Puncturing the Myth of the Internet as a Commons

Mark Raymond, Ph.D.

Mark Raymond is a Research Fellow at the Centre for International Governance Innovation and has taught international relations at the University of Toronto and the University of Waterloo. He holds a Ph.D. in political science from the University of Toronto.

The notion that the Internet is a commons has gone viral. It features prominently in military thinking, including a 2011 report issued by the North Atlantic Treaty Organization (NATO).[1] It is also prevalent in journalistic thinking, in regards to the challenges of Internet governance; two recent examples from prominent news outlets illustrate the point. Bill Davidow wrote an article entitled "The Tragedy of the Internet Commons" for *The Atlantic* in May 2012.[2] Dominic Basulto wrote a blog entry for the *Washington Post* entitled "The 'Doomsday' Virus and the Tragedy of the Internet Commons" in July 2012.[3] The notion of the Internet as a commons is also evident in the thinking of Internet activists and evangelists, perhaps most notably in the declaration of the Internet Society that "the Internet is for everyone."[4,5]

Unfortunately, like many things that go viral, the idea of an Internet commons is also misleading. In its first section, this article will argue that the Internet does not possess key features associated with a commons, a concept drawn from the economics literature on the provision of public goods. The article will also assert that Internet commons arguments conflate a variety of issues with the core policy problem associated with commons management: the prevention of

destruction by overuse. In its second section the paper will advance the argument that, rather than a commons, the Internet is better understood in terms of the concept of club goods. In particular, it consists of a set of nested clubs. In this view, the analytic focus should be squarely on processes of rule-making for these various clubs, especially including rules for membership that govern inclusion and exclusion. Finally, in its concluding section, the article briefly illustrates some of the core implications of the analysis by addressing the contemporary challenges of Internet governance. Notably, the argument advanced here does not imply either the desirability or inevitability of a greater degree of control – as opposed to freedom – online. Rather, it suggests the importance of avoiding negative externalities resulting from the simultaneous rule-making efforts made by a large number of overlapping and interdependent clubs. It also suggests that treating the Internet as a series of nested clubs is a more effective means of safeguarding the openness and global interoperability typically valued by proponents of commons arguments than the assertion of declarations of principle.

Common Sense about 'the Commons'.

Concern with commons problems derives from the seminal work by Garrett Hardin, who argues that commons are extremely prone to destruction by overuse. This assertion stems from incentives created by privately-realized profits and publicly-borne costs that encourage a lack of restraint in consumption.[6] A later work by Elinor Ostrom paints a more nuanced picture. Ostrom identifies a wider range of potential outcomes than Hardin, and demonstrates empirically that human communities have shown the capacity to effectively manage various kinds of common pool resources, primarily by creating and applying rules of conduct.[7] Even if the Internet is a commons, her work implies that there is more basis for optimism than is sometimes suggested by proponents of commons arguments in the popular press.

However, the very assertion that the Internet is a commons is vulnerable to serious objections.[8] The defining properties of a commons are that "it is difficult and costly to exclude potential users" and that the good in question yields "finite flows of benefits".[9] Specifically, a commons is rivalrous and non-excludable. The Internet is neither.

A good is rivalrous if multiple people cannot use it simultaneously, or if its use by one person reduces the quantity and/or quality of the good available for others. The Internet is technically rivalrous in the sense that the computer networks on which it depends (its "physical layer") accommodate a finite amount of traffic. At peak usage times, especially in congested sections of the network, users may experience degraded performance; that is, bandwidth-intensive use by a large number of users may mean that many receive lower-quality service.[10]

In practice, however, such problems have relatively easy solutions: build more physical infrastructure, easing congestion; create more efficient protocols for routing packets, accomplishing a similar goal; and usage-based

billing can entice users to moderate consumption of bandwidth. All three of these solutions are already part of Internet governance, and while there are potential drawbacks or limitations associated with each, there is little reason to expect that combinations of such policies cannot continue to meet demand for bandwidth given appropriate investment strategies.

At worst, then, the Internet is rivalrous only at the margins and only on a local scale. From a global perspective (and especially at the content layer), the Internet more closely resembles a network good, which generates positive returns for all users as more individuals adopt it.[11] This is the opposite of a rivalrous good, as increased consumption leads to increased value.

