and other "cyber-realists" have suggested, today, in some settings, it is unclear which is more empowered by the Internet: the power of civil society and protest movements to stand up to the state or the coercive control abilities of governments (Drezner 2010, Morozov 2011). Clearly much depends on the particular regulatory and restriction environment.

The approaches employed by governments to restrict or control Internet access and content have greatly expanded over the last decade. While both democracies and non-democracies have moved towards greater regulation, different types of non-democratic regimes have particularly cultivating a wide variety of technical and regulatory approaches in their efforts to control the influence of the Internet within their societies. These restrictions are not limited to the most closed authoritarian regimes, and they are not limited to keyword filtering or site blocking. While some of the most closed authoritarian regimes have attempted to completely cut their citizens off from the global Internet (e.g. North Korea), and others have implemented strict filtering and blocking regimes aimed to prevent their citizens from accessing content concerning any sensitive political or social issues and in some cases blocking their use of internationally popular social media sites (e.g. China, Saudi Arabia, Uzbekistan, Turkmenistan, Ethiopia, Thailand, Singapore), other countries have employed a variety of different approaches – some of them less obvious – to control content or access to particular materials or at particular moments. These include, for example, cutting off the Internet or other ICT networks entirely at critical moments (e.g. Egypt in January 2011), slowing Internet traffic (e.g. Iran in 2009), ensuring high costs for Internet access to limit the number of users, or the use of what Deibert, Rohozinski, and their OpenNet Initiative colleagues have called "second-generation" or "next-generation controls" (Deibert and Rohozinski 2010; Deibert et al. 2008, 2010, 2011; Murdoch and Roberts 2013; Crete-Nishihata et al. 2013; Pearce and Kendzior 2012; Howard et al. 2011; Milner 2006; Drezner 2010).

In his discussion of the influence of ICTs on the relative power of states and civil society, Dan Drezner details some of the specific innovations that have enabled "repressive states … to control information technologies more effectively than previously thought [,]" in spite of the growth of the technological tools available to citizens. Here, he points to the new "[t]echnical measures" that have emerged "to regulate the internet[,] include[ing] the creation of firewalls and proxy servers, routers, and software filters to block content labeled as undesirable." He also points out the employment of "[n]on-technical measures" such as "the imprisonment of relevant individuals, active policing, high taxation of internet access, and pressuring internet service providers (ISPs)."

Another issue seems to be the relative willingness (or unwillingness) of authoritarian governments to make the Internet widely available to their citizens. Controlling for economic development levels, a number of studies have shown that more repressive regimes have lower Internet usage rates. Beilock and Dimitrova, for example, "found that countries with lower Freedom House scores for civil liberties had significantly lower internet usage[,]" and Helen Milner's 2006 study of Internet diffusion shows that "*ceteris paribus*, democracies permit much greater online access, both in terms of internet users per capita and internet hosts per capita" (Drezner 35, citing Beilock and Dimitrova 2003). This would seem to support the notion that some authoritarian regimes limit Internet infrastructure growth in order to retain control over their segment of the web. As Jack Goldsmith and Timothy Wu have argued, keeping Internet transaction costs high for users is another effective, if imperfect way of limiting the spread of inconvenient information (Goldsmith and Wu 2006; Drezner 2010).

But, as Drezner points out, the control over the Internet is not just about minimizing Internet use or "crude" content filtering. Legal restrictions on web content, voluntary pledges administered to ISPs and web portal companies concerning what material they will disseminate, re-routing from foreign web service sites (such as search engines) to equivalent services provided by government owned companies, and the outright blocking of certain troublesome Web 2.0 social media applications all have permitted governments to retain a large amount of control over Internet content and uses, while simultaneously reaping the gains of foreign investment in information technologies. He points to Singapore as an example of a "nondemocratic state" that has "succeeded in restricting political content on the internet without sacrificing commercial possibilities" (Drezner 2010). This is the path of regimes "with a greater interest in maximizing economic growth" by

avoiding crippling their ICT sectors, and it "has become the model for many East Asian governments," he argues, "including China."

Authoritarian approaches to the Internet also appear to have grown increasingly pro-active and aggressive, with "coercive governments … learning how to turn Web 2.0 technologies to their advantage." This includes the growing use of: surveillance (the "monitoring of networking sites like LiveJournal" in Belarus that has prompted Evgeny Morozov to refer to social media as "a digital panopticon"), the use of online information to target activists or their families for persecution, and the use of "hackers [to] engage in cyber-attacks" (such as those that prompted Google's 2010 departure from China – seeking supposedly to steal information about both intellectual property and the identities of Chinese rights activists) (Drezner 2010; Morozov 2011).

Like Drezner, Deibert and Rohozinski and their collaborators also particularly stress the importance of the so-called "next-generation controls" – that go beyond more obvious approaches such as continuous site-blocking. The OpenNet Initiative's 2010 book, *Access Controlled: The Shaping of Power Rights and Rule in Cyberspace*, analyzed Internet regulations in over three dozen countries to indicate growing levels of restrictiveness and growing use of next-generation controls (Deibert and Rohozinski 2010; Deibert et al. 2010). These include "legal measures," "informal requests," "outsourcing," "just-in-time blocking," "patriotic hacking," and "targeted surveillance and social-malware attacks" (Deibert and Rohozinski 2010; Deibert et al. 2010). **Table 1** (on the following page) provides a brief description of each of these types of measures.

The existence of such a variety of "first" and "next" generation approaches clearly raises a question as to why different regimes have adopted different policy options and what is likely to influence these decisions further in the future. So far this question has attracted more theoretical discussion than empirical research. Most research that does exist so far on the subject of authoritarian Internet policy is more focused on examining and cataloguing the different approaches regimes are using to control the Internet, as opposed to seeking to explain the causal processes influencing regime adoption of these policies.

One theme that comes up frequently in the existing literature discussing authoritarian and hybrid regime Internet policy is the constraint imposed on some – if not all – states by a "dictator's dilemma"[1]

[1] Samuel Huntington famously coined the term "king's dilemma," to refer to the challenge confronting a ruler in deciding whether and to what extent to repress his populace to maintain order: "A forward-thinking king, who gives rights and freedom to serfs and makes them citizens, may end up abdicating his throne as these citizens agitate for more and more freedom over time …. But a worse

Table 1. Next Generation Internet Restrictions and Control Measures.

Type of Restriction	Description
Legal Measures	These new state techniques for regulating cyberspace include the use of "legal measures" and the threat of legal action to justify censorship, create a "climate of fear," and induce self-censorship. Sometimes these laws are justified explicitly in terms of national security, anti-extremism, anti-terrorism, or national values.
Informal Requests	Another major form of state Internet control is exercised through "informal requests" by which government officials put pressure on private companies – both "Internet Service Providers (ISPs) and online hosting services" – "to remove offensive posts or information that supposedly threatens 'national security' or 'cultural sensitivities.'" This extends even to governments asking "the companies that run the infrastructure, such as ISPs and mobile phone operators, to render services inoperative". (This includes examples such as the slowing down of internet traffic in Iran during the Green Movement in 2009, and the shutting down of most internet traffic in Egypt in January 2011.)
Regulation of Private Companies	The authors further stress the role of private companies and "outsourcing" in shaping the Internet's architecture of control. "[C]yberspace is owned and operated primarily by private companies [,]" they explain. "The decisions taken by those companies about content controls can be as important as those taken by governments." But such company decisions are often weighted against the bottom line of profit, with "[p]rivate companies often [being] compelled in some manner to censor and surveil Internet activity in order to operate in a particular jurisdiction[.]" Various privately-run access points to the Internet at different levels can be regulated. This includes Internet cafes, ISPs, telecommunication companies, heads of households with Internet access, and even computer manufacturers that sell personal computers within a given country. Various sorts of data-hosting services are also vulnerable, especially with the growing use of cloud-computing, webmail, and social media.
Just-In-Time Blocking / DDoS Attacks	Another increasingly prevalent new form of control involves the "disabling or attacking [of] critical information assets at key moments in time—[including] during elections or public demonstrations[.]" Distributed denial-of-service (DDoS) attacks using paid Botnets can be used for this purpose. "Cruder methods" have also been used, "such as shutting off power in the building where servers are located or tampering with domain-name registration so that information is not routed to its proper location." As the authors aptly point out, such temporary outages are often plausibly deniable – especially where infrastructure is already weak and outage prone, and when the actual attacks are perpetrated by contracted underground organizations.
Patriotic Hacking and 50 Cent-ers	Of course, not all pressures against dissenting Internet users within a country must be carried out by the government; some can be the work of other citizens. Some governments also pay or recruit citizens to take part in such "patriotic hacking" efforts. This includes the Wu Mao Dan ("50 Cent Party") in China (paid to post pro-regime statements in chatrooms and blog forums), the Iranian Cyber Army (that "took over Twitter and some key opposition websites" in 2009), and the supposed Russian "'seed[ing]' [of attack] instructions [to hacker groups] on prominent nationalist websites."
Targeted Surveillance	Another new emerging tool of Internet control is "targeted surveillance" – often through the use of "social-malware attacks." This includes highly targeted forms of espionage that seek out particular information or infiltrate social networks or networks of civil society activists. Viruses compromise unprotected computers or browsers, often unbeknownst to their users, and then become "vectors of attack" for the viruses' propagation.

Observers of internet policy in non-democratic states have indicated a number of measures used to restrict internet access, content, and use that go beyond the more obvious "first-generation" approaches of site blocking and filtering. This table describes several of the major "next generation" approaches to internet restriction. In addition to these, ICT use can also be restricted by measures explicitly targeting the use of smart phones (e.g. cellular network outages), or offline physical or legal attacks on individuals or organizations playing prominent roles in online media, commentary, or activism. Complete internet network shutdowns also have been utilized regionaly or nationally in some countries during moments of political crisis.

fate awaited those who clamped down on reform and repressed the populace; the pent-up demand for power, coupled with new ways for people to self-organize and communicate, led to an explosive reaction, usually with the result of the leader losing not only his throne but his head as well" (Huntington 1968). Dan Drezner, Clay Shirky, Ethan Zuckerman, and Philip Howard all point to similar dilemmas which might pose challenges to regimes which otherwise would choose to restrict Internet use.

situation that rulers face in determining whether or not to restrict Internet access or control its content. While these regimes might worry about the impact of new networked technologies on their control over society, they might also face significant costs in opting to restrict the use of these technologies. In non-democratic settings, growing Internet use is often thought to have significant impacts on patterns of communication, information-sharing, and civil organizing that can in turn impact state-society relations. It can potentially, for example, facilitate more rapid spread of information, increase preference revelation and shared awareness of grievance amongst citizens, heighten the ease and flexibility of protest mobilization, allow activists to bypass state media reaching new audiences, permit the development of new online protest tactics, and strengthen anti-regime organizational capacity. All of these changes might indeed appear to strengthen the hand of society and threaten the regime's stability. But regimes must weigh such concerns against the economic and legitimacy costs of restricting the new technologies. Economically, the costs of curtailing Internet use or content can be potentially significant, reducing a country's ICT sector development and cutting it off from many of the benefits of participation in the global economy. Depending how visible and widely noted such policies are, they can also reflect quite negatively on a regime's international reputation; what is more, they can also actually further reduce a regime's support at home.

While existing literature addresses such dilemmas and their potential influence on Internet policy decisions, it tends to gloss over how these trade-offs and their results might differ in particular contexts. Rather, the observation of such trade-offs has led different authors to reach opposite general conclusions concerning the likely resulting policy trends. While some suggest that the potential for economically viable high-control environments such as Singapore or China has shepherded the way for future global developments, others suggest that the associated economic and legitimacy prices will ultimately avert or undermine the most draconian policy choices. While I agree with these authors that a "dictator's dilemma" model can play an important role in the conceptualization of state policy choices, such variation in expected outcomes suggests the limits of a universal application of such a model without consideration of differences across states and over time. The costs and benefits of adoption will vary across states due to their specific characteristics, values, and international relationships. They will also vary across time, depending on changes in domestic and global context and policy trends.

In the following section, building on the notion of a dictator's dilemma model of state Internet policy decisions, I present a preliminary typological model showing how the domestic and international

characteristics and context of states might be integrated into understanding their Internet policy choices. While states' Internet policy choices clearly are heavily influenced by regime values and consistency with other aspects of state-society relations, I argue that the specific domestic economic and stability trade-offs, the international politicization of the issue of "Internet rights," and the high technical expertise required to implement certain policies have made Internet policy choice often distinctive from other areas of state control over society. I further suggest that the current global contest of "Internet Freedom" versus "Internet Restriction" can be seen as a complex process of global norm contestation in which the norm of "Internet Freedom" (itself still in the process of being defined) has been generally endorsed and promoted (though not universally followed) by democracies, while less democratic regimes have made a variety of different decisions. Domestic factors, regional and international interdependencies, and changes in the overall global context can all be seen as impacting the vulnerability of non-democratic states to norm-adoption pressures as well as impacting the set of available Internet policies from which they choose.

