The Janus Face of the Liberal Information Order

By

Henry Farrell and Abraham L. Newman

Memo prepared for the IO@75 Conference, Madison Wisconsin, September 7-8, 2018.
Please send comments to henry.farrell@gmail.com and aln24@georgetown.edu

In 2016, Russia employed sophisticated data manipulation to disrupt the US presidential election, information technology firms such as Apple and Amazon ranked among the most valuable in the world, and drone campaigns surpassed conventional aircraft in the US war in Afghanistan. These three disparate facts suggest the far-reaching consequences of information technology and information flows for wealth and power. However, international relations scholars have paid far less attention to these issues in relative terms than to more traditional domains such as trade, money and security (Brien and Helleiner 1980; Farrell 2006; Simmons 2011). Information is not only important in its own right, but cuts across these more traditional issues, raising important global challenges – how to maintain the technological infrastructure of information; how to distribute the rents that result; and how to manage the power asymmetries and vulnerabilities generated by it.

While there is no comprehensive multilateral institutional order for information, nor direct hegemony, the United States has led an effort to embed information flows into the international liberal order, based on principles of open communication and open access, and the limitation of censorship and interference in the development of markets for information technology and information exchange.

This regime had its roots in the prehistory of the Internet. During the Cold War, liberal states vaunted their opposition to censorship although their actual attachment to civil liberties was sometimes sporadic. Government funded broadcasting stations such as Radio Free Europe were set up to challenge authoritarian governments' control over public information, and hence perhaps undermine their rule. Research on Internet governance by scholars concerned with power and institutions found that the US (with some interaction with the European Union) deflected direct challenges to its preferred approach through the 1990s. The US blocked any agreement on rules or norms that would limit its ability to broadcast across borders (Krasner 1991), while using the OECD and other venues to press against "unjustified barriers to the international exchange of data and information." (Drake and Wilson 2005).

Domestically, policy-makers and scholars argued that information openness, like economic openness, would go hand-in-glove with political liberalization and the spread of democratic values. This was perhaps, in part an accident of timing: the Internet – which seemed to many to be inherently resistant to censorship – burgeoned shortly after the collapse of Communism in the Soviet Union and Eastern Europe. Politicians celebrated the dawn of a new era of open communication, while scholars began to argue that the spread of the Internet would lead to the spread of democracy (Diamond 2010; Shirky 2008). A second wave of literature suggested that Internet based social media had played a crucial role in spreading freedom in the Arab Spring (Howard 2010; Hussain and Howard 2013).

There were some skeptics who highlighted the vexed relationship between open networks and the closed national politics of autocracies (Goldsmith and Wu 2006), or who pointed out that the Internet was nowhere near as censorship-resistant as early optimists had supposed (Deibert et al. 2008). Even these pessimists seemed to believe that the Internet could bolster liberalism in healthy democracies, although it would by no means necessarily prevail over tyranny.

The international liberal order for information, however, finds itself increasingly on shaky ground. Non-democratic regimes ranging from China to Saudi Arabia have created domestic technological infrastructures, which undermine and provide an alternative to the core principles of the regime (Boas 2006; Deibert 2008). The European Union, while still generally supportive of open communication and free speech, has grown skeptical of the regime's focus on unfettered economic access and has used privacy and anti-trust policy to challenge its most neo-liberal elements (Newman 2008). Non-state actors like Wikileaks have relied on information openness as a channel of disruption and perhaps manipulation.

More troubling are the arguments of a new literature – that open information flows are less a harbinger of democracy than a vector of attack. Debates about cybersecurity are rapidly moving from arguments about how best to secure open international information networks to arguments over whether open networks were ever a good idea in the first place (DiResta 2018; Goldsmith 2018; Goldsmith and Russell 2018). Skeptics suggest that not only do open information flows not spread and strengthen the liberal order, but they actively threaten to undermine it, by weakening the operation of democracies within it. In this view, the liberal international policy of open cross-national networks allows flows of information and speech that actively threaten liberal politics at the domestic level (Goldsmith and Russell 2018). States and non-state actors from Russia to transnational terrorists seek to exploit the regimes openness for their own advantage, targeting the US and its allies through cyberattacks and disinformation campaigns transforming the core strength of the regime – openness – into a vulnerability.

How can IR scholars make sense of this Janus-face quality of information? In this brief memo, we argue that much of the existing work on information technology and information flows suffers from two key deficiencies. First – there has been an unhelpful separation between two important debates about information flows and liberalism. One – primarily focused on the international level – concerned global governance of information networks, examining how states (especially the US) arrived at and justified their policy stances, and how power dynamics shaped the battles between liberal and illiberal states over what the relevant governance arrangements should be (Klein 2002; Singh 2008; Mueller 2009). The other examined domestic adjustment processes, focusing on the steps that states (especially illiberal states) were taking to control their citizens' access to information (Boas 2006; Deibert and Rohozinski 2010; Deibert et al. 2008). There was remarkably little examination of the interplay between these two levels, largely because the relationship was assumed to be straightforward – an international information regime that had been shaped by liberal states was assumed to have liberalizing consequences at the domestic level.

This leads to the second problem – that research has failed to appreciate the dynamics of contestation over time. Scholars have looked to build general theories of the relationship between information and domestic and international politics, often extrapolating from observed tendencies at a particular moment. In contrast, the relationship between international information flows and domestic politics has changed substantially, as actors, who found themselves on the losing end of either the international or national political debate, have sought to undermine the status quo. Hence, rather than assuming that there is a straightforward relationship between an international liberal regime and domestic liberalism (or illiberalism), we adopt a historical institutional perspective, highlighting how the relationship has a temporal dimension, as different actors struggle either to preserve or to overturn the institutions that structure politics (Büthe 2002; Farrell and Newman 2010; Fioretos 2011; Rixen, Viola, and Zürn 2016).