The case for regarding the Internet as non-excludable is even weaker than the case for believing that it is rivalrous. Multiple kinds of exclusion are already occurring. First, many states already employ domestic laws to block or filter various kinds of content, including child pornography, hate speech, intellectual property violations, and political dissent. This kind of exclusion is increasingly accomplished by requiring Internet service providers (ISPs) to prevent the resolution of certain domain names and their associated Internet Protocol (IP) addresses. The so-called 'Great Firewall of China' and Iran's attempts to create a 'Halal Internet' are two of the most extensive forms of ongoing Internet exclusion.[12] However, this kind of exclusion is not limited to authoritarian regimes; the United Kingdom also plans a significant expansion of Internet filtering.[13] In the extreme, political exclusion entails states ordering the physical shutdown of Internet service. The governments of Egypt and Myanmar have both employed this tactic, albeit for limited periods of time, and there are indications the Syrian government has done the same.[14]

From a global perspective, the Internet more closely resembles a network good, which generates positive returns for all users as more individuals adopt it.

Second, some recently proposed pieces of legislation (for example, the Stop Online Piracy Act, or SOPA, in the United States Congress) have sought to strengthen copyright protections, including requiring web hosting companies, search engines, and ISPs to sever relations with websites and users found to violate copyright.[15] While such measures have met with strong resistance, it is likely they will remain on the agenda at the insistence of copyright-owning firms.

Third, Distributed Denial of Service (DDoS) attacks accomplish short-term exclusion by bombarding a targeted website with requests for information, overwhelming server capacity, and preventing servicing of legitimate requests. These attacks are relatively inexpensive and difficult to attribute to particu-

lar agents, making them an attractive option for hackers and cybercriminals as well as state agents. They are also blunt instruments, which can have significant unintended consequences such as denying access to additional, unintended targets. Finally, they allow virtually anyone with minimal technical expertise and computer hardware to engage in excluding others from the Internet. The critical point here is that the barriers to entry in terms of accomplishing limited degrees of exclusion are low; these capabilities are already in the hands of a range of actors, and their continued proliferation is highly likely.

Fourth, it is possible to exclude people from the Internet by destroying physical infrastructure (fibre or wireless) critical to their connectivity. Such attacks are imaginable both in the context of terrorism and in the context of a major military conflict. While the decentralized nature of the Internet means that terrorist attacks would be unlikely to cause widespread long-term disruption, a major military conflict could pose a significant risk to the Internet.

Other domains classified as commons include airspace, oceans, and outer space. Conflict can take place in any of the three, and some degree of exclusion is possible in each case. As a result, it might be most productive to regard commons arguments as ideal-typical in nature; real world cases may approach the ideal type to differing degrees without fully exemplifying its core features. Here Internet commons arguments fare comparatively badly for two reasons. First, exclusion is much less expensive on the Internet and in cyberspace than in these other domains. Second, unlike the other domains, cyberspace does not exist in the state of nature. Its existence is wholly dependent on manufactured infrastructure, and the vast majority of that infrastructure is privately owned.

The conclusion warranted by this analysis is that Internet commons arguments are inaccurate. An exhaustive survey of the kinds of errors made by their proponents is beyond the scope of this article, but a handful of illustrative examples may be helpful in explaining why this fallacy has gone viral.

'Common' Errors. The first possibility is analytical error. Davidow, for example, advances the claim that a tragedy of the commons exists online because online retailers "live off their bricks-and-mortar brethren" and "get fat off the bricks-and-mortar commons."[16] Note, however, that in this example the Internet itself is not destroyed by overconsumption. Rather, old-fashioned businesses are driven from the marketplace by new entrants exploiting technology to operate at lower cost. This may be regrettable, but it does not follow that it is also a commons problem. Rather, it is Schumpeterian creative destruction.[17]

Davidow also argues that "we spend hours filtering out junk email, updating passwords, and worrying about stolen identity."[18] Again, while these are problems with real costs, they are not commons problems. None of these issues entails the destruction of the Internet by overuse; rather, they are transaction costs generated by a variety of factors including the decreasing ratio of signal to noise online, and the relative ease of infiltrating individual

networked devices without detection or attribution.

Basulto writes: "we are so used to thinking of the Internet as an unlimited resource that it is almost impossible to think otherwise. But think about the debate over charging customers for their data usage… it's easy to see that the Internet is not unlimited, and that each of us is like the farmer letting their cow over-graze the commons."[19] This argument fundamentally misunderstands the commercial basis of Internet access. The very existence of price mechanisms of any kind governing access indicates the absence of a commons. Even wi-fi access offered 'free' to end-users is paid for by some entity (often a business), and purchased from a network operator. Such access is typically governed by terms of service agreements that permit exclusion in the event of improper use.