THEORETICAL ARGUMENT: INTERNET POLICY AS NORM ADOPTION

Why has the norm of "Internet Freedom" become so increasingly challenged and what explains why some states choose to restrict Internet content, access, or the rights of Internet users while others do not? While today it is clear that the Internet should not be seen in the manner of early cyber-utopians as constituting a separate realm from the real world of politics, and while Internet regulation in particular states must be understood in relation to the overall regime type and governance structures of those states, it is also clear that this technology constitutes a new and unique challenge to many states and that their reactions cannot be consistently predicted based solely on "regime type" or the manner in which a given state has tended to regulate some analogous set of offline phenomena such as civil society and association, media, or free expression.

In this paper, I argue against any one-size-fits all understanding of Internet policy choice by non-democratic states, and rather seek to explain the variety of levels and forms of restrictions adopted by seemingly similar regimes. While all non-democratic regimes might face some dictator's dilemma-type trade-offs influencing their Internet policy choices today, the pressures encountered by different regimes in making these decisions often differ in degree or kind, with some states facing more significant economic or legitimacy trade-offs, and others confronting more extreme challenges to domestic political stability. The perceived

balance of pressures and resulting policy options considered by particular states will therefore vary depending on the state's domestic characteristics and its relations with other states globally.

To explain regime Internet policy choice, therefore, it is necessary to take account of both individual state-level characteristics and aspects of the international context such as interdependencies, exogenous shocks, and global trends that might weigh on these decisions, and the mechanisms through which this influence occurs. In this section I discuss in turn the domestic and international state-level factors and the forms of interdependencies that are likely to influence individual regime policy choices at any given moment in time. I then present a preliminary typological model and related causal hypotheses by which to make sense of these varying influences and their effects on the diverse Internet policies adopted by different types of non-democratic regimes globally.

State-level characteristics of concern will include both domestic traits and aspects of a state's position and relationships in the international system. *Domestically, these factors will include the regime's prior policies in related areas such as the regulation of offline civic freedoms, the regime's perception of the threat it is facing from protest movements, and the degree to which it believes this to be heightened by growing Internet use, as well as the perceived benefits of growing Internet usage and how these would be influenced by different forms of Internet restrictions, the costs of implementing restrictive policies and the state's capacity to do so, and the additional domestic costs and risks that the regime expects to accrue as a result of restricting Internet usage in various ways.* In other words, this is the domestic portion of the "dictator's dilemma" described above. *International factors influencing a regime's Internet policy decision will include the degree of expected international pressure and reputation loss associated with restricting the Internet, the regime's vulnerability to that pressure, policy collaboration with other states, and diffusion following policy choices and their observed consequences in other states.*

Each of these domestic and international factors weighed in the regime calculation are based in turn upon the combined impact of several constituent elements. I explain these factors and their influences in substantial detail in **Appendix I**, at the end of this paper. Here I focus on developing a preliminary predictive typology and set of causal hypotheses, showing how these factors might be combined to predict the most likely Internet policy (and restriction) choices of particular types of states.

Preliminary Typology

Overall, I suggest that domestic and international factors operate together to influence the Internet

policies adopted by authoritarian and hybrid regime states. This adds up quickly to become a fairly complex causal picture, but one which I will seek to simplify. Below I develop a typological model for predicting the range of policy approaches likely for different types of regimes, indicating several overarching hypotheses.

Just considering the domestic state-level characteristics described above, we can draw out at least six factors that are likely to play important roles in the determination of how restrictive a policies to adopt and what specific forms these policies should take. These include: *"offline" regime type*, *Internet penetration / use levels in society*, *recent or current domestic protest levels*, *perceived restriction legitimacy or justifiability in the society*, *expected economic costs of restriction*, and the *state's technical "restriction capacity."* Looking just at regimes that are not fully democratic and considering just dichotomous values for each of these factors ("Authoritarian" / "Hybrid," "High" / "Low"), we end up with 64 potential combinations – some more or less plausible than others.

But for predicting large differences in overall restriction likelihood and level, the first three factors can likely do a good bit of the heavy-lifting. While economic costs, societal value resonance or perceived legitimacy of restrictions, and the state's technical capacity for mounting sophisticated restrictions will certainly also play important roles, I suspect these factors are heavily autocorrelated with the first three, and that specific distinct effects of these factors are most likely to influence the particular details of Internet policies and restrictions chosen more so than the overall level of restriction. [2]

Table 2, below, shows this simplified typology for predicting expected state Internet restriction levels and forms based on *"Offline" Regime Type* ("Authoritarian" or "Hybrid"), *Internet Penetration* ("High" or "Low"), and *Recent Protest Level* ("High" or "Low"). The fourth column shows the relative likelihood of a state having or adopting restrictive approaches to Internet regulation, and the final column suggests differences in the types of restrictions to be found in the different regime contexts. While offline regime type will certainly play one of the most significant roles in determining "online" restrictiveness, here we see that the degree of Internet penetration or use and the presence or absence of significant domestic protest

[2] There will likely be, for example, some correlation between the level of protest in the society and Internet penetration rate, on the one hand, and the perceived lack of legitimacy of Internet restrictions, on the other. Internet penetration level can be expected to correlate significantly with the level of economic development of a country, and particularly of its ICT sector, thus also most likely correlating with economic costs of Internet restriction, and the state's technical capacity to restrict the Internet. Where there are already significant grievances and the regime's legitimacy is already in question, and where unrestricted Internet use has already become common, the initiation of new restrictions is most likely to attract negative attention. Similarly, since countries with already high rates of Internet penetration are likely to be relatively technically advanced, such countries are both most likely to gain from continuing unrestricted ICT sector development and, at the same time, most likely to have the technical capacity to apply sophisticated Internet restrictions when or if the regime decides to do so.

movements against the regime are also likely to play important roles in determining the nature of this relationship.

Table 2. Domestic Factors: Simplified Typology of Expected Internet Restriction Levels.

"Offline" Regime Type	Internet Penetration Rate	Recent Protest Level	Restrictive Policy Likelihood	Likely Rescriction Type(s)
Authoritarian	H	H	*Very High*	1st & Next Gen Controls. Censorship of Political & Social Issues, Extremism, Pornography, & Copyright. Restrict Access, Content, & User Rights. Possibly sophisticated Technical Controls.
Authoritarian	H	L	*High*	
Authoritarian	L	H	*Medium*	Some 1st & Next Gen Controls. Blocking & filtering in all categories possible, though might be less technically sophisticated / "off-the-shelf."
Authoritarian	L	L	*Medium*	
Hybrid	H	H	*High*	Possibly sophisticated Next Gen. Controls. Any 1st Gen Blocking & Filtering likely non-transparent or only transparently applied to legally defined areas such as pornography, extremism, copyright. Restrictions likely increase in reaction to protest.
Hybrid	H	L	*Medium*	
Hybrid	L	H	*Medium*	Some Next Gen Controls or non-transparent 1st Gen Controls possible, though probably low-sophistication. Efforts might increase in reaction to web-enabled protest movements.
Hybrid	L	L	*Low*	

The table shows a simplified typology for predicting expected state internet restriction levels and forms based on regime type, ICT penetration level, and the recent protest level in the society. The fourth column shows the relatively likelihood of a state having or adopting restrictive approaches to internet regulation, and the final column suggests differences in the types of restrictions to be found in the different regime contexts. This typology only accounts for the most salient domestic factors, and outcomes will be subject to further influence by international pressures and relationship.

This typology suggests several core hypotheses: The most closed authoritarian regimes are, not surprisingly, expected to be the most likely to adopt the strictest forms of Internet restrictions. But not all such regimes will do so. As penetration rates increase, they are more likely to. As Internet access becomes increasingly widespread, the asymmetry between extreme offline restrictions on media, free expression, association, and political discourse and a wide-open online space for such forms of engagement will begin to appear more dangerous to the regime's stability, threatening the status quo as a larger public begins to engage in online discourse and association. This threat will be even more acutely felt in situations where active anti-regime protest movements have emerged, making regimes facing such instability also more likely to adopt new restrictions.

Thus ***high-penetration closed authoritarian regimes*** *are likely to have the strictest Internet restrictions, including both "1st generation" restrictions such as site blocking and keyword filtering, and possibly also a wider panoply of "next generation controls" as well.* Content related to sensitive political and social issues and protest efforts will likely be censored, possibly using sophisticated targeted censorship technologies. While such regimes are, in general, more likely to adopt restrictive Internet policies, they are most likely to do so if also faced with (and particularly at moments when faced with) significant domestic protest movements or other regime-threatening social and political instabilities.

Low-penetration closed authoritarian regimes *will in many cases also have extreme Internet restrictions, but this will likely be much more inconsistent, varying across regimes.* Those which have experienced large anti-regime protest movements will again be more likely to have cracked down even in spite of the low numbers of Internet users – possibly observing that protest leaders are disproportionately active Internet users. Since low penetration states are likely to be less technologically and economically developed, these states might not have access to or the ability to develop the most sophisticated technical controls; their ability to access off-the-shelf censorship or surveillance systems might depend on their relations with neighbor or peer states that also have adopted such systems.

For hybrid regime states – competitive authoritarian regimes or even authoritarian regimes which have attempted to retain the show of being electoral democracies and which have allowed their citizens some degree of civil liberties – the regime's decision process is likely to be even more complicated as Internet penetration increases. These states, like the closed authoritarian states, will feel the pressure of increasing Internet use creating a more open environment for political discourse, uncensored news, and free association,

leading to an online-offline asymmetry as Internet penetration grows. Even in states where some modicum of offline civic activity and political discourse have existed, the Internet and social media's engagement of a wider public brings this to a new order of magnitude – a risky change in a nondemocratic state, especially if there are widespread grievances or if a major protest movement emerges. But these ***high-penetration hybrid regime states*** often have based part of their domestic and international legitimacy on their status as "democracies." *An outright crackdown on the rights of Internet users or the obvious application of blunt "1st generation" filtering and blocking mechanisms might lead to significant reputation costs both at home and abroad. These states are therefore more likely to adopt more surreptitious and plausibly deniable "next generation" approaches to Internet control.* But the balance is tricky, and *large scale protest movements or other factors might push such regimes to crack down more bluntly, if they feel the softer targeted approach to have been ineffectual.* Such a visible and dramatic movement towards more repressive Internet policies (less in-keeping with democratic norms of "Internet Freedom"), however, will likely frequently mark a regime's loss of commitment to retaining "democratic" legitimacy, and will probably be accompanied by a more general shift of regime type towards a more closed authoritarian model. (We see this, for example, with the current Russian hardening of Internet policy, preceding and coinciding with the crisis in Crimea.)

There are reasons to expect ***low-penetration hybrid regime*** states to be both more and less likely to put restrictions on Internet use. At lower penetration rates, these states are less likely to feel as much risk of new political or social instabilities emerging from online activism or discourse. They also are likely to be less economically and technologically developed, and therefore have less access to sophisticated filtering, blocking, or other censorship or surveillance technologies. On the other hand, with Internet use less widespread and less foreign businesses quite possibly also involved in the domestic market, Internet restrictions are probably less likely to be widely noted. Such regimes, therefore, might face less domestic and international scrutiny when or if they do restrict Internet use, dulling some of the legitimacy cost pressures otherwise faced by hybrid regimes in applying various 1st or next generation restrictions.[3] Thus, *though we can expect that all hybrid regimes will be less likely to adopt the most extreme forms of Internet restrictions, it is also likely that the low-penetration hybrid regimes will show a fairly broad range of restriction levels. As*

[3] Thus Internet penetration rates among hybrid regimes might either have the reverse relation to likely Internet restriction levels or a weaker positive relation, compared to the relationship amongst closed authoritarian regimes.

with low-penetration closed authoritarian states, much will depend on the level of perceived instability and protest in the society and what particular technologies these regimes have access to.

As is clear in these descriptions, international factors are also likely to play some role in determining restrictive outcomes. **Appendix II**, at the end of this paper, develops an expanded typology that accounts for a regime's "International Pressure Vulnerability" and whether it has "Restrictive Peers / Neighbors" in addition to the three primary domestic characteristics just discussed, showing a heuristic prediction for how these international and intraregional interdependencies might further contribute to predicting Internet policy outcomes. Overall, while these international and regional forces will surely have some influence on state Internet policy adoption dynamics – especially with diffusion of particular legal or technical restriction mechanisms across regions or groups of states of particular regime types – it is unclear how much independent predictive force regarding restriction level can be expected from these factors relative to the domestic factors already mentioned.[4] That said, *we can expect to see regional and regime type clusters in terms of both restriction level and particular restriction types (technologies and legal mechanisms) being adopted.*

Summarizing the predictions of the above typology and preceding discussion, ***several major hypotheses*** can be made about the adoption of restrictive Internet policies in different types of states. Here I focus on policies that restrict Internet access, content and use in ways not broadly accepted by democratic states. The prevalence of surveillance or of filtering or blocking of child pornography or copyrighted materials become complex issues in their own rights as their acceptability are broadly contested within the conceptual debate over the meaning of "Internet Freedom." Restricting discussion therefore to more widely acknowledged violations of the "Internet Freedom" norm, we can make the following overall predictions:

(1a) *Democratic states are likely to have the least restricted Internet content and use. Though the actual levels of restriction will vary a little, the most open regimes will almost all conform to the main principles of "Internet Freedom" such as absence of major online content censorship around political and social issues.*

(1b) *Closed Authoritarian states are most likely to have the most restricted Internet content and use, though the actual restriction levels will vary considerably across regimes depending on other state characteristics.*

[4] Democratic and hybrid regime states are far more likely to be vulnerable to rhetorical pressure about "Internet Freedom" than are closed authoritarian states. Those with developed or developing ICT sectors and high Internet penetration are likely most vulnerable to economic pressure (perhaps mediated by foreign companies not wanting to engage in highly restricted environments). Regime type is likely to cluster in regions at least as much as Internet policy. So, while international and regional pressures and interdependencies are likely to play some role in the actual mechanisms influencing Internet policy, the outcomes might already be largely accounted for by the domestic variables.