Specifically, we argue following Krasner (1991) and Cowhey (1990) that different kinds of states (and factions within them) have different interests over information. Liberal states broadly prefer open flows of information, since they rely on an active civil society that is largely independent of the state and require free access to information and communication to work well. Illiberal ones prefer controlled flows, since they view civil society more as a threat than a resource (Milner 2006; Holkeboer and Vreeland 2013). This means that international communications regimes are less shaped by efficiency considerations than by distributional conflict (Bussell 2011; Newman 2010), leading to outcomes that favor or disfavor particular states, depending on their preferences.

However, contrary to Krasner and Cowhey, we assert that these distributional dynamics do not lead to stable equilibria, but instead provide states that feel themselves to be disadvantaged with strong incentives to destabilize international regimes that disfavor them. Moreover, the distributional conflict plays out in a transnational setting, in which actors may engage in strategies at the international or the domestic level to influence either or both (Risse 1995; Sikkink 2005; Farrell and Newman 2014). Thus, we argue that the relationship between the international regime and domestic politics is a cross-roads rather than a one-way street. Influence flows in both directions, so that just as international politics shapes and limits states' options at the domestic level at time *t*, disadvantaged states' responses can have international consequences at time *t+1*, reshaping the regime in unexpected ways.

Hence, we provide a quite different account of the liberal information regime, which emphasizes its fragmentation and incompleteness rather than its seamlessness, how it has opened up opportunities to actors looking to reshape it, and how this has resulted in important empirical variation over time. We draw not only on international relations, but on debates in law and computer science, weaving together a history of empirical changes with a history of changes in the academic debates that sought to characterize them.

In this history, the initial process of bargaining – which was dominated by the US – created a global information regime in which the Internet was largely isolated from existing multilateral international institutions and instead was structured around self-regulation and a 'multistakeholder' model of governance. Even as the US pressed for substantive norms of open communication and information flows, it resisted the creation of truly multilateral institutions, in which governance disputes might be resolved. This decision would have lasting effects on how losers of the information regime would seek to resolve their dissatisfactions and ultimately open up vulnerabilities to the regime. Scholars who looked to characterize this regime did so from within, treating the Internet largely as an extension of US values.

Illiberal states and non-state actors that were dissatisfied with this regime did not simply accept it, but sought out strategies to change it at the international level, and, when that was unsuccessful, to shield themselves from its domestic consequences. This led to a second wave of research, that focused on the circumstances under which the Internet might or might not have liberalizing global consequences, and the specific resistance strategies.

We are now in a third phase, since domestic strategies centering on disrupting open information flows turned out to have unsuspected international purchase – they could not only be used to divide domestic political opponents but could be weaponized against liberal states, turning the liberal regime of international information flows against the states which had created it. A new wave of skeptical scholarship argues that the Internet was never the liberalizing force it was made out to be, and that instead, key aspects of the open information order have turned out to generate critical security vulnerabilities for liberal democracies, and the absence of multilateral institutions has made it more difficult to coordinate to fix them.

In contrast to nearly all of the existing literature, which proceeds from general arguments about the relationship between information and liberalism, we look to capture the dynamic nature of contestation over the liberal order. In contrast to arguments that effectively insulate international and domestic interactions from one another, or treat them as being related through some unvarying mechanism, we examine how the interaction between the two levels has changed over time.

A new liberal order for information flows – open but unembedded

The modern liberal approach to information flows had its origins in the early 1990s, when it became clear that the Internet, which had begun as a means of connecting academic research institutions, had the potential to become a global network, with potential transformative consequences for human interaction, but an accompanying need to solve global coordination and cooperation problems. This led the US government to try to fashion a liberal information order, which prioritized market and political openness, as well as industry led self regulation, sidelining the existing multilateral framework for telecommunications in favor of private, 'multistakeholder' bodies.

A key early challenge for the Internet centered on maintaining the stability of and control over the standards used to get information from point a to point b on the network. Up until the 1990s, the Internet had been run by a largely self-appointed community of volunteers, centered around the Internet Engineering Task Force (IETF), and in particular Jon Postel, who had informal control of the 'root' system through which Internet domain names were translated into Internet Protocol addresses. As the commercial value of the Internet became clearer, conflicts began to disrupt this informal system, leading Postel and others to sign a memorandum of understanding with the International Telecommunication Union (ITU) and other multilateral organizations, to create a Switzerland-based organization that would organize the technical aspects of the Internet. However, when the US government decided to intervene in the dispute, threatening criminal charges against Postel for his efforts to demonstrate his independent control of the root, the memorandum became moot (Goldsmith and Wu 2006, Mueller 2009).

The new regime for international information flows relied on self-regulation and 'multistakeholderism' rather than traditional multilateral institutions (Kiggins 2015). This regime was in large part a product of US preferences (Drezner 2007; Bach 2010). Other liberal jurisdictions, such as the European Union, were largely inattentive to the political questions that the Internet presented – they had neither the technical capacity nor the organizational resources to properly understand its long term consequences. Illiberal states were similarly disengaged. China had a highly limited role in international discussions over Internet governance, and a "marginal" position in early policy debates (Shen 2016), while Russia was undergoing its own great political and economic upheavals.

The result was that domestic debates within the US played a greater role than international disputes in shaping the emerging regime. The political debates had three key consequences. First, a primarily US-based argument between the technical community, emerging business interests and the US government over how the Internet's domain name system should be run led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization incorporated under Californian law (Bach 2010), as an alternative to locating Internet governance in the ITU or UN. ICANN was contracted by the US Department of Commerce to handle the technical maintenance of the root system. This system reflected the desire of Ira Magaziner, the president's senior adviser on Internet policy to keep the Internet "as free as possible from government control, while at the same time giving the imprimatur of government control for purposes of security." (Goldsmith and Wu 2006). ICANN had a complicated internal governance system based on 'multistakeholderism,' which sought, with indifferent success, to provide voice to a variety of different commercial and political constituencies. States had an advisory role through ICANN's Government Advisory Committee, but no formal veto, while the US retained an *ultima ratio* through its contractual relationship with ICANN.