The second possibility is that a commons argument conceals or reflects a particular political agenda. At least two such agendas are readily identifiable. NATO asserts the existence of a "global commons" in cyberspace alongside the high seas, international airspace, and outer space. This cyber commons encompasses "the electromagnetic spectrum by which digital data are transmitted… as well as the infrastructure of cables and towers, satellite communications on the terrestrial side, server networks, computers, and especially the internet, that make the spectrum useful."[20] Again, the NATO argument exhibits analytical errors. It acknowledges that "there are parallel, sequestered regions of the internet… that are not part of the Commons" but argues that "even these remain linked at critical nodes." While true, this is immaterial to whether cyberspace or the Internet is technically a commons. The existence of exclusion means it is not. Strangely, the report also correctly identifies the non-rival, network effect properties of the Internet: it notes that cyberspace cannot be "used up" and that "the more people add to it, the larger and generally more useful it becomes."[21]

Given the apparent awareness of the report's authors of the conceptual difficulties in applying the notion of a commons, the decision to do so requires explanation. Fortunately, the report reveals the underlying concern. It argues that "two things are clear about cyberspace: first, the global economy and modern militaries are deeply dependent on assured access to cyberspace; and second, access is increasingly threatened by hackers (state and non-state) and malicious software ('malware')."[22] Framing cyberspace as a commons is thus a rhetorical wedge meant to ensure access to an economically and strategically vital 'space.'

Similar concerns with access can be identified in the positions taken by advocacy groups like the Internet Society, Electronic Frontier Foundation (EFF), and others. The EFF has argued that the Digital Millennium Copyright Act (DMCA) has had significant adverse, unintended consequences for consumers, competition and innovation by virtue of its mechanisms to protect copyrights and other forms of intellectual property online.[23] Similarly, the Internet Society has argued that future agreements dealing with intellectual property in the context of Internet governance should conform to a set of principles based on the goal of

preserving (as much as possible) open access to information online for purposes of education and criticism. These principles also explicitly advocate establishing multistakeholder governance of intellectual property in online contexts, and ensuring that intellectual property protection is "addressed in ways that do not undermine the global architecture of the Internet or curtail internationally recognized rights."[24]

Intellectual property effectively plays the role of a fence or enclosure around a piece of intangible property, making information more excludable than it would otherwise be, typically via a price mechanism. Properly balanced against public interests, this enclosure serves the social purpose of encouraging innovation. The Internet Society and EFF take the position that this balance is currently skewed toward permitting excessive enclosure, privileging particular narrow private interests at the expense of both other private interests and the overall public interest. It should be noted, however, that it is seductively easy to conflate the descriptive assertion that the Internet itself actually is a commons with the normative assertion that particular cultural works -- however narrowly defined -- should be freely accessible to all as the common property of humanity. It is perfectly possible to understand that the Internet itself is not a commons while also accepting various kinds and degrees of restrictions on intellectual property rights, which are derived from the kinds of balancing tests commonly applied in law. Nevertheless, such proponents of commons arguments are concerned with maintaining freedom of access online. While their reasons for preserving access clearly differ from those motivating NATO, the deployment of commons rhetoric for political purposes is analogous.

The Internet as a Set of Nested Clubs. If the Internet is, in fact, non-rivalrous and excludable, it more closely resembles what economists call a club good. Club goods include satellite television and the status that comes with a country club membership. Some clubs, however, are more exclusive than others; different clubs also have varying rules, norms, and bylaws. Clubs can be seen as similar to institutions, which scholars of international relations have studied extensively. Attempts to differentiate institutions on the basis of their properties are especially helpful, given significant political pressure for change in the modalities for Internet governance.[25]

If the Internet is, in fact, non-rivalrous and excludable, it more closely resembles what economists call a club good.

At the most general level, there are three key properties of the current Internet governance regime that merit attention: it is highly open, yet in the process of growing more closed in important respects; it is generally organized on consensus principles,

with authority emerging from technical expertise; and it is striking for the extent to which crucial governance functions are accomplished by private sector actors.

The Internet is easily mistaken for a commons because it has historically functioned as an extremely open club with very sparse rules for its members. In some ways, barriers to joining the club continue to fall rapidly: Internet access is more affordable for more people than ever before, and Internet penetration rates, especially in the Global South, continue to rise.[26] However, in other