(1c) *Hybrid Regimes will show significant variation in restriction levels, though generally avoiding the most extreme, visible, and obviously political content and use restriction measures.*

(2a) *As Internet penetration increases, while overall Internet regulation might increase, Democratic states will tend to have less obviously "norm-violating" restrictions (converging on a more-open model).*

(2b) *As Internet penetration increases, Closed Authoritarian states will tend to adopt more severe restrictions (converging on a more closed or filtered model).*

(3) *When faced with major domestic political instability (particularly regime-threatening Internet-enabled protest movements), regimes will tend to adopt more restrictive Internet measures.*

(4) *Some clear patterns of policy clustering can be expected, indicating elements of diffusion, learning, and knowledge transfer, especially within culturally and geographically interconnected regions.*

These hypotheses leave the future of "hybrid regime" states a bit of an open question: as Internet penetration increases, especially if faced with mass protest mobilization, will such regimes adopt the more extreme restrictions common among full authoritarian states, will they further liberalize and come to resemble the more democratic open model, or will they continue to maintain a distinctive approach to Internet regulation?

The following section draws upon empirical data to further examine the sources of Internet policy approaches across different non-democratic regimes. Demonstrating that regime type alone is not sufficient to explain observed variation in policy choice, the analysis provides evidence in support of the typology and hypotheses developed above. Cross-sectional and longitudinal data is used to analyze the effects of the different domestic and international causal factors that have been discussed, and identify developing trends in global Internet policy norms. More detailed case discussions illuminate some of the particular causal processes currently at play – particularly in hybrid regime or formerly hybrid regime states where Internet penetration rates have risen rapidly.

EMPIRICAL FINDINGS AND ANALYSIS

This section utilizes both "large-N" data and case studies to further examine causal factors and processes hypothesized in the previous section. For large-N statistical analysis of Internet restrictions, I focus here on the use of "first generation" Internet content filtering and blocking schemes for which multi-country cross-sectional data is available. Longitudinal observations of several states in the Middle East and North Africa and the former Soviet Union permit a closer examination of processes of change across time for individual states and regions, as they react to domestic instability, regional policy norm shifts, or changes in

global trends. Analysis examines the implications of the apparent causal patterns, particularly scrutinizing the pressures faced by hybrid regime countries as Internet penetration increases and Internet policy choices become more globally politicized. Prominent hybrid regime examples show how "next generation" approaches to Internet restriction have been applied sometimes in the absence of or in addition to minimal filtering and blocking mechanisms, but they also show how such regimes might face increasing pressure to adopt more absolute Internet restrictions, faced with perceived existential threat as penetration and protest levels increase.

Global Internet Censorship Patterns

Global Internet censorship data provides clear evidence of a more complex causal relationship than a simple correlation between offline regime type and online restrictions. Some degree of policy linkage should clearly be expected, with the very most repressive closed authoritarian regimes permitting little freedom of speech or association in either offline or online settings, and the most free liberal democratic regimes permitting high levels of freedom both off- and online. Nonetheless, there is considerable variation in the relationship of the freedoms regimes permit in these two settings, with some quite repressive regimes permitting relatively unrestricted Internet content and access, and wide variety in the forms and degrees of Internet restrictions among slightly more open hybrid regime states. Other factors developed above help to explain some of this variation.

Regime Type and Policy Linkage:

Figure 1 demonstrates this point, showing a plot of approximate Internet filtering levels (OpenNet Initiative data 2011[5]) versus civil liberties restrictions (Freedom House Freedom in the World data 2011) globally, for all states for which the two scores are available. The filtering data is based on a five point scale (with 4 as the highest filtering value), and the civil liberties scores are measured on a seven point scale (where 7 is the most repressive). We can observe here that most of the data points fall on or below the diagonal line from the lower left to upper right corners of the graph – the line that would represent the approximate expected pattern of correlation, if online-offline policy-linkage were to explain all variation in Internet filtering levels. But this "lower right-hand corner" distribution pattern of the plot suggests that a high FIW Civil Liberties score (restricted civil liberties) is necessary, but not sufficient to predict a high level of Internet

[5] The 2011 ONI data consists of the most recent available data for each country in 2011. Global country data was collected between 2007-2011 (OpenNet Initiative 2011).

filtering (Ragin 2010). The states that fall far below the line indicate cases of "policy asymmetry," in which the Internet is left relatively unfiltered compared to the level of offline restrictions citizens face on their civil liberties (Etling et al. 2010).

Figure 1:

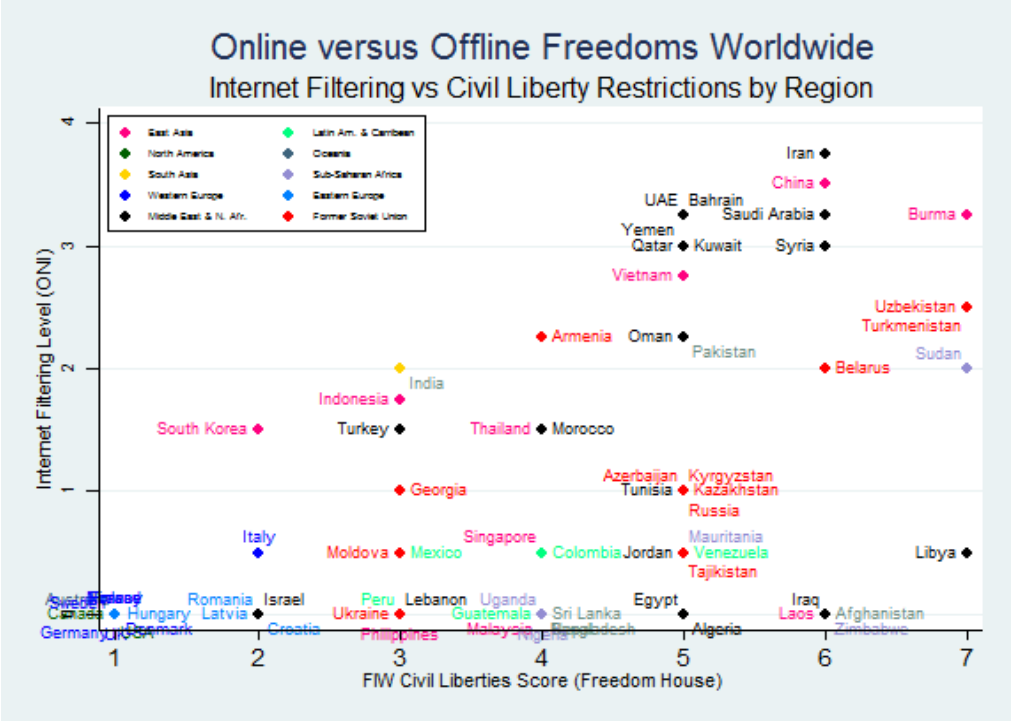


Figure 2 replicates Figure 1, but uses Freedom House's combined "civil and political liberties" scores for each country, demonstrating that this pattern of wide variation in Internet policy even amongst the most repressive regimes is fairly robust, whether considering only the offline repression of civil liberties or the overall context of political and civil freedoms.

Table 3 further reinforces this point, showing the OLS regression results of the regression of the country ONI Internet Filtering index versus the Freedom House Civil Liberties, Political Rights, and Combined Freedom in the World (FIW) indexes respectively. For each model, the relationship between online filtering and regime restrictiveness is positive and statistically significant, but the adjusted R^2 scores ranging from 0.2877 to 0.3037 show that none of these measures of offline regime type are sufficient to explain all the variation in Internet filtering levels.

Figure 2:

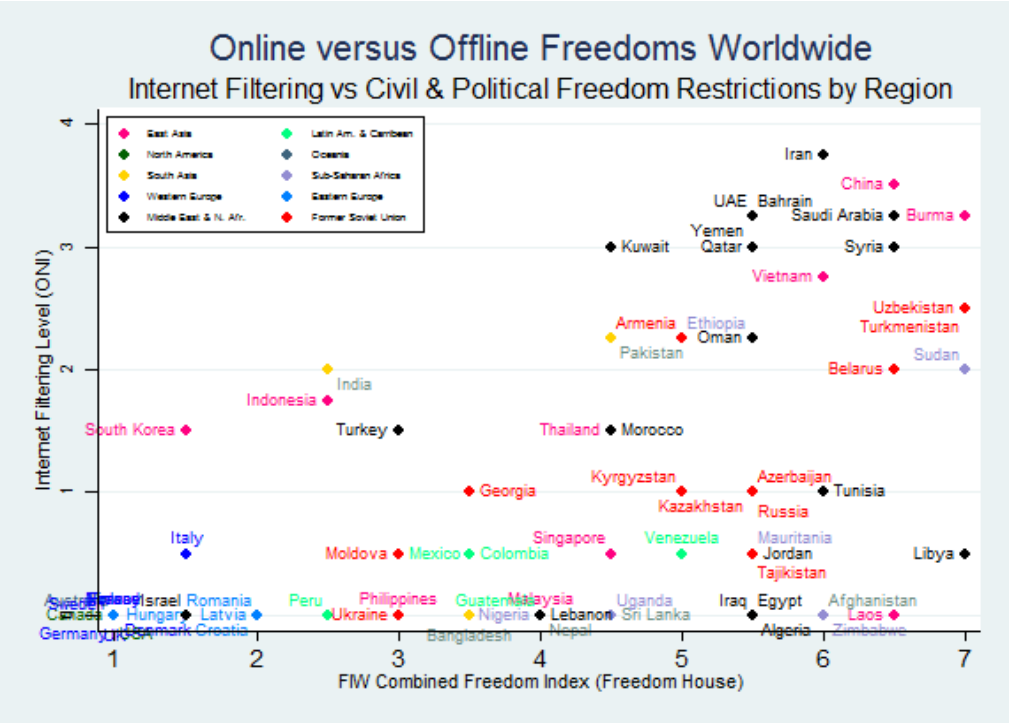


Table 3. Online versus Offline Freedoms Worldwide:
OLS Regression of Online versus Offline Regime Restrictions

Variable	Internet Filtering Level	Internet Filtering Level	Internet Filtering Level
Civil Liberties Restrictions	0.369*** (5.66)		
Political Rights Restrictions		0.299*** (5.49)	
FH Combined Index			0.341*** (5.69)
Constant	-0.458 (-1.61)	-0.260 (-1.00)	-0.393 (-1.44)
Adjusted R^2	0.3011	0.2877	0.3037
Observations	73	73	73

t statistics in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

As Figures 1 and 2 and Table 3 make clear, regime type – and particularly a regime's level of repressiveness of offline behavior – is causally relevant to Internet policy, but not sufficient to predict regime

policy choice. Turning back to the hypotheses developed in the previous section, these findings support *Hypotheses 1a-1c* regarding the likely range of Internet restriction levels for different regime types. What can we say of the relationships with Internet penetration rates and regime stability or protest levels?

Internet Penetration:

Internet penetration rate proves to have a divided effect, having distinct and opposite influences on the filtering levels among the most authoritarian and democratic regimes, but with a more ambiguous relationship to the hybrid regimes in the middle.

Figure 3:

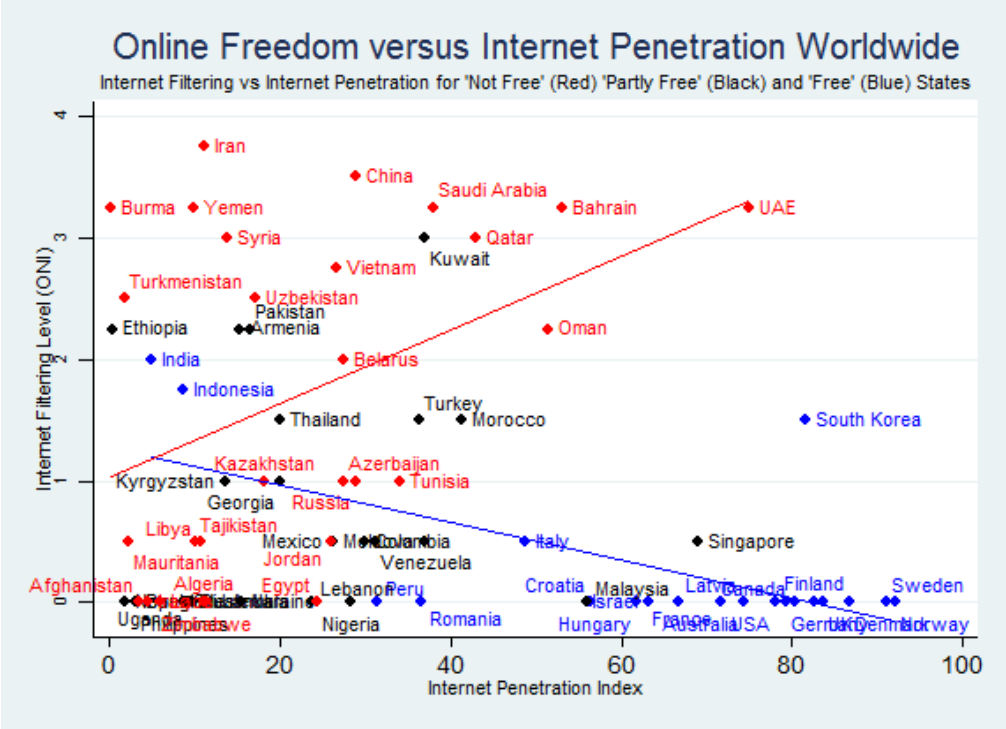


Figure 3 shows a scatterplot of Internet filtering levels versus Internet penetration rate (IPR) indexes by country, with countries color coded as "free" (blue), "partly free" (black) or "not free" (red) by their combined Freedom House index of regime type (FIW). The best fit regression lines for the "not free" (most authoritarian) and "free" (most democratic) regimes show evidence that authoritarian and democratic regimes are actually following two distinct trends as Internet penetration rates increase. While, among the most authoritarian states, filtering levels are likely to increase with increased penetration, the opposite is true for democracies, with filtering levels decreasing as penetration rates grow. These findings support *Hypotheses 2a-2b* above, while again raising the question of the likely trajectory for "hybrid regimes."