Second, an early dispute between business and national security interests over cryptography promoted liberal values of political openness in the nascent regime. National security officials wanted weak standards for encrypted communication, which would have made it far easier for the National Security Agency (NSA) to tap into Internet communications. Business interests – supported by Magaziner and others in the administration – feared that this would stunt the development of international electronic commerce (which required strong cryptography to ensure trust). Business pressure, together with the efforts of privacy activists deliberately to subvert US export controls on cryptography led to the apparent collapse of the US cryptography regime, and its replacement by a mixture of private technology and government recommended standards (which were nominally set by NIST rather than the national security community). US national security interests were not relegated, but were instead reinterpreted in light of the need for greater economic growth (Kiggins 2015), and the spread of communication technologies that would in turn make the world less hostile to US interests. US politicians saw the Internet as inherently embodying liberal US values, providing a communications infrastructure that appeared to be inherently resistant to censorship and control.

Third, the US set out a "Global Framework for Electronic Commerce," drafted by Magaziner, which posited that the "success of electronic commerce will depend on continued private sector leadership," forcefully advocated self-regulatory solutions across a variety of controversial issue areas, and made economic openness a cornerstone of the regime. This document was drafted in close consultation with US business: as one of the drafters noted later, the "project was driven pure and simple by interests of American companies who wanted to create [a global] electronic commerce market and did not want to be bogged down by inconsistent regulation" (Kiggins 2015, 96). Notably, the US was prepared to push for strong regulation in areas, such as intellectual property, where US interests would otherwise be damaged. However, it also reflected the sincere belief of Magaziner and other officials that self-regulation was superior to standard multilateral or bilateral instruments. US officials feared that without such a framework, the "purpose of the Internet as a platform for expansion would be impeded by multilateral governance structures." (Kiggins 2015, 95). It also reflected the interests of US e-commerce firms, which saw an opportunity to dominate global markets so long as they were not impeded by regulatory barriers. Finally, it sought to mirror the domestic US approach, which was also based heavily on self-regulation (Farrell 2003; Newman and Bach 2004).

Most importantly, e-commerce companies that provided a platform for third party users received a wide-ranging 'safe harbor' for sharing their users' content under Section 230 of the Communications Decency Act, which both insulated them from private action and allowed them (if they wanted) to remove content without legal liability, encouraging them to set up private schemes of regulation. The US wanted to implement this self-regulatory approach (which proved crucial to the development of e-commerce businesses like Google and Facebook) on the global as well as national level. While the Framework of course had no binding force on other states, it played an important agenda setting role, especially when combined with the burgeoning power of US e-commerce firms and the willingness of the US government to back them up.

This US-centric vision of the Internet was reflected in academic debates, which were primarily conducted among legal and information technology scholars rather than social scientists. Much of this scholarship reflected libertarian beliefs. Thus, for example, Johnson and Post (1996) built on libertarian arguments about the relationship between the Internet and freedom to argue that the Internet was creating its own space and political order, independent from traditional notions of territorial integrity and national borders, which would and should be governed by self-constituting self-regulatory arrangements (Spar 1999). Others, such as Larry Lessig (1999), disputed this account from within liberalism, arguing that the values of the Internet could only be preserved through some kind of constitutional order, or that the Internet would create more complex forms of overlapping sovereignty, resembling the medieval era (Kobrin 2001). As it became clear that the Internet was not somehow magically protected from state intervention, a more skeptical literature began to emerge, arguing that the jurisdictional problems that the Internet presented were not unprecedented and that states could continue to use their regulatory tools to achieve their preferences (Goldsmith 1997; Goldsmith 2000; Boas 2006), albeit with more success against some actors than others (Swire 1998). Even the skeptics, however, tended to think of the political battles in terms of possible limits on the ability of US style liberal regimes to impose their preferences, rather than about possible challenges that the Internet presented to these liberal regimes themselves.

Thus, a new cross-border information order emerged in the 1990s as a result of US pressure. Aside from an early conflict with Europe over privacy rules (Farrell 2003; Newman 2008), there was remarkably very little effort by other states to shape this order in ways that reflected their own, different priorities, at this early stage. This meant that the new order was in large part a product of arguments within the US rather than arguments between the US and other states. This order was deliberately built on very different foundations than the previous telecommunications regime, spurning multilateral organizations such as the ITU in favor of multistakeholder organizations such as ICANN, where some veneer of governmental authority was needed, and more or less pure self-regulation where it was not. The decisions made in this early period – to avoid a state-based, multilateral governance institution as well as the belief in open communication and markets – set the stage for many of the most consequential conflict to emerge in later periods.

Distributional dispute within the liberal order

As other states began to realize the political and economic importance of the Internet, bitter distributional disputes emerged. These focused on the content of the new international regime, which privileged open communication and the industry interests of US firms, as well as procedural issues. Other liberal states that were more friendly to government regulation and consumer protection, saw the information order as threatening the competitiveness of their incumbent firms and politicians as well as other fundamental rights like privacy (Newman 2010; Bussell 2011). Illiberal states such as China and Russia (after its 'managed democracy' had started to coalesce) began to fear that open information flows might threaten their internal regime stability (Milner 2006). Both groups sought to relocate control of the Internet within a more traditional multilateral framework, where they would have veto power, and to create new international norms around 'information security.' Internal divisions within the reform camp, however, limited its effectiveness, leading to effective global stalemate

As other jurisdictions began to develop their own technical knowledge and specialized bureaucratic structures, they were better able to articulate and press for their own goals. This led to a complex set of international disputes in which states and non-state actors challenged the apparent US *fait accompli*, but quarreled among themselves about what ought to replace it.