It is interesting here to observe the dynamic among the "partly free" states. Though certainly not a perfect measure of regime type, this categorization provides some sense of those regimes that might have a mix of democratic and non-democratic traits and institutions, and for which their status as "democracies" (however imperfect) might play an important role in their legitimizing strategy. This group – including states like Turkey, Venezuela, Kyrgyzstan, and Thailand – appears to be not quite clearly following either trend. Rather, these states still appear *mostly* on the lower-penetration side of the plot, not yet having reached the penetration level at which the differentiation between the high-penetration authoritarian and democratic groups becomes clear. The OLS models in **Table 4** confirm this distinction in cross-sectional statistics: While, among "free" regimes there is a statistically significant negative relationship between Internet penetration and filtering level, and for not "not free" regimes there is a statistically significant positive relation between penetration rate and filtering level, for "partly free" regimes, there is no statistically significant relationship.

Table 4. OLS Regression
Internet Filtering Levels for "Free," "Partly Free" and "Not Free" Countries

Variable	Internet Filtering in "Free" Countries	Internet Filtering in "Partly Free" Countries	Internet Filtering in "Not Free" Countries
Internet Penetration (IPR)	-0.0156** (-3.36)	0.00961 (0.84)	0.0276* (2.10)
Constant	1.283*** (4.03)	0.484 (1.44)	1.140** (3.17)
Adjusted R^2	0.3507	-0.0136	0.1057
Observations	20	23	30

t statistics in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

What determines what will happen in these erstwhile less repressive non- (or partial-) democracies as penetration levels increase? What will determine which ones follow the path of the most closed authoritarian regimes, cracking down on Internet freedoms versus which ones are more likely to follow the path of the democratic states, becoming less likely to filter the Internet as penetration increases? One explanation here is that many of the "partly free" / "hybrid regime" states are still at lower penetration rates – and at lower

penetration rates policy choices remain less differentiated by regime type. But other domestic and international factors also appear to be playing important roles in determining these policy choices.

Domestic Protest Levels

As discussed above, domestic protest levels and regime stability concerns are likely to play an additional role in determining policy choice. It is difficult to observe this effect directly with cross-sectional data, as the dynamic is most likely to unfold longitudinally within particular states. We might expect to see an increase in Internet restriction in states where new forms and levels of protest emerge as Internet penetration increases, or where significant existing protest movements make use of the Internet to further their mobilization efforts. The best evidence of such an effect will be the observation of increased Internet restriction by regimes experiencing or having just experienced significant domestic protest movements – particularly if these increases seem disproportionate to any simultaneous increase in Internet penetration rate and do not result in an overall liberalization and change of regime-type.

While the work to develop the type of global longitudinal dataset of protest events and filtering levels necessary for a Large-N analysis of such dynamics is beyond the scope of this paper, some indication of the possible larger-scale pattern can be gleaned from the observation of a few known cases. During the Arab Spring and its aftermath, some examples of this sort in MENA states have been widely publicized. Egypt, Libya, and Syria, for example, have each experienced complete or near-complete national Internet shutdowns during periods of domestic protests and conflict. Bahrain was added to the Reporters Without Borders' 2012-2014 "Enemies of the Internet" lists after its further crackdown on Internet freedom in reaction to the country's February 2011 pro-democracy protest movement. Iran has also faced a significant Internet crackdown during and following the 2009 post-election Green Movement, with significant decreases in national Internet speed, increases in censorship and surveillance over cybercafés, and the announcement of a national plan to create an isolated "Halal Internet" national intranet, cut off from the broader World Wide Web.

The FSU region also offers a number of interesting examples, as a region that has, until recently, made more limited use of 1st generation restrictions. Uzbekistan, which – along with Turkmenistan – has the most pervasive Internet restrictions in the FSU region, significantly increased Internet site blocking and cracked down on online freedom of expression following the so-called "Andijan Massacre" (the shooting of hundreds of protesters by state troops) in May 2005. Belarus, which has increased Internet filtering, legal

restrictions[6], and other next-generation restrictions in reaction to protest movements in 2006 and 2011[7], has been included in the Reporters Without Borders "Enemies of the Internet" lists in 2005-2008, and 2012-2014. In Kazakhstan, after YouTube, online media outlets and blogs were used to publicize the violent crackdown on a large oil worker's strike in the town of Zhanaozen in Western Kazakhstan in December 2011, the regime temporarily shut down local Internet and cellphone networks in the region, detained and harassed bloggers, mobilized competing "blog tours" to publicize a more pro-regime interpretation of the events, and ultimately prosecuted the online media outlets that had reported on the story. By many accounts, site blocking in the country has also increased.

Russia's recent move towards more repressive approaches to Internet regulation particularly stands out, as it has long been an exemplar of a country that, though perfecting many of the "next generation" approaches to Internet regulation has nonetheless permitted a fairly vibrant online space to develop – including significant online political discourse and regime-critical blogging – with limited or no blunt 1st generation site blocking or filtering even as Internet penetration rates have rapidly increased. In reaction to massive anti-regime protests in 2011 and 2012[8], however, and to the ongoing simmering protest movement partly galvanized around the charismatic and popular opposition blogger Alexei Navalny, the regime has taken unprecedented measures since 2012, for the first time creating a national list of blocked sites and requiring ISPs to censor the Internet, as well as prosecuting Navalny and others involved in the protest movement. As an electoral democracy that has had at least some protection of basic civic freedoms like the freedom to associate, Russia has, until recently, been widely considered some form of "hybrid regime;" the recent online and offline crackdown, however, suggests that the vibrant new activism unleashed by growing Internet penetration has in fact ultimately caused the country to move more towards closed authoritarianism, and it certainly has led to an increase in Internet restrictions in response to domestic instability. Since the summer of 2012, a series of new laws, legal prosecutions, and extralegal pressures have been used to shut down or alter the course of independent civil society and media outlets, as well as enabling the blocking of online materials and prosecuting some prominent online activists and bloggers. As of October of 2014,

[6] These legal restrictions include laws increasing the liability of Internet service providers and café owners, restricting legal access to foreign websites, and increasing online slander liabilities.

[7] After the quelling of large protests around the 2006 elections, the simmering protest movement again broke out into larger "clapping" demonstrations during the summer of 2011, organized through groups on social media platforms such as VKontakte.

[8] From 2009-2012 the country experienced escalating protest movements concerning issues such as environmental conservation, driver's rights, corruption, and culminating in the "White Ribbon" or "Snow Revolution" protest movement against Vladimir Putin and his political party surround the legislative and presidential elections of winter 2011-2012.

restrictions on Internet content and independent media have reached a new unprecedented level, with a series of new restrictive Internet laws adopted over the preceding year and the sites of Navalny's blog, leading independent online media outlets, and social media group pages supporting Ukraine's new government blocked, while other media outlets have been closed, had their editors replaced by Kremlin royalists, or pushed towards the brink of financial ruin. This raises some interesting questions about the possible future trajectories of other hybrid regimes facing growing Internet penetration and the development of significant domestic protest movements. It also shows that, at moments of crisis where the relative (asymmetric) freedom of a less restricted Internet appears as a liability, at least some hybrid regimes will move towards more of a closed authoritarian model – reducing freedom both online and offline – as opposed to permitting continued unrestricted Internet use.

These longitudinal case observations appear to support *Hypothesis 3* above, suggesting that many regimes (particularly non-democracies) are likely to restrict Internet freedom when confronted with mass protests or other threats to regime stability.

International and Regional Influences:

As we have discussed in the previous section, domestic characteristics are not the only factors potentially influencing state Internet policy decisions. The level and forms of Internet restrictions a regime adopts are also likely to bear similarities to those adopted by its neighbors and peers, and, while some such similarities can be explained by similar reactions to similar domestic circumstances, it is also quite likely that such choices are influenced by the degree to which a state's neighbors and peers adopt restrictions (as well as the types of restrictions they adopt), and by the degree to which it is subject and vulnerable to international pressure and reputation costs encouraging it not to adopt restrictions.

We can observe some evidence of these dynamics in the ONI's 2011 global filtering data. In this data, geographic neighborhood clearly stands out as a predictor of Internet filtering level and other restrictive policy choices. Returning to the plots of filtering levels versus offline regime type in Figures 1 and 2, above, note the regional color coding of states from "East Asia," "South Asia," "Latin America and the Carribean," "North America," "Sub-Saharan Africa," "Western Europe," "Eastern Europe," the "Middle East and North Africa," and the "Former Soviet Union."

The regional color-coding of these plots demonstrates some level of apparent regional and sub-

regional clustering, with the Gulf (GCC) states[9], for example, constituting a clear group in the upper right corner of these plots, joined by the non-democratic states of East Asia, Iran, and Syria. Even "partly free" Kuwait joins its geographic and cultural neighbors in the same approximate level of high Internet filtering. The "not free" states of the former Soviet Union form two apparent clusters, with Uzbekistan, Turkmenistan, and Belarus gravitating towards the high-filtering range, while the rest of their regional peers constitute a cluster in the lower right corner, joined by most of the non-GCC Arab states. (Since this data is from 2011 it likely underrepresents the current levels of filtering in Russia and Kazakhstan following recent crack-downs.) In Latin America, even the most non-democratic states show little signs of Internet filtering in this data, while even some democracies in East and South Asia (Indonesia, South Korea, India) have moderate levels of filtering (exceeding the levels in Russia and Kazakhstan at the time of measurement, for example).

A similar clustering pattern is evident in **Figure 4**, below, which repeats the plot of Internet filtering versus Internet penetration rates from Figure 3 with regional color-coding. Here the regional and sub-regional clusters are again quite evident, with Western and Eastern Europe and North America forming most of a high-penetration low-filtering cluster, the GCC states within the Middle East and North Africa (MENA) region constituting a high-penetration high-filtering cluster, and states of the former Soviet Union (FSU) region forming a noticeable cluster in the low-to-middle penetration and low-to-moderate filtering range. Latin American states form a cluster in the lower-penetration and lower-filtering range, while the majority of East Asian states are clustered in the lower-penetration higher-filtering corner of the plot.

These regional clustering patterns appear to indicate different propensities towards Internet filtering in different world regions, all other things being equal. **Table 5** provides further evidence of this regional differentiation, showing separate regression models of Internet filtering level against Freedom House civil liberties restriction scores for the FSU, MENA, and East Asian regions, considering all regimes in which Internet penetration rates had reached the minimal threshold of 15% in 2010. These regression models show that the predicted filtering values for the FSU region are below those for the other regions at all civil liberties values in the "partly free" and "not free" range. What is more, the regression coefficient for the civil liberties index in the FSU model (0.416) is less than those for the MENA (0.713) and East Asia (0.580) models, indicating that a given increase in offline civil liberties restrictions in the FSU region correlates with less of an increase in Internet filtering than it does in these other two prominent regions.

[9] (The GCC appears as a sub-region of the Middle East and North Africa (MENA) region.)

Figure 4:

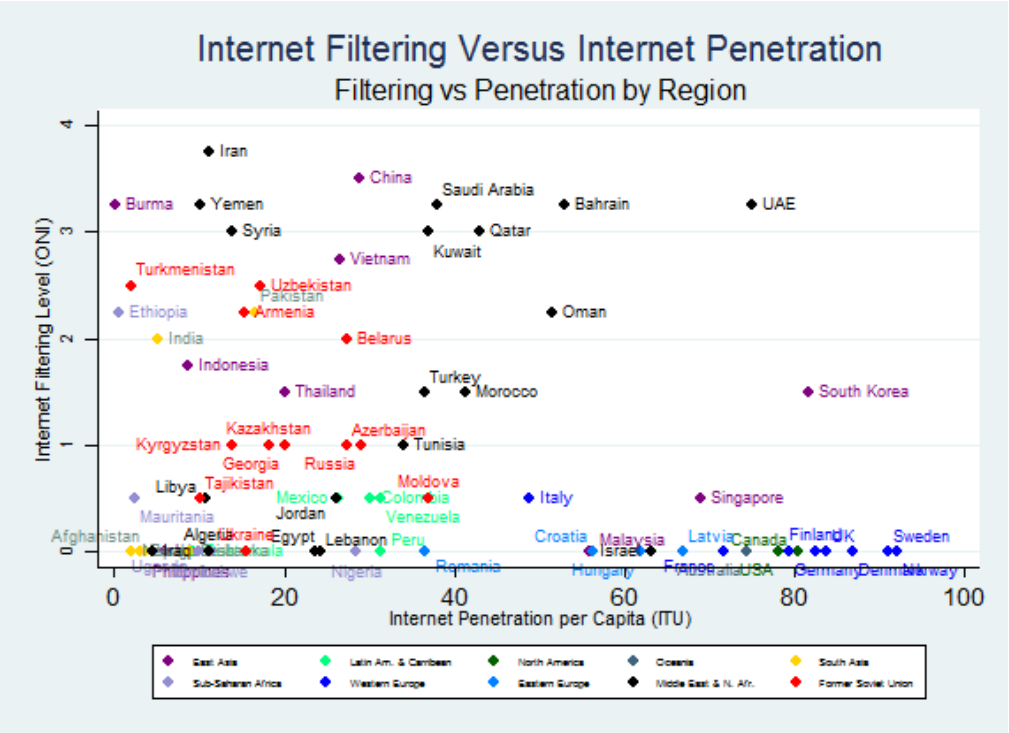


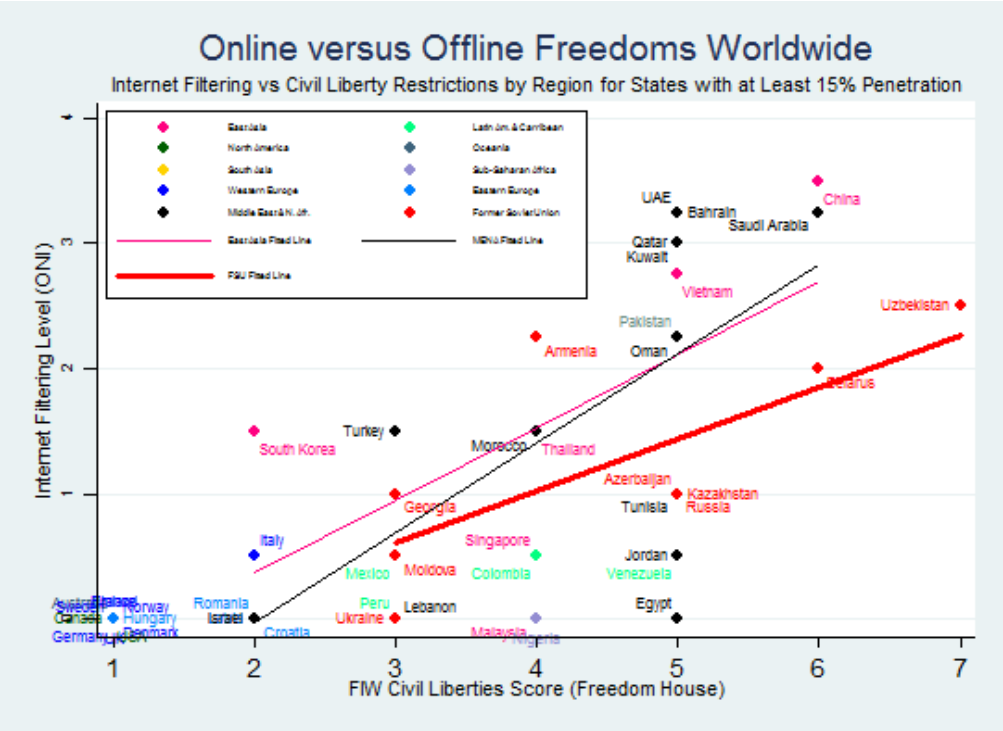
Table 5. OLS Regression
Models of Internet Filtering by Region for IPR>15%

Variable	Internet Filtering in Former Soviet Region	Internet Filtering in East Asia Region	Internet Filtering in MENA Region
Offline Civil Liberties Restriction	0.416*	0.580	0.713*
	(2.70)	(1.44)	(2.49)
Constant	-0.646	-0.792	-1.452
	(-0.88)	(-0.45)	(-1.10)
Adjusted R^2	0.4408	0.1763	0.3013
Observations	9	6	13

t statistics in parentheses
* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Figure 5 illustrates this relationship graphically, repeating the plot from Figure 1 above for Internet penetration rate (IPR) >15% and showing the three regional regression lines.

Figure 5:



These models are built on too few cases to prove definitive causally-significant regional disparities, especially if controlling for all possible causal variables; but they do further suggest some distinctive patterns across regions, providing support for *Hypothesis 4* from the previous section. While more longitudinal and process tracing analysis is needed to say for sure which of the diffusion mechanisms or other possible explanations for clustering might be at play here, it seems highly likely that regional exemplars and cultural norms have at least played some significant role, along with regimes learning from the apparent successes and failures of neighbors, and even direct transfer or emulation of particular restrictive technologies or laws. In addition to the possible influences of diffusion effects, particularly affecting states with restrictive neighbors and peers, states might also face different levels of coercion from Western democracies or international organizations to comply with less restrictive policies perceived as global "Internet Freedom" norms. To examine such disparate pressures in depth will require both an analysis of global patterns of "linkage" and "leverage" factors influencing likely pressure and vulnerability, and more detailed process tracing to understand when and how persuasive or coercive pressure on this particular issue is most likely to be

effectively applied.[10]

Analysis

While this investigation is far from sufficient to explain all dynamics of Internet policy adoption among nondemocratic states, it does provide some evidence in support of the typology and hypotheses introduced in the previous section. At least with regard to 1st generation approaches to restricting Internet content, we have seen that neither offline regime type nor Internet penetration level alone are sufficient to predict the restrictive policy choice. While in combination they appear to provide a somewhat fuller explanation for the more extreme democratic and authoritarian regime types, furthermore, they neither provide sufficient insight into the likely policy choices of hybrid regimes, nor do they account for more specific details of legal or technical approaches selected for Internet regulation. In addition to these key factors, domestic protest levels as well as regional norms and intra-regional diffusion appear to significantly influence regime policy choices. While longitudinal patterns indicate that regimes choose to adopt tighter restrictions when they face challenges from domestic Internet-enabled protest movements, regional policy clustering – clearly in part the effect of cross-regional similarities in regime type and cultural norms – most likely cannot be explained by domestic factors alone and is also indicative of some form of policy diffusion.

Hybrid regimes emerge as a particularly intriguing category to observe more closely as Internet penetration levels grow globally. Until recently, many such states have still had somewhat low penetration rates, but case examples suggest that as penetration rates grow these regimes face particularly tricky trade-offs, balancing their remaining democratic legitimacy at home and abroad against the potentially-existential risks of increasing online-offline "asymmetry" and emerging Internet-enabled protest movements. Where protest movements emerge and appear to threaten regime stability, in the absence of other countervailing pressures, it appears that such regimes sometimes choose to adopt much stricter Internet policies. At the extreme in such cases, as regimes face critical decisions of whether to open further or crack down once

[10] While such detailed analysis of coercion and persuasion effects is beyond the scope of this paper, it is worth noting that major ICT markets such as China's have often proven sufficiently attractive to Western IT companies that the desires of such companies to participate in the growing market has run at cross-purposes with and perhaps undercut pro-"Internet freedom" diplomacy. With lower levels of linkage to smaller states with less attractive ICT markets, however, Western powers might be less inclined to pay attention to Internet restrictions where they exist in such settings, thus putting less diplomatic pressure on states which might in fact be more vulnerable to pressure on this issue. If effective pressure is to be exerted, therefore, it seems paramount that Western IT companies and governments cooperate to insure some degree of consistency regarding their policies on the protection of Internet user rights. While corporate responsibility initiatives such as the Global Network Initiative (GNI) and civil society Internet freedom advocacy networks (groups such as the Electronic Frontier Foundation, EFF) have tried to stress the importance of thoughtful corporate policy, given the historic absence of effective coordination, it is unclear to what extent Western diplomacy on this issue has acted as a significant deterrent against growing global Internet restrictions.

Internet penetration reaches a certain critical level, regime type itself might even ultimately be influenced by Internet policy choices. I return to this issue in the concluding discussion of possible emerging global trends.

Future Research

The empirical research in this study constitutes a preliminary investigation into the hypothesized factors and processes affecting Internet policy choice; but more detailed research is clearly needed. This paper's empirical analysis has focused on global patterns of first generation (filtering and blocking) approaches to the restriction of Internet content. The cross-sectional ONI data I have used codes the levels of censorship, but it does not account for the technical mechanisms likely being utilized. Nor does it provide consistent measures over time at sufficiently regular intervals to track global patterns of longitudinal policy shift. A more thorough investigation must incorporate examination of technical mechanisms being used for censorship in different countries and more detailed analysis of the specific types of content being blocked.[11] It must also examine the implementation of key "next generation" Internet restrictions (such as repressive Internet laws, prevalent DDoS attacks, and various forms of surveillance) as well as cellular and other ICT network policies intended to restrict public use of the Internet and social media through the use of mobile devices.[12]

CONCLUSION: THE FUTURE OF INTERNET GOVERNANCE

In their prescient 2006 book, *Who Controls the Internet? Illusions of a Borderless World*, Columbia law professors Jack Goldsmith and Tim Wu argued that early cyber-utopians and globalization theorists alike had dramatically underestimated the control likely to be asserted by traditional territorial state governments

[11] For excellent case-study and small-n analysis of specific content censored and technical approaches utilized, see: King, Gary, Jennifer Pan, and Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression" (2013), and Gill, Philipa, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wisemean, "Characterizing Censorship of Web Content Worldwide: Another Look at the OpenNet Initiative Data" (2013).

[12] Sufficiently global data is not yet available on all of these policies to permit large-N analysis, and the available data has not been compiled into the sort of longitudinal and cross-sectional panel data that will most facilitate observation of trends such as policy diffusion. In addition to incorporating more thorough and consistent coding of Internet policy approaches, such a dataset should also incorporate measures of domestic protest levels (global data on which is increasingly available with the release of the GDELT and other event-based datasets), and other plausible economic and political explanatory factors. In addition to the simple regional coding used in this study, domestic value data (e.g. most prominent religion, or value survey results showing attitudes towards censorship) and state relational data (e.g. network relations with trading partners and political allies) could be incorporated, in order to better scrutinize the different factors possibly contributing to the development of observed regional clusters.

A dataset of the sort discussed will allow for more detailed analysis of factors influencing Internet policy choice and global patterns of policy diffusion over time. This more precise data will permit the refinement of the typological model and hypotheses developed above and possibly also the development of a heuristic formal model by which to understand the different policy approaches taken in response to the Internet "dictator's dilemma" by different types of non-democratic states – and the potential implications for longer-term global Internet policy norm trends.

over digital networks operating within their countries, suggesting the future of Internet governance was most likely to appear more balkanized and more like the regulation of other traditional forms of domestic state governance than most theorists of the day were yet willing to admit (Goldsmith and Wu, 2006). The evidence of such a move towards individual state control of domestic Internet access, content and use has clearly mounted dramatically in the past eight years, with increasingly significant variation in Internet regulation and levels of Internet freedom within different states. But the issue is far from resolved, and the appropriate global norms for Internet policy have become an issue of vehement contention.

As Internet penetration levels increase globally, the laissez-faire policies of the 1990s and 2000s are bound to be replaced by more regulation in *both* democratic and non-democratic states. As the Internet becomes an ever-more integrated part of the global infrastructure for commerce, media, provision of services, communication, association, and public discourse, it inevitably raises new challenges for governance, as states, international organizations, corporations, and citizens struggle to define the limits of "intellectual property," "online privacy," "libel," "hate speech," and many other legal and conceptual bounds which now take on new international as well as domestic significance. Though some greater forms of regulation are inevitable, however, the question remains what forms these new regulations will take. One need only think of the global protests over SOPA, PIPA, and ACTA, the British government's pressure on RIM to share encryption keys in the wake of the London Riots, the extra-legal pressures arguably applied to financial companies in order to shutdown WikiLeaks, the divisive debate over Google's policy regarding the "Innocence of Muslims" video, or the ongoing scandal in the US over NSA surveillance revelations, to realize that the contestation over new policies and norms for the regulation of the Internet is not just a problem of contestation between democratic and non-democratic states.

The outcome of this contestation is of particular importance to the future of today's non-democratic hybrid regime states however. While the strictest authoritarian states are most likely to respond to increasing Internet penetration with immediate efforts to restrict the technology's potential to influence politics, less closed regimes have not, in the past, appeared to respond as immediately or consistently in the implementation of restrictive measures. As Internet penetration grows within these states, it offers a real potential change in openness and increases the prospects for political transparency and accountability that could bring about gradual democratization, improving channels of communication and participation between government and society. This could go the other way, however. Witnessing the supposed repercussions of

growing Internet penetration in events such as the Arab Spring revolutions and conflagrations and the riots in reaction to the Innocence of Muslims video, many non-democratic regimes might deem the greater information-sharing and protest organizing potential resulting from unrestricted Internet use to be of more potential danger than good, and might seek to take prophylactic measures to protect against such destabilizing influences.