A literature, dominated by scholars working on information policy rather than international relations, described the resulting international battles (Klein 2004; Mueller 2010). Illiberal states preferred traditional multilateral institutions such as the ITU, where they believed that they would have greater influence. Liberal states disagreed. Some, like Japan, were willing to acquiesce to the US position. Others, such as the European Union, pressed for a stronger role for government, while remaining suspicious of the motives of illiberal states. Others yet, such as Brazil, harked back to pre-Internet debates about "trans-border data flows," where non-Western countries had sought a real say over the global information order, only to be sidelined by the US and its allies (Drake 2016). These disputes were complicated by international organizations such as the ITU, which pressed their own interests, and "civil society" actors, who looked to build a non-governmental voice (while never being able to agree among themselves about where civil society began and ended).

These fractious relations came to a head in the United Nations' World Summit on the Information Society, which began with an ITU initiative to reestablish a dominance it feared it was losing, as ever more telecommunications activity was based on Internet platforms. Between 2002 and 2005, a series of meetings took place, with ICANN, and the US government's control over it, dominating the agenda (Klein 2004). Brazil took the lead in arguing for an alternative regime where national governments would have "full involvement" (Mueller 2010). The US responded by announcing that it intended to continue to "preserve the security and stability" of the domain name system; however, the European Union, which had previously tacitly supported the US position, broke with it, and began to argue for greater government involvement. The result of the summit was a tacit acceptance by the US that other governments should have greater influence within ICANN – so long as they accepted the ICANN framework, and the sidelining of further political debate into an Internet Governance Forum (IGF) that merely had exhortatory power. This was, effectively, a stalemate in which US preferences continued to play a dominant role, because other states were incapable of organizing effectively to reverse the choices that the US had made, and because even if they had been successful, they would only have been able to exercise very limited power.

This international stalemate allowed large e-commerce firms, most of which were based in the US, to build their own private international orders, filling in the governance gap left by the US with corporate rules, practices and Terms of Service. Although ICANN played a crucial technical role, and offered some possible means of influence and suasion, the real regime of international information flows was being built by large private firms, which largely operated outside the reach of dissident non-Western states. This regime went largely undiscussed in the political science literature (Farrell 2006).

The underlying communications networks that enabled the Internet to work had grown in such a way that the key nodes of exchange were located in the US and Western Europe (Farrell and Newman 2018). The giants of e-commerce that shaped the social lives and communications of billions of consumers worldwide were again primarily based in the US, which magnified the importance of interaction effects between the US regulatory approach and the international vacuum of rules. Section 230 of the Communications Decency Act provided firms with effective safe harbor from liability for content that was uploaded by their users (this safe harbor was more limited against intellectual property violations, but still provided protection so long as they took down such content when they were notified). These protections combined with new forms of algorithmic management to create businesses that could serve billions of consumers with thousands of employees. The complex work of Facebook's advertising markets, for example, was outsourced to algorithms that used machine learning to categorize Facebook users in a myriad different ways, and then sell their attention to advertisers in algorithmically managed markets. This business model scaled globally as well as nationally, so long as domestic government regulations did not interfere. Instead, platform firms became their own regulators, creating Terms of Service and informal corporate practices to shape their users' behavior, and mitigate excesses that might drive away other users. Decisions that involved difficult ethical tradeoffs and had profound political consequences were made according to a primarily commercial logic (Gillespie; 2018).

A second domestically focused literature examined and sought to categorize the emerging forms of domestic censorship and information control (Boas 2006; Deibert 2008; Deibert and Rohozinski 2010). While one of the most prominent participants in this literature was a political scientist, Ronald Deibert, his and other scholars' findings got remarkably little attention among comparativists and international relations scholars, instead speaking to a community of subject matter specialists. In this world, illiberal states could not effectively impose their international preferences, but could still fortify borders against unwanted information flows. Thus, for example, Deibert and others described how Saudi Arabia ensured that all broadband communications into and out of the country went through two locations, allowing it to censor for unwanted political and sexual content. Equally, illiberal states could demand that platform companies block certain content as a requirement of doing business in their jurisdiction. However, surveillance and censorship involved tradeoffs, so that effectively blocking problematic content (in the eyes of the state) was likely to lead to the blocking of content that was popular with a country's inhabitants. If, for example a country blocked all access to YouTube, it was likely to make its own citizens unhappy. If, alternatively, it required YouTube to block access to particular kinds of content, it had to recognize that this would at best be only partly effective (Zuckerman 2015). The only country that solved this problem was China – which had a sufficiently large internal market that it could effectively drive US based e-commerce firms away and encourage the growth of economically sustainable domestic competitors that were more amenable to censorship. Even here, the strategy ran into limits, since Chinese companies' business models required them to operate at large scale with limited scope for human censorship of content that was carefully worded to avoid automatic filters (MacKinnon 2008; Zuckerman 2015).

Thus, for a decade or more, a stalemate at the international level allowed US preferences to prevail passively, and US based e-commerce services to spread through much of the world. This created a regime in which government played a relatively limited role, and private ordering principles dominated governance. These companies appeared to reinforce liberal principles, precisely to the extent that liberal ideals and the profit motive coincided. Furthermore, individual states could limit the domestic impact of cross border information flows, albeit at a cost. The consequence was a spatchcock regime with notable incongruity between the international level – where US preferences blocked others from creating a more traditional multilateral framework, and the domestic level – where open information flows seemed to support liberal states, while presenting illiberal states with a series of awkward choices, that they resolved through different mixes of censorship and openness.