Growing Internet penetration in authoritarian and hybrid regime settings has great potential to influence the nature and dynamism of protest movements in such settings, and the balance of power between the state and society in authoritarian settings more generally. The nature of this influence is contingent, however, and will depend both on the agency and inventiveness of protest movements themselves, and on the nature of the policies chosen by the regimes to control the new technology's use. Given the significant impact that Internet policies can have, more research is clearly needed to examine the reasons states choose the particular policies that they do. In the aftermath of the Arab Spring, and especially following the blow to US Internet governance leadership credibility following the NSA PRISM disclosures, many states might be tempted to react against the perceived risk of Internet-enabled protest movements leading to political instability. It is therefore imminently important at this time to gain greater understanding of what factors might in fact serve to best promote the long-term global spread of less restricted models of Internet governance.

APPENDIXES

APPENDIX I: Domestic and International Causal Factors

Domestic Factors

Perhaps the most obviously relevant domestic state-level characteristic is a state's overall "regime type." *All other things being equal, we might expect a given regime to adopt Internet policies most commensurate with its approach to the management of societal pressures in offline settings. Thus, we would expect to see* ***online and offline policy-linkage****, with greater freedom of expression and association offline correlating with less restrictive Internet policies, and with greater offline repression and restriction on free association and free expression also correlating with more restrictive Internet policies.* While this factor alone can explain many cases, this fails to account for instances of "policy asymmetry" where authoritarian regimes do not restrict their Internet. It also does not always explain the particular choice of approach to Internet regulation that a state might adopt – what materials are and are not filtered, and which of the "next generation controls" are employed. Many modern non-democratic regimes – especially "hybrid" or "competitive authoritarian" regimes – do not apply all-or-nothing approaches to control over society, but rather adopt more nuanced strategic approaches. This can be seen clearly in the diversity of approaches adopted to Internet regulation.

With regard, in particular, to Internet content or access restrictions, all other things being equal, we might expect the most extreme closed authoritarian regimes (e.g. North Korea, Turkmenistan, Saudi Arabia, Iran, China) to most strictly and blatantly restrict access to the Internet or tightly censor domestic online content. These regimes rely on keeping a tight lid on public discourse and civic engagement, and have little legitimacy at stake in maintaining the appearance of a "free Internet." The most open democratic regimes (e.g. US, EU members), on the other hand, are least likely to place restrictions on Internet access or content, with rare exceptions regarding to the blocking or restricting of pornographic or copyright-infringing online content. Between these extremes, however, amongst "hybrid regimes" (e.g. Turkey, Lebanon, Georgia, Kuwait) that share some characteristics of both authoritarian and democratic regime types, we see a much broader range of policy choices – even amongst some of the most restrictive regimes within this category (e.g. Belarus, Venezuela, Russia, Kazakhstan) – with some regimes adopting the more blatantly restrictive

approaches, others permitting completely unrestricted access and content, and others adopting a wide range of less-obvious partial restrictions or pressures on content and use. All other things being equal, these regimes are probably more likely to consider reputation costs in adopting the most obvious blunt restrictions that would be broadly considered violations of "Internet freedom."

All other things being equal, a regime's Internet policy is likely to be responsive to concerns over its ability to maintain domestic political control and stability. *Regimes that see their domestic stability as threatened – either generally by domestic tensions and protest or specifically as a result of Internet use – are more likely to adopt restrictive measures to limit the role of the Internet in spreading critical discourse or mobilizing protest.* A ***regime's perception of the threat of protest movements*** will be in part based on observations of the experiences such as the Colored Revolutions and the Arab Spring in neighboring or similar states. They also will be based on the regime's evaluation of its own domestic hold on power, which will be based, for example, on: its level of domestic support and perceived legitimacy; recent violence, uprisings, or separatist movements; level of coercion needed to maintain control; where relevant, the stability and reach of a patronage system; the economic situation and grievances based in poverty, inequality, or recent downturns; and, probably most importantly, the prominence, mobilization levels, and goals of recent or ongoing protest and opposition movements at home. When faced with a present real threat of mass protest mobilization, regimes are more likely to take significant steps to limit the Internet's use in anti-regime discourse and mobilization.

Even when concerned over stability, regimes don't always focus on the Internet as a primary target for control. Control over or repression of traditional forms of "offline" media (e.g. television and print media) and civic organizing (e.g. civil society, public protests events, etc.) might be increased while little attention is paid to the Internet. A regime's evaluation of the ***particular threat posed by the Internet*** *per se* will likely depend on some combination of: the relative novelty in that society of the forces of information sharing, free speech and association that the unrestricted Internet releases (i.e. the degree of online-offline policy "asymmetry"); how much the regime stands to lose from a more complete mutual preference revelation among the population (i.e. level of shared awareness of grievance levels); the degree of Internet penetration and usage frequency in the society and how rapidly it has been growing; the extent to which protest movements are observed to be growing in strength as a result of increasing Internet usage and, relatedly, the online presence of anti-regime political groups and rhetoric; possible legitimate concern about religious or

nationalist extremist presence online; and the perception of the Internet explicitly posing a revolutionary risks based on recent global or regional experiences such as the Arab Spring or Iranian Green Movement in which Internet usage was prominently publicized as a key causal ingredient (whether or not correctly).

These factors, contributing to the threats regimes expect from growing Internet use, must be weighed against the perceived benefits of Internet development and the costs of restricting Internet use. Relevant here will be the ***expected economic benefits of ICT sector development***, the ***expected economic costs of Internet restriction*** (or potential benefits of some types of restrictions), and the expected impact of Internet restrictions on domestic regime legitimacy and support. The first two (economic) factors will be influenced by: the state's level of economic development, the presence of natural resource wealth or other insulating income sources, Internet- and ICT-reliant economic linkages and interdependencies, and the importance or prominence of the ICT sector itself. The country's population and level of Internet penetration will also be important factors here, influencing the potential size of the market for Internet-based technologies, its attractiveness to foreign investment, and the potential for the development of large-scale domestic Internet services to replace foreign competitors.

Overall, *all other things being equal, we might expect large and more economically developed countries to face less of an economic burden in restricting their Internet, both because they are less likely to lose their place in the world economy as a result, and because they can afford and are more equipped to restrict the Internet in nuanced ways that are not as likely to cripple ICT businesses or businesses that rely on Internet use*. While larger and more developed countries (with higher Internet penetration and more potential for economic growth in their ICT sectors) might face greater potential losses if they were to lose their access to foreign direct investment, restrict ICT sector growth, or become less integrated in the global economy, some evidence suggests that it is precisely these states that are at the least risk of such adverse effects. Drawn to compete in these large and powerful markets, multinational ICT companies are less likely to forsake these countries unless explicitly forced to do so (i.e. through government sanctions or reputational costs). Also, with the capacity and human capital to develop domestically-based economies of scale, these countries might stand to gain economically from developing their own platforms for widespread domestic use in place of foreign competitors (e.g. Weibo's use in place of Twitter in China, VKontakte and Yandex in Russia in place of Facebook and Google, etc.), so their ICT sectors might even benefit from closing parts of the market to foreign competitors (e.g. through blocking foreign social media platforms or other Internet resources).

Also of importance here is the actual cost of implementing various possible Internet restrictions and the capacity of the state to do so. Not all states have the economic or technical wherewithal to build their own "Great Firewalls," so lack of state capacity, wealth, or technical sophistication could certainly contribute to the ultimate choice of particular less-costly or labor-intensive restrictive measures. More developed, larger countries are more likely to have the human capital and economic capacity to invest in nuanced technologies to restrict particular Internet resources without effectively crippling all industries that rely on the Internet. This depends, for example, on a country's ability to afford and consistently utilize customized filtering systems using more advanced technologies such as "deep packet inspection" (DPI) that block specific pages rather than whole platforms or IP addresses. While many smaller, poorer or less technologically sophisticated countries purchase mass-produced filtering devices with ready-made block-lists, or use clunky techniques that result in widespread "collateral blocking" (of sites or pages other than those targeted for blocking), the most advanced systems (such as China's "Great Firewall") involve much more sophisticated, costly, and surgically precise approaches.

The expected ***legitimacy costs of Internet restrictions*** will in turn depend upon societal norms, availability of "legitimate" grounds for the chosen Internet restrictions (as perceived by the domestic society), and the portion of the population that would be directly impacted by new restrictions (i.e. whether this amounts to the withdrawal of an already widely entrenched privilege or if it only impacts an elite or idealistic sliver of the population). Some societies might be more accepting of certain types of restrictions (such as restrictions on pornographic content in conservative cultural settings such as the GCC states), especially if these restrictions are transparently applied. Other populations, for historical reasons, might have particularly negative reactions to any hint of "censorship" even of forms widely accepted in many older Western democracies. (Witness the large protests in Poland in 2012 against new online copyright protections sought in the Anti-Counterfeiting Trade Agreement (ACTA).) The presence of what are perceived as real risks – such as online extremist groups and previous national experiences with terrorism – can clearly also lend legitimacy to certain forms of restriction, as people are willing to make certain concessions, permitting greater surveillance or content restriction for the sake of security. Overall, *we can expect to see the levels and forms of Internet restrictions adopted by otherwise similar states influenced and constrained by perceived domestic legitimacy or illegitimacy of Internet restrictions, a sense that in turn is based particularly on the strength of*

societal values regarding civil liberties (sometimes opposed to more conservative or religious values) and the presence or absence of serious domestic security concerns.

International Pressures

The international factors can be similarly broken down. The degree of ***expected international pressure and reputation loss*** associated with restricting the Internet will depend in turn on: the clarity of international norms (particularly democratic norms) concerning Internet policy and the notion of "Internet Freedom;" the presence or absence of any legal convention to which the state is party and which its policy would transgress; the level of "linkage" between this state's domestic society, economy, and political institutions and those of its Western democratic counterparts, influencing in turn the levels of international attention to norm violations in the given state; and the extent to which the state's international reputation rests on its fulfillment of democratic norms.

Following Levitsky and Way (2007, 2010), linkage factors can be further broken down to include: geographic proximity to major Western democracies; the society's level of cultural proximity and social connection to the West; information flows; the density of network connections between domestic civil society groups and transnational activism networks; the degree of economic interdependence with the West; and the level of intergovernmental linkage and cooperation with the West.

International reputational costs will likely depend also upon the extent to which a state has based its international legitimacy and standing on membership in the community of democratic states. For some hybrid regime states where the visible extremes of repression are carefully avoided, this could influence choice of Internet policy, prompting them to avoid the most obvious and draconian measures unless they are ready to also give up the benefits of their reputations as (at least partial) democracies. Also significant here will be the availability of "legitimate excuses." Just as these factors influence domestic legitimacy, they also play a role in international community perceptions. States that can argue that they censor their Internet to meet "cultural norms" or protect their country and the international community from "extremism" (religious, nationalist, etc.) might face less reputational cost and greater international community leniency, especially if the norms or threats they point to seem credible. Blocking or filtering child pornography or copyrighted materials, for example, would be widely accepted as legitimate norms by many democratic states, and the censoring of pornography or certain extremist materials might be seen as acceptable by some as well – certainly more so than the blocking of materials on LGBT or minority rights or on sensitive political topics or oppositional

political groups. Further relevant factors to this end might be: a country's dominant religion(s); "War on Terror" collaboration; existence of known extremist groups (religious extremist or xenophobic/neo-Nazi) within the country or past history of terrorist attacks within or originating from the country's territory; and a clear web-presence of extremist groups within the country.

Overall, *states that are heavily linked to the Western democratic states through economic and social transnational or intergovernmental linkages and that have based their international reputation in part on their status as democracies (even if debated) are most likely to be subject to significant international community pressure or risk losing reputational benefits as a result of obvious Internet restrictions (though less so if these restrictions can be justified in accordance with other accepted values such as security against terrorism)*.

The existence of such pressure does not necessarily influence regime Internet policy choice, however. *The **regime's vulnerability to international pressure** will in turn depend on factors contributing to Western "leverage" by influencing a state's bargaining power, ability to avoid punishment, and the actual potential impact of such punishment* (Levitsky and Way 2007, 2010). These factors include: the state's market size and economic strength; other economic or strategic Western interests at stake in the given state; and the existence or absence of close ties with other powerful "black knight" ally states that can stand up for and protect a state from international pressure and that will not punish the state for restricting Internet use.

As with normative pressures on many issues, states that play key strategic roles vis-à-vis the interests of powerful Western democracies might have their own leveraging power to avoid international community pressures. Partners in the "war on terror" (e.g. Pakistan, Afghanistan) or in withdrawal of Western troops (e.g. Kazakhstan), for example, might be less likely to face sanctions or softer pressures regarding a (secondary) issue such as "Internet freedom" which is clearly not as vital to the specific national interests of the Western states involved, even if it is seen as a valuable norm. Likewise, states that are closely connected with such powerful states might be protected from international community pressure by their leverage (e.g. Russia's role vis-à-vis Belarus or Kazakhstan).