Weaponized liberalism

After September 11, 2001, leaders in the US increasingly sought to resolve these contradictions in favor of global liberalism. US leaders had long believed, in a version of the "open door" approach, that open communications would help disseminate liberalism globally. Even in the 1990s, Bill Clinton had quipped that attempts to recreate censorship in cyberspace were "sort of like trying to nail Jello to the wall." However, they had seen this as a largely passive process. The George W. Bush administration and the Obama administration were respectively inspired by neo-conservative and liberal beliefs about the desirability of spreading democracy to actively disseminate communications technology as a means towards that end. This generated new concerns for illiberal governments who began to see information technology not just as a new technological challenge but as an inimical expression of US power.

These foreign policy measures were in part driven by a new literature that spanned the academy and the public space. Technology intellectuals like Clay Shirky (2008) argued that new communications technologies empowered civil society against potentially oppressive governments by radically lowering the costs of collective action (Warren 2015). Scholars like Larry Diamond (2010) wrote about the enormous potential benefits of "liberation technology," which enabled "citizens to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom." These arguments built on what Tim O'Reilly had dubbed "Web 2.0," social media sites such as Facebook, YouTube and Twitter that made it quick and easy for people to publish content that could be seen by many others.

The result was that US Secretary of State Condoleezza Rice created a Global Internet Freedom Task Force in 2006 (Dobriansky 2008), and began to actively fund efforts to develop and spread anti-censorship technology towards the end of the George W. Bush administration. These efforts continued under the Obama administration: under both Republicans and Democrats,

> the US government comprehensively link[ed] the provision of the Internet in a form that enhances the free flow of information to the development and expansion of democratic government internationally [suggesting] a causal connection between democracy and the free flow of information—the provision of the free flow of information will lead to democratic government (McCarthy 2010, 99).

In 2010, Secretary Clinton gave a much heralded speech, which explicitly outlined a US policy dedicated to promoting Internet freedom abroad, emphasizing the freedom to access information, for individuals to generate content, and to participate in citizen-to-citizen communication.

The actual funding devoted to these efforts was relatively tiny. Furthermore, the US had little institutional capacity to oblige US firms such as Google, Facebook and Twitter to spread freedom (Farrell and Newman 2018). While a State Department official, Jared Cohen, claimed that he had influenced Twitter to delay a maintenance update so as to ensure that Twitter was available during a period of widescale protests in Iran during social protests, it later became clear that Twitter was not, in fact, widely used to help organize these protests (Aday et al. 2010). Cohen went on to work for Google and co-authored a book with Google CEO Eric Schmidt, *The New Digital Age*, which outlines how information technology would transform societies worldwide.

These expectations were heightened by a wave of revolutions that appeared to be driven, at least in part, by decentralized communications networks, and were certainly treated as such in news reports and by think tanks and some scholars (Howard 2010; Hussain and Howard 2013; Warren 2015). There is still debate over the causal importance and underlying mechanisms through which social media mediated change in the "Arab Spring" (Lynch 2011). It is clear that social media allowed new public spheres to develop in many non-democratic countries, and plausibly undermined the "preference falsification" that bolstered authoritarian regimes, but its role was exaggerated by media in liberal countries, and it has furthermore failed to support durable democracy in many of the countries that experienced upheavals (Farrell 2012).

Nonetheless, the combination of widespread upheavals, and US cheerleading for the liberalizing effects of social media technology spurred fears in illiberal governments that they were being targeted for elimination. This led states such as Russia and China to redouble their efforts to reshape the international data regime. In 2011, Russia proposed a "Convention on International Information Security" that was intended to delegitimize interference in the internal affairs of states and strengthen the ability of states to limit communication flows for security reasons. Notably, the Convention sought to outlaw "information warfare" under international law, including actions aimed at:

> undermining political, economic, and social systems; carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents.

This initiative was supported at the UN by China, which argued that "practicing power politics in cyberspace in the name of cyber-freedom is untenable." However, again, these efforts failed to make headway against the opposition of liberal powers, which saw free information flows as reinforcing rather than undermining their own systems of rule. When the Snowden revelations in June 2013 made clear that the US had been secretly using its privileged position in global information networks in notably illiberal ways, it seemed for a period that states such as Brazil (which had been the target of extensive surveillance) might defect from the blocking coalition, but moderate US concessions defused the threat.

Again, illiberal governments found that they had more resources at the domestic level. China had already started to push for data sovereignty, regulating companies to limit cross-border data flows, ostensibly to limit cyberattacks and enhance information security, but also to limit the circulation of Chinese data through US data centers. In 2010, Google effectively ceased to operate on China's mainland, although other companies such as Apple sought to remain on the Chinese market. Illiberal states also began to experiment with new technological approaches. While China had a highly developed censorship regime, Russia did not. Both states began to experiment with approaches that did not involve direct censorship but the opposite, using third party agents or (in the case of China), low level state employees to “flood” social media with propaganda and messages actively intended to sow confusion in communities, making conversation among potential antagonists impossible. In contrast to more conventional propaganda, which directly promotes a state message, ‘flooding’ seeks to overwhelm the cognitive capacity of regime antagonists. By promoting multiple narratives, distraction, and internal dissent within communities, they sought to stymie collective action (King et al. 2013; Roberts 2018; Tucker et al., 2018).

Weaponized liberalism, rather than leading to the spread of democracy, plausibly prompted authoritarian regimes to develop technological approaches that could be turned to their own advantage, generating a new descriptive and explanatory literature, which is notably better integrated into the social sciences than its predecessors (Deibert 2015; Gunitsky 2015; MacKinnon 2011; MacKinnon 2013; Roberts 2018; Tufekci, 2017; Tucker et al., 2017). Increasingly, authoritarian innovation has had international as well as domestic implications, as, for example, illiberal states began to use Distributed Denial of Service (DDoS) attacks to cripple web servers located in other jurisdictions. The liberal information order not only reached its apparent limits in promoting domestic change, but prompted the development of tools that could be used to weaken or undermine it.

Reversing the Flows

Over the last few years, it has become clear that liberal states too may be vulnerable to the destabilizing consequences of cross-border information flows. Digital technologies open up new channels of communication and contestation for non-state actors ranging from regulators to NGOs to terrorist networks (Cronin 2003; Carpenter 2007; Newman 2008). This creates a situation of complex governance, where traditional state actors lose their monopoly of control over international affairs (Keohane and Nye 1998; Kahler 2016). Non-state actors have leveraged information dissemination as a new weapon to put pressure on liberal states. Wikileaks, the Panama Papers and the Snowden revelations demonstrate how open information policy has generated new opportunity structures for transnational politics (Farrell and Newman 2018).

At the same time, domestic innovations in illiberal states have begun to spill over globally. Flooding attacks may increase the stability of authoritarian regimes, which depend on a divided opposition, but by the same token may help destabilize liberal states, which rely on decentralized forms of knowledge and agreement to maintain political legitimacy (Farrell and Schneier 2018). By either accident or design, illiberal states such as Russia have found ways to turn the open international information regime into a vulnerability for the United States and other liberal states.

Russia, in particular, began using the Ukraine conflict as a test bed for these strategies. Russia perceived the election of a pro-western government in 2014, as a direct attack on its influence in the “near abroad,” and a possible dress rehearsal for an information attack on Russia itself. This led the Russian government to sponsor a range of activities, including the use of flooding and other domestic disinformation campaigns on an international level, hacking election systems, promoting conspiracies and false information, and creating fake social media accounts, which were used to generate confusion and distraction (Greenberg 2017). These same tactics were then deployed in the US presidential election of 2016, the BREXIT vote, as well as a series of electoral campaigns in Europe. The direct effects of these attacks in changing voters’ minds are at best uncertain (Tucker et al., 2018). However, the indirect consequences, in spurring confusion and distrust in electoral systems have been substantial.

The private governance order created by the US has not been able to address the problem, and has sidelined multilateral institutions such as the UN and the ITU from decision-making. Instead, governments are obliged to turn to private companies (e.g. Facebook, Google, Twitter) to act as intermediaries on their behalf. This has proved difficult, especially in the US where these companies are largely insulated from state control, and have only limited direct motivation to address the problem. This has created a difficult Catch 22 for the US and its allies, in which earlier decisions taken to create a liberal information order constrain them from taking direct action to protect liberal political institutions from very serious threats.

Conclusions

In this memo, we applied our framework to understand the evolution of international information flows and domestic information politics since the early 1990s. We show how the early choices of states – and in particular the United States – have had long-lasting consequences for global information flows, many of which were not anticipated *ex ante*, and how information flows that at one point were depicted as "mass psychological campaigns" against illiberal states are now accused of fostering such campaigns against liberal ones. Early US decisions created an information order that was dominated by private actors, which are now perhaps proving more resistant to liberal pressures than illiberal ones. Companies such as Facebook and Google are at best grudgingly cooperating with efforts to limit information attacks, while Google is reportedly prepared to make sweeping concessions on state control and surveillance to regain access to the Chinese market.

Our account puts information where it should be – at the heart of research in international affairs (Brien and Helleiner 1980; Simmons 2011; Branch 2017; Farrell and Newman 2018). While scholars of international relations have focused on trade and security, a global information order has been built that has primary consequences for global liberalism and world politics. Our memo contributes to the special issue project by demonstrating the deep connection between information and the liberal order, refocusing attention on how that order privileged open communication; a fact that has now become one of the liberal order's central vulnerabilities.

Our account emphasizes the disparity between the ideal typical depiction of the liberal order and how it has evolved in practice. The liberal information order rested on a set of very powerful ideas about political openness and economic freedom, even while it rejected the standard multilateral approach. In doing so, it opened the door to political opposition from illiberal states, who saw little value in helping Western-based technology firms, and deviated domestically from the core norms of the order. The ideal of the liberal information order not only misled its proponents, but prompted its opponents to undermine it. We do not claim that this means collapse and catastrophe, but instead predict that the counter-efforts of liberal states, should they succeed, will likely lead to a new regime that is very far removed from their previous rosy assumptions.

It also cautions against standard depictions of the international liberal order, which create artificial distinctions between international and domestic politics. Ruggie (1982)'s iconic description of embedded liberalism, for example, suggested that the post war order for trade was largely separable from domestic interventions and adjustments. Alternatively, work in the second image reversed tradition tend to emphasize the one way street from international forces to the domestic. Neither provides much room for true transnational politics, in which political forces at the international and domestic exert mutual influence. These intellectual blinders created overconfidence in the trade regime and its independence from feedbacks generated at the domestic level. They have similarly led to misunderstanding in the case of information politics of the reciprocal relationships underlying the international regime for information, domestic responses by illiberal states, and the reverberations of these responses as they are deployed to unsettle or transform the liberal order.

We depict the international liberal order as being less an order as such than a system of complex contention, that evolves over time. Rather than thinking of the international liberal order as a stable equilibrium, we emphasize its flux. Actors who are dissatisfied with the order develop strategies to challenge it and look to exploit international and domestic interactions to transform it (Tarrow 2001; Sikkink 2005). This allows us to avoid nostalgia for a perceived golden age, and instead understand how the inherent tensions of the liberal order itself sowed the seeds of its possible destruction or possible transformation.

Finally, we emphasize that if we are properly to understand the global information order, we not only need to place it at the heart of international relations, but integrate insights from other scholarly understandings into how it operates. Throughout our narrative, we have described not only the empirical changes in the liberal information order, but the changes in the scholarly literatures that have sought, with greater or lesser success, to describe it. Understanding – rather than merely explaining – will require the embrace of new research techniques, and the integration of insights from computer scientists and others about how the order operates in practice. For example, a proper understanding of "flooding" techniques and their consequences will require the mapping of social media networks, the ability to discern humans from automated systems and a sound technical understanding of emerging approaches such as generative adversarial networks which may have profound consequences both for attacks that look to weaponized cross-border information flows and for efforts to mitigate or prevent them. On the one hand, there is a vibrant literature in computer science that looks to map and understand the technical aspects of new security and informational threats, but has little engagement with the systematic political implications (Ferrara, 2017, Shao et al. 2017, Shao et al. 2018). On the other, there is an emerging political science literature that has the opposite strengths and weaknesses (e.g. Hafner-Burton, Kahler, and Montgomery 2009; King, Pan, and Roberts 2013). Bringing them together is an urgent challenge for scholarship and policy-making.

Bibliography

Aday, Sean, Henry Farrell, Marc Lynch, John Sides, John Kelly, and Ethan Zuckerman. 2010. *Blogs and Bullets: New Media in Contentious Politics*. Washington DC: United States Institute of Peace.

Bach, David. 2010. Varieties of Cooperation: The Domestic Institutional Roots of Global Governance. *Review of International Studies* 36(3): 561–89.

Bach, David and Abraham L Newman. 2007. The European Regulatory State and Global Public Policy: Micro-Institutions, Macro-Influence. *Journal of European Public Policy* 14(6): 827–46.

Boas TC. 2006. "Weaving the authoritarian web: The control of Internet use in nondemocratic regimes." Eds. John Zysman and Abraham Newman. In *How revolutionary was the digital revolution*. (Stanford: Stanford University Press: 361-78).

Brien, R.C.O. and Helleiner, G.K., 1980. The political economy of information in a changing international economic order. *International Organization*, *34*(4), pp.445-470.

Branch, J., 2017. Territorial Conflict in the Digital Age: Mapping Technologies and Negotiation. *International Studies Quarterly*, *61*(3), pp.557-569.

Bussell, J., 2011. Explaining cross-national variation in government adoption of new technologies. *International Studies Quarterly*, *55*(1), pp.267-280.

Büthe, T., 2002. Taking temporality seriously: Modeling history and the use of narratives as evidence. *American Political Science Review*, *96*(3), pp.481-493.

Carpenter, R.C., 2007. Studying issue (non)-adoption in transnational advocacy networks. *International Organization*, *61*(3), pp.643-667.

Cowhey, P.F., 1990. The international telecommunications regime: the political roots of regimes for high technology. *International Organization*, *44*(2), pp.169-199.

Cronin, A.K., 2003. Behind the curve: Globalization and international terrorism. *International security*, *27*(3), pp.30-58.

Deibert, Ron. Cyberspace Under Siege. *Journal of Democracy* 26(3): 64–78.

Deibert, Ronald and Rafal Rohozinski. 2010. Liberation Vs. Control: The Future of Cyberspace. *Journal of Democracy* 21(4): 43–57.

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

Diamond, Larry. 2010. Liberation Technology. *Journal of Democracy* 21(3): 69–83.

DiResta, Renee. “The Information War is on. Are We Ready for it?” *Wired*, 2018.

Dobriansky, Paula. 2008. *New Media Vs. New Censorship: The Authoritarian Assault on Information: Remarks of Paula J. Dobriansky to Broadcasting Board of Governors, September 10, 2008*.

Drake, William. 2016. *Background Paper for the Workshop on Data Localization and Barriers to Transborder Data Flows*. 2005. The Governance of Global Electronic Networks.

Drezner, D.W., 2008. *All politics is global: Explaining international regulatory regimes*. Princeton University Press.

Farrell, Henry. 2003. Constructing the International Foundations of E-commerce: The EU-US Safe Harbor Arrangement. *International Organization* 57(2): 277–306.

Farrell, Henry. 2006. Regulating Information Flows: States, Private Actors, and E-commerce. *Annual Review of Political Science* 9353–74.

Farrell, Henry. 2012. The Consequences of the Internet for Politics. *Annual review of political science* 15

Farrell, Henry and Newman, Abraham L., 2014. Domestic institutions beyond the nation-state: charting the new interdependence approach. *World Politics*, *66*(2), pp.331-363.

Farrell, Henry and Abraham L. Newman. 2018. Linkage Politics and Complex Governance in Transatlantic Surveillance. *World Politics*, October, pp. 1-40.

Farrell, Henry and Abraham L. Newman. 2018. *Weaponized Interdependence*. Unpublished Paper.

Farrell, Henry and Bruce Schneier. 2018. Common Knowledge Attacks Against Democracy.

Ferrara, Emilio. 2017. *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*. Unpublished Paper.

Fioretos, O., 2011. Historical institutionalism in international relations. *International Organization*, *65*(2), pp.367-399.

Greenberg, Andy. 2017. How an Entire Nation Became Russia’s Test Lab for Cyberwar. *Wired*. June 20.

Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

Goldsmith, Jack. 1997. Regulation of the Internet: Three Persistent Fallacies. *Chicago-Kent Law Review* 731119.

Goldsmith, Jack. 2000. Unilateral Regulation of the Internet: A Modest Defence. *European Journal of International Law* 11(1): 135–48.
Goldsmith, Jack. 2018. *The Failure of Internet Freedom*. New York, NY: Knight First Amendment Institute.

Goldsmith, Jack and Stuart Russell. 2018. *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations*. Palo Alto, CA: Hoover Institution.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet: Illusions of a Borderless World*. New York: Oxford University Press.

Gunitsky, Seva. 2015. Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability. *Perspectives on Politics* 13(1): 42–54.

Hafner-Burton, E.M., Kahler, M. and Montgomery, A.H., 2009. Network analysis for international relations. *International Organization*, *63*(3), pp.559-592.

Holkeboer, C.B. and Vreeland, J.R., 2013. Calling Democracies and Dictatorships: The Effect of Political Regime on International Long-Distance Rates. *Kyklos*, *66*(3), pp.417-437.

Howard, Philip N. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford University Press.

Hussain, M.M. and Howard, P.N., 2013. What best explains successful protest cascades? ICTs and the fuzzy causes of the Arab Spring. *International Studies Review*, *15*(1), pp.48-66.

Johnson, David R and David Post. 1996. Law and borders: The Rise of Law in Cyberspace. *Stanford Law Review* 1367–402.

Kahler, M., 2016. Complex governance and the new interdependence approach (NIA). *Review of International Political Economy*, *23*(5), pp.825-839.

Keohane, R.O. and Nye Jr, J.S., 1998. Power and interdependence in the information age. *Foreign Affairs*, *77*, p.81.

Kiggins, Ryan David. 2015. Open for Expansion: US Policy and the Purpose for the Internet in the Post--Cold War Era. *International Studies Perspectives* 16(1): 86–105.

King, Gary, Jennifer Pan, and Margaret E Roberts. 2013. How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review* 107(2): 326–43.

Klein, Hans. 2002. ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society* 18(3): 193–207.

Klein, Hans. 2004. Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society. *Information Technologies \& International Development* 1(3-4): 3–13.

Kobrin, Stephen J. 2001. Territoriality and the Governance of Cyberspace. *Journal of International Business Studies* 32(4): 687–704.

Krasner, Stephen D. 1991. Global Communications and National Power: Life on the Pareto Frontier. *World Politics* 43(3): 336–66.

Lynch, Marc. 2011. After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State. *Perspectives on politics* 9(2): 301–10.

MacKinnon, Rebecca. 2008. Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China. *Public Choice* 134(1-2): 31–46.

MacKinnon, Rebecca. 2011. China's "Networked Authoritarianism". *Journal of Democracy* 22(2): 32–46.

MacKinnon, Rebecca. 2013. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

McCarthy, Daniel R. 2010. Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet. *Foreign Policy Analysis* 7(1): 89–111.

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

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT PRess.

Mueller, Milton L. 2009. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. MIT press.

Newman, Abraham. 2008. *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press.

Newman, A.L., 2008. Building transnational civil liberties: Transgovernmental entrepreneurs and the European Data Privacy Directive. *International Organization*, *62*(1), pp.103-130.

Newman, A.L., 2010. What you want depends on what you know: Firm preferences in an information age. *Comparative Political Studies*, *43*(10), pp.1286-1312.

Newman, A.L. and Bach, D., 2004. Self-Regulatory Trajectories in the Shadow of Public Power: Resolving Digital Dilemmas in Europe and the United States. *Governance*, *17*(3), pp.387-413.

Risse, T., 1995. *Bringing transnational relations back in: Non-state actors, domestic structures and international institutions*(Vol. 42). Cambridge University Press.

Rixen, T., Viola, L.A. and Zürn, M. eds., 2016. *Historical institutionalism and international relations: explaining institutional development in world politics*. Oxford University Press.

Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside Chinas Great Firewall*. Princeton University Press.

Ruggie, J.G., 1982. International regimes, transactions, and change: embedded liberalism in the postwar economic order. *International organization*, *36*(2), pp.379-415.

Shao, Chengcheng, Giovanni Luca Ciampaglia, Onur Varol, Alessandro Flammini, and Filippo Menczer. 2017. The Spread of Fake News by Social Bots. *arXiv preprint arXiv:1707.07592*

Shao, Chengcheng, Pik-Mai Hui, Lei Wang, Xinwen Jiang, Alessandro Flammini, Filippo Menczer, and Giovanni Luca Ciampaglia. 2018. Anatomy of an Online Misinformation Network. *PloS one* 13(4): e0196087.

Shen, Hong. 2016. China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication* 9(3): 304–24.

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

Sikkink, Kathryn. 2005. Patterns of Dynamic Multilevel Governance and the Insider-Outsider Coalition. *Transnational Protest and Global Activism*, edited by Donatella Della Porta and Sidney Tarrow, 151–73. New York: Rowman and Littlefield.

Simmons, Beth. 2011. International studies in the global information age. *International Studies Quarterly*, *55*(3), pp.589-599.

Singh, JP. 2008. Negotiation and the Global Information Economy (Cambridge: Cambridge University Press).

Spar, Debora L. 1999. Lost in (Cyber) Space: The Private Rules of Online Commerce
Private Authority in International Affairs. edited by Inge Kaul, Isabelle Grunberg, and Marc A. Stern, 31–52. Albany, NY: SUNY Press Albany.

Swire, Peter P. 1998. Of Elephants, Mice, and Privacy: International Choice of Law and the Internet University of Pennsylvania Law Review. 32(4)(4): 1975–2001.

Tarrow, S., 2001. Transnational politics: contention and institutions in international politics. *Annual review of political science*, *4*(1), pp.1-20.

Tucker, Joshua, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. 2018. Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.

Tucker, Joshua A., Yannis Theocharis, Margaret E. Roberts, and Pablo Barberá. 2017. From Liberation to Turmoil: Social Media and Democracy. *Journal of Democracy* 28(4): 46–59.

Tufekci, Zeynep. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

Warren, T.C., 2015. Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research*, *52*(3), pp.297-311.

Zuckerman, Ethan. 2015. Cute Cats to the Rescue? From Voice to Influence: Understanding Citizenship in a Digital Age. edited by Danielle Allen and Jennifer S. Light, 131–54. University of Chicago Press.

Zysman, J. and Newman, A., 2006. *How revolutionary was the digital revolution. National Responses, Market Transitions, and Global Technology*. (Stanford: Stanford University Press).