As addressed above regarding economic costs and benefits, the state's capacity to develop its ICT sector in the absence of foreign investment as well as the relative attractiveness of its market to foreign ICT sector investment will play important roles in determining both the potential impact and actual likelihood of a withdrawal of Western companies and investors from the state's ICT market. While large states like China or

Russia might be able to develop home-grown web-platforms and services in lieu of their Western equivalents (and might even profit by doing so), it is much harder for small states with small tech sectors and limited numbers of Internet users to develop vibrant national alternatives to the globally available platforms and services. Likewise, as has often been pointed out, many Western IT companies find China is too large a market to stay out of on the basis of reputational or normative concerns, even if they would stay out of less lucrative markets for similar reasons.

Overall, while states will face some international pressure to conform with existing norms concerning "Internet Freedom," the ability of the democratic community to exert any significant coercive pressure regarding this issue alone is likely to be somewhat limited, especially when concerning states where other strategic concerns of the norm-enforcing states might take a higher priority. The more contested the definition of this norm becomes, even amongst Western democratic allies (e.g. the debate around the appropriate balance between security and surveillance brought to the fore by the Snowden disclosures), the harder its enforcement is likely to prove (Kerr 2013). While the choices of more closed authoritarian regimes are most likely to be influenced by the economic burdens of foreign ICT companies being unwilling to participate in their markets (when and if this happens), the more frequently observed *"soft" international normative pressure (e.g. rhetorical shaming, etc.) is most likely to influence the Internet policy choices of hybrid regimes and partial democracies, as these states might face other negative repercussions from legitimacy loss if they become known as states that censor the Internet*.

Cooperation and Diffusion Dynamics

Insofar as the state-level factors so far described result in Internet policy similarities and clustering across states, these could be grouped as "similar responses to similar conditions" – whether domestic or international (Simmons and Elkins 2005). In addition to these factors influencing the domestic costs and benefits of Internet restrictions and the international costs and coercion an individual state is likely to face as a result of restricting Internet use, *states also might collaborate to develop policy frameworks, or they might be independently influenced by the decisions and outcomes they witness in other states. These forms of "complex interdependencies" appear to be playing ever more significant causal roles in Internet policy decisions today*, as international norms in this area become more vehemently contested, advanced restrictive technologies become more widely available, events such as the "Arab Spring" and "London Riots" raise attention to

potential "risks" of ICT-enabled protest or crime, and increasing Internet penetration rates globally raise the stakes.

Policy cooperation *can take the form of treaties or implicit agreements that might either endorse unfettered Internet access and content or support some level of restrictions.* Like-minded regimes can collaborate in international organization settings, seeking to alter global rules for Internet regulation. This dynamic was underscored in December 2012, by Russia's submission of a proposal backed by China, Saudi Arabia, Algeria, Sudan, and the UAE, at the World Conference on International Telecommunications (WCIT-12) in Dubai, that sought to change fundamentally the rules for global Internet governance.[13] Cooperation can further be mediated by consensual technology transfer whereby technologies developed or licensed in one state for building certain controls over Internet and ICT infrastructure or for filtering Internet content are knowingly transferred to another state. Factors influencing the likelihood of such technology transfer might be the existence of close relationships with other governments facing similar risks and benefits associated with Internet restriction, particularly if those states also are more developed, have served as "black knight" protectors, or have themselves already begun the introduction of new restrictions. Rebecca MacKinnon has noted, for example, how the Sunnyvale-based network security company Narus, which has also sold its products to Pakistan and Saudi Arabia, signed a deal in 2005 with the Egyptian company Giza Systems "to license its [deep packet inspection (DPI)] technology across the Middle East and North Africa" (MacKinnon 2012).

In addition to deliberate policy cooperation amongst states, *we can expect* ***uncoordinated diffusion processes*** *also to be playing a significant role in Internet policy selection* (Simmons and Elkins 2004, 2005; Gilardi 2011; Ambrosio 2010). *First, the policy choices of other states might "alter the conditions of adoption" (i.e. the associated costs and pressures) for a given regime*. If a large enough group adopts restrictive Internet policies, for example, this can provide group cover and hence limit the negative attention, pressure, and reputational costs associated with a state's decision to adopt new Internet restrictions. Policy makers might also come to consider the approach adopted by similar states to be normatively correct and appropriate – for example if they genuinely worry about the consequences for their society's values and

[13] The bloc's leaked proposal would have revised the legally-binding 178-country International Telecommunication Regulations (ITR) treaty, to increase the authority of individual states to regulate and block materials from their domestic Internet, while transferring the US-partisan ICANN's long-contested authority to the UN's International Telecommunications Union (ITU) – an agency in which all states would have equal votes.

culture of allowing unfiltered online pornography or other materials contrary to perceived national values. Thus the adoption of such policies by states with similar values might in fact lead to emulation based on a "logic of appropriateness."

The adoption of a specific type of Internet restriction by a growing number might also alter the perceived value of that approach because of a shared reliance on the same technical designs – whether of software or infrastructure. Here (as in the Narus example) the presence of companies assisting multiple countries in the building of Internet infrastructure controls or the development of filtering software might contribute further to the perception of a "support group" increasing the benefits associated with a particular technological solution. Rebecca MacKinnon, Jillian York, and others have further shown that many Western security companies have specifically targeted marketing efforts at nondemocratic states in the Middle East and elsewhere, providing them with "off-the-shelf" technological solutions for Internet blocking or surveillance – even including "pre-established censorship lists" with "tens of millions of websites in dozens of designated categories" offered "in anticipation of client's needs" (MacKinnon 2012).

Competition dynamics between states can also influence Internet policy diffusion in several ways. For countries seeking to attract to their market foreign technology companies or other companies reliant on Internet use, the decision not to restrict the Internet by other states that are direct competitors for foreign investment could discourage such restrictions by the state in question, increasing the associated economic costs. (All other things being equal, companies will likely choose to invest more heavily in the country in which they can do business most freely, with access to the unrestricted Internet or, in the case of technology companies, without having to worry about censoring content or surveillance.) The adoption of restrictions by competitors, on the other hand, could reduce the costs of Internet-restricting policies for the given country. (And companies will not always pass up opportunities to do business in restrictive countries – particularly in countries with large and lucrative markets.)

Even where the costs and benefits of policies are not altered by the policy adoption choices of others, *policy diffusion might also follow from regimes' observations of and learning from the policy choices of other states and the apparent consequences of these choices*. Information cascades are particularly likely to develop among countries that see themselves as facing similar risks and challenges from growing Internet penetration and societal protest movements. This is particularly likely across unfree or only partly free states in which the Internet is likely to greatly expand the capacity for discussion of and protest organizing around

shared grievances. Thus authoritarian or hybrid regime states are likely to particularly observe and learn from the Internet policies of other non-democratic states. If a large portion of other such states are seen to be adopting a particular approach to Internet regulation, then this might be assumed to be a relatively safe approach or even necessary to insuring regime control. Some of the rapid movement towards increasing Internet filtering in recent years might be explained by such an information cascade.

Available information about cases of success or failure of given policies will also be influential. While highly visible instances of "failure" (e.g. possibly some of the Internet policies in Arab authoritarian states prior to the Arab Spring) can reverse existing cascades, leading many states to question the worth of previously common approaches, prominent examples of apparently "successful models" – especially amongst countries with which a state interacts a great bit – are likely to serve as exemplars. Examples here might include Russia's "next generation" approaches to Internet management, China's "Great Firewall," or Saudi Arabia's conservative value-based filtering. Learning-based diffusion is particularly likely to occur across reference groups. As stressed by Simmons and Elkins, this might be among geographically or culturally close countries (same geographic region, same language, religion, colonial origins). I would add that it is also likely to occur across countries of similar regime types.

While the overall influence of cooperation and diffusion effects on Internet policy choice outcomes will be complex, it appears likely that these processes will contribute to certain clustering dynamics in policy choice – both in terms of general patterns of greater Internet restriction or freedom, and regarding the specific mechanisms and policies of restriction being utilized. All other things being equal, similar approaches and restrictive technologies are likely to appear across states of similar regime type, states that are economic competitors, states that share certain cultural values (e.g. concerning civil liberties protections or conservative religious beliefs), allied states or states sharing a "black knight" protector, or states that are geographic neighbors. *Considering the nature of regional neighborhoods, this likely results most frequently in policy diffusion across similar regime type states within geographic regions – resulting in particular regional approaches to Internet control. But it can at times also lead to global cross-regional emulation of particularly visible models such as China's "Great Firewall."*

APPENDIX II: Expanded Typological Model

Table A1, below, shows an expanded typology taking account of a regime's "International Pressure Vulnerability" and whether it has "Restrictive Peers / Neighbors" in addition to the three primary domestic characteristics just discussed. The far right column predicts the likelihood for the adoption of restrictive Internet policies for each type of regime. Lines separate each of the eight domestic-characteristic-based typological categories from above, making it evident how different international relationships and forces might combine to alter the likelihood of adoption of restrictive Internet policies, all other things being equal.[14] This typology is only a rough heuristic, but it gives some sense of how changes in international and regional Internet policy norms are likely to have effects on the decisions of individual states.

Table A1. Internet Restriction Levels Typology: Domestic and International Determinants

Regime Type	Internet Penetration	Recent Protest Level	Restrictive Peers / Neighbors?	International Pressure Vulnerability	Restrictive Policy Likelihood
Authoritarian	H	H	Y	L	*very high*
Authoritarian	H	H	Y	H	*high*
Authoritarian	H	H	N	L	*high*
Authoritarian	H	H	N	H	*medium*
Authoritarian	H	L	Y	L	*high*
Authoritarian	H	L	Y	H	*high*
Authoritarian	H	L	N	L	*medium*
Authoritarian	H	L	N	H	*medium*
Authoritarian	L	H	Y	L	*medium*
Authoritarian	L	H	Y	H	*medium*
Authoritarian	L	H	N	L	*low*
Authoritarian	L	H	N	H	*low*

[14] Here it is assumed: that high Internet penetration has a more pronounced effect on closed authoritarian regimes, though making both regime types more likely to adopt restrictive policies; that a high recent protest level will make all types of regimes more likely to restrict, but that this effect will be magnified in regimes with high Internet penetration; that hybrid regimes with high international pressure vulnerability will be more strongly influenced away from restrictive measures than the most vulnerable authoritarian regimes; and that, all other things being equal, states are likely to be influenced by neighboring or peer-country regimes, so that those for which a high proportion of their closest relations have adopted restrictive Internet policies are themselves more likely to do likewise.

Authoritarian	L	L	Y	L	*medium*
Authoritarian	L	L	Y	H	*low*
Authoritarian	L	L	N	L	*low*
Authoritarian	L	L	N	H	*very low*
Hybrid	H	H	Y	L	*medium*
Hybrid	H	H	Y	H	*low*
Hybrid	H	H	N	L	*low*
Hybrid	H	H	N	H	*very low*
Hybrid	H	L	Y	L	*medium*
Hybrid	H	L	Y	H	*low*
Hybrid	H	L	N	L	*low*
Hybrid	H	L	N	H	*very low*
Hybrid	L	H	Y	L	*low*
Hybrid	L	H	Y	H	*very low*
Hybrid	L	H	N	L	*very low*
Hybrid	L	H	N	H	*very low*
Hybrid	L	L	Y	L	*low*
Hybrid	L	L	Y	H	*very low*
Hybrid	L	L	N	L	*very low*
Hybrid	L	L	N	H	*very low*

The table shows an expanded typology, incorporating both domestic and international factors to predict state Internet restriction levels based on regime type, Internet penetration level, recent domestic protest level, a state's connection to restrictive peers or neighbors, and the state's likely exposure and vulnerability to international pressure opposing Internet restrictions. The final column shows the relatively likelihood of a state having or adopting restrictive approaches to Internet regulation in the different regime contexts. Lines separate regimes types based on domestic characteristics, making clear how otherwise similar regimes might be expected to adopt different degrees or forms of restriction depending on their international position and relations.

REFERENCES

Aron, Leon. "Nyetizdat: How the Internet Is Building Civil Society in Russia." *Russian Outlook*. American Enterprise Institute for Public Policy Research. Spring 2011.

Balzer, Harley. "Managed Pluralism: Vladimir Putin's Emerging Regime." *Post-Soviet Affairs* 19, No. 3 (2003): 189-227.

BBC News Asia. "Kazakh Zhanaozen oil unrest spreads to regional capital." December 18, 2011. http://www.bbc.co.uk/news/world-asia-16235282.

BBC News Technology. "Russia internet blacklist law takes effect." October 31, 2012. http://www.bbc.co.uk/news/technology-20096274.

Beilock, Richard and Daniela Dimitrova. "An Exploratory Model of Inter-country Internet Diffusion." *Telecommunications Policy* 27, April/May 2003: 237-252.

Bennett, Andrew and Alexander L. George. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press, 2005.

Bunce, Valerie, Michael McFaul, and Kathryn Stoner-Weiss, Editors. *Democracy and Authoritarianism in the Postcommunist World*. Cambridge: Cambridge University Press, 2009.

Crete-Nishihata, Masashi, Ronald J. Deibert, and Adam Senft. "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls." *IEEE Internet Computing*, vol. 17, no. 3 (May-June 2013): 34-41.

Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain (Editors) Access Contested: Security, Identity and Resistance in Asian cyberspace (Cambridge: MIT Press, 2011).

Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain (Editors) Access Controlled: The shaping of power, rights, and rule in cyberspace (Cambridge: MIT Press, 2010).

Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski and Jonathan Zittrain (Editors) Access Denied: The Practice and Policy of Global Internet Filtering (Cambridge: MIT Press, 2008).

Deibert, Ronald, and Rafal Rohozinski, "Liberation vs Control: The Future of Cyberspace," *Journal of Democracy*, Volume 21, Number 4, October 2010: 43-57.

Diamond, Larry. "Liberation technology." *Journal of Democracy*, 21, No. 3 (July 2010): 69-83.

Drezner, Daniel W. "Weighing the Scales: The Internet's Effect On State-Society Relations." *Brown Journal of World Affairs*. Vol. 16, No. 2 (Spring/Summer 2010): 31-44.

Earl, Jennifer and Katrina Kimport. *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: The MIT Press, 2011.

Elder, Miriam. "Azerbaijani police break up opposition rally in runup to Eurovision." Guardian. May 24, 2012. http://www.guardian.co.uk/world/2012/may/24/azerbaijan-police-break-opposition-rally-eurovision.

Elder, Miriam. "Censorship row over Russian internet blacklist." Guardian. November 12, 2012. http://www.guardian.co.uk/world/2012/nov/12/censorship-row-russian-internet-blacklist.

Elkins, Zachary, and Beth Simmons, "On Waves, Clusters, and Diffusion: A Conceptual Framework," ANNALS, AAPSS, 598, March 2005.

Etling, Bruce, Karina Alexanyan, John Kelly, Rob Faris, John Palfrey, and Urs Gasser. "Public Discourse in the Russian Blogosphere: Mapping RuNet Politics and Mobilization." Berkman Center for Internet and Society. October 18, 2010.

Etling, Bruce, Robert Faris and John Palfrey. "Political Change in the Digital Age: The Fragility and Promise of Online Organizing," *SAIS Review*, Vol. 30, No. 2, December, 2010: 37-49.

Evans, Alfred B., Jr., Laura A. Henry, and Lisa McIntosh Sundstrom, Editors. *Russian Civil Society: A Critical Assessment*. Armonk, NY: M.E.Sharpe, 2006.

Farrell, Henry. "The Internet's Consequences for Politics." *Crooked Timber* Blog. Sept 13, 2011.

Finnemore, Martha, and Kathryn Sikkink, "International Norms and Political Change." *International Organization* 52, No. 4 (1998): 887-917.

Fitzpatrick, Catherine A. "Uzbekistan: Internet Sites Blocked." Eurasianet.org. August 10, 2011.

Freedom House. "Annual Survey of Freedom House Country Scores, 1972-73 to 2011-2012." Reports and data available online at: <http://www.freedomhouse.org>.

Freedom House. *Freedom in the World, 2012*. Washington, DC: Freedom House, 2012.

Freedom House. *Freedom on the Net, 2011*. Washington, DC: Freedom House, 2011.

Freedom House. *Freedom on the Net, 2012*. Washington, DC: Freedom House, 2012.
Freedom House. *Freedom of the Press, 2012*. Washington, DC: Freedom House, 2012.
Garrett, Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICT's." *Information, Communication & Society*. 9:2 (April 2006): 202-224.
Georgetown University. "Weighing the Limitations Against the Added-Value of Social Media as a Tool for Political Change." *Democracy & Society*. Vol. 8, Is. 2, Summer 2011.
Gilardi, Fabrizio. "Transnational diffusion: Norms, ideas, and policies," *Handbook of International Relations*, Walter Carlsnaes, Thomas Risse, Beth Simmons (eds), SAGE Publications, 2012.
Gill, Philipa, Masashi Crete-Nishihata, Jakub Dalek, Sharon Goldberg, Adam Senft, and Greg Wisemean. "Characterizing Censorship of Web Content Worldwid: Another Look at the OpenNet Initiative Data." Published online through Stony Brook University, 2013. Available at: http://www.cs.stonybrook.edu/~phillipa/papers/ONIAnaly.html.
Gladwell, Malcolm. "Small Change: Why the revolution will not be tweeted." *The New Yorker*. October 4, 2010.
Gladwell, Malcolm and Clay Shirky. "From Innovation to Revolution: Do Social Media Make Protests Possible?" *Foreign Affairs*. March/April 2011.
Goldsmith, Jack and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. New York, NY: Oxford University Press, 2006.
Goodwin, Jeff and James M. Jasper. *The Social Movements Reader: Cases and Concepts*. Malden, MA: Blackwell Publishing, 2003.
Görtz, Birgit, Galina Petrovskaya, and Vladimir Dorokhov. "Internet revolutionaries lead protests in Belarus." *Deutsche Welle*. July 20, 2011.
Grigoryan, Marianna. "Armenia: Yerevan Opposition Protest Draws Large Crowd." Eurasianet.org. March 1, 2011. http://www.eurasianet.org/node/62983.
Guidry, John A., Michael D. Kennedy, and Mayer N. Zald, Editors. *Globalizations and Social Movements: Culture, Power, and the Transnational Public Sphere*. Ann Arbor, MI: The University of Michigan Press, 2000.
Heinze, Torben. "Mechanism-Based Thinking on Policy Diffusion: A Review of Current Approaches in Political Science," *KFG Working Paper Series*, No. 34, December 2011, Kolleg-Forschergruppe (KFG) "The Transformative Power of Europe", Freie Universitat Berlin.
Howard, Philip N. "How digital media enabled the protests in Tunisia and Egypt." Guest Contributor to *The Great Debate* (Blog). January 28, 2011.
Howard, Philip N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press, 2010.
Howard, Philip N., Agarwal, Sheetal & Hussain, Muzammil, When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media (August 9, 2011).
International Partnership for Human Rights. "Central Asia: Censorship and Control of the Internet and Other New Media," Briefing paper. November 2011.
International Telecommunications Union (ITU). Percentage Internet Usage Data, 2001-2011. ICT Statistics Database. Available online at: <http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx#>. Accessed November 2012.
Katzenstein, Peter J., Editor. *The Culture of National Security: Norms and Identity in World Politics*. New York: Columbia University Press, 1996.
Keck, Margaret E. and Kathryn Sikkink. *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca, NY: Cornell University Press, 1998.
Kendzior, Sarah. "Digital distrust: Uzbek cynicism and solidarity in the Internet Age." *American Ethnologist*, Volume 38, Issue 3 (August 2011): 559-575.
Kerr, Jaclyn. "Authoritarian Management of Cyber-Society in Post-Soviet States. Internet Penetration, Policies and New Protest Movements" Studies in Public Policy No. 503 (July 2013). Available online at: http://www.cspp.strath.ac.uk/view_item.php?id=503, or http://www.academia.edu/4128572/AUTHORITARIAN_MANAGEMENT_OF_CYBER-SOCIETY_IN_POST-SOVIET_STATES._Internet_Penetration_Policies_and_New_Protest_Movements.
Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink, Editors. *Restructuring World Politics: Transnational Social Movements, Networks, and Norms*. Minneapolis, MN: University of Minnesota Press, 2002.
King, Gary, Jennifer Pan, and Margaret E. Roberts. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review* (May 2013): 1-18.

Konieczny, Piotr. "Book review: Earl, Jennifer & Kimport, Katrina. *Digitally Enabled Social Change*. MIT Press: Cambridge, Mass." *Interface: a journal for and about social movements*, Volume 3 (2): 459-477 (November 2011).

Kraidy, Marwan M. *Reality Television and Arab Politics: Contention in Public Life*. New York, NY: Cambridge University Press, 2010.

Krebs, Ronald R. and Patrick Thaddeus Jackson. "Twisting Tongues and Twisting Arms: The Power of Political Rhetoric." *European Journal of International Relations* 13, No. 1 (2007): 35-66.

Kuran, Timur. *Private Truths, Public Lies: The Social Consequences of Preference Falsification*. Cambridge, MA: Harvard University Press, 1997.

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York, NY: Basic Books, 2000.

Levitsky, Steven and Lucan Way. *Competitive Authoritarianism: Hybrid Regimes After the Cold War*. New York, NY: Cambridge University Press, 2010.

Lieberman, Evan S. "Nested Analysis as a Mixed-Method Strategy for Cross-National Research." *American Political Science Review* 99, No. 3: 435-452.

Lillis, Joanna. "Kazakhstan: Activists Occupy Almaty Street with Zhanaozen Photos." *Eurasianet.org: Inside the Cocoon, Central Asia Today*. May 15, 2012. http://www.eurasianet.org/node/65403

Lynch, Marc. "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State." *Perspectives on Politics: Reflections*. June 2011.

MacKinnon, Rebecca. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York, NY: Basic Books, 2012.

McAdam, Doug, Sidney Tarrow, and Charles Tilly. *Dynamics of Contention*. Cambridge, UK: Cambridge University Press, 2001.

McGlinchey, Eric. "Transitions 2.0: The Internet, Political Culture and Autocracy in Central Asia," Paper delivered at APSA 2009 Annual Meeting, Toronto. August 24, 2009.

Meier, Patrick Philippe. *Do 'Liberation Technologies' Change the Balance of Power Between Repressive States and Civil Society?* Doctoral Thesis, Tufts University. November 2011.

Milner, Helen. "The Digital Divide: The Role of Political Institutions in Technology Diffusion." *Comparative Political Studies* 39, no. 2 (2006): 176-199.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: Public Affairs, 2011.

Murdoch, Steven J. and Hal Roberts. "Introduction to Internet Censorship and Control." *IEEE Internet Computing*, vol. 17, no. 3 (May-June 2013): 1-4. Available online through the Berkman Center for Internet and Society, at: https://cyber.law.harvard.edu/pubrelease/internet-control/.

Nodus Labs. "The Dynamics of Facebook Protest," February 10, 2012.

Norris, Pippa and Ronald Inglehart. *Cosmopolitan Communications: Cultural Diversity in a Globalized World*. New York, NY: Cambridge University Press, 2009.

OpenNet Initiative. Internet Filtering Country Profiles. Most recent reports for FSU region, 2010.

OpenNet Initiative. Filtering Data: ONI Country Data 2011. Most recent data by country, 2007-2011. Data for FSU region collected 2008-2010. Data made available online November 2011: <https://opennet.net/research/data>.

Pearce, Katy E. and Sarah Kendzior. "Networked Authoritarianism and Social Media in Azerbaijan." *Journal of Communication* (2012): 1-16.

Radio Free Europe / Radio Liberty: Caucasus Report. "Azerbaijani Opposition Plans New Wave Of Protests." July 30, 2012. http://www.rferl.org/content/azerbaijani-opposition-plans-new-wave-of-protest/24661517.html.

Ragin, Charles. *Fuzzy Set Social Science*. Chicago, IL: University of Chicago, 2000.

Reporters Without Borders. *Enemies of the Internet Report 2012*. March 13, 2012.

Reuter, Ora John, and David Szakonyi. "Online Social Media and Political Awareness in Authoritarian Regimes" (April 18, 2013). Available at SSRN: http://ssrn.com/abstract=2148690 or http://dx.doi.org/10.2139/ssrn.2148690.

Robertson, Graeme B. *The Politics of Protest in Hybrid Regimes: Managing Dissent in Post-Communist Russia*. New York, NY: Cambridge University Press, 2010.

Schedler, Andreas, Editor. *Electoral Authoritarianism: The Dynamics of Unfree Competition*. Boulder, CO: Lynne Rienner Publishers, 2006.

Shirky, Clay. *Here Comes Everybody: The Power of Organizing Without Organizations*. New York, NY: Penguin Group, 2008.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs*. January/February 2011.

Simmons, Beth and Zachary Elkins. “The Globalization of Liberalization: Policy Diffusion in the International Political Economy.” *American Political Science Review*. Vol. 98, No. 1 (February 2004): 171-189.
Stepanova, Ekaterina. “The Role of Information Communication Technologies in the ‘Arab Spring’: Implications Beyond the Region.” *PONARS Eurasia Policy Memo* 159, May 2011.
Sullivan, Jonathan. “China’s Weibo: Is faster different?” *New Media & Society* 0, no. 0 (2013): 1-14.
Tarrow, Sidney. *The New Transnational Activism*. New York, NY: Cambridge University Press, 2005.
Taylor, Adam. "WATCH: Unbelievable Footage Of The Arms Depot Explosion Turkmenistan Tried To Cover Up." *Business Insider International*. July 18, 2011.
Transitions Online. “The Kremlin’s pay-a-blogger program,” February 10, 2012.
Tufekci, Zeynep. “Too Many Messages and Only One Facebook Page: April 6th Movement in Post-Mubarak Egypt.” *Technosociology Blog*. September 19, 2011.
Way, Lucan, and Steven Levitsky, “Linkage, Leverage, and the Post-Communist Divide,” *East European Politics and Societies*, Volume 21, Number 1 (2007): pp.48-66.
Zayani, Mohamed. “Social Media and the Reconfiguration of Political Action in Revolutionary Tunisia,” *Democracy & Society*, Volume 8, Issue 2, Summer 2011.
Zittrain, Jonathan. *The Future of the Internet – and How to Stop It*. New Haven, CT: Yale University Press, 2008.
Zuckerman, Ethan. "The First Twitter Revolution?" *Foreign Policy*. January 14, 2011.
Zuckerman, Ethan. “The connection between cute cats and web censorship.” *My Heart’s in Accra Blog*. July 16, 2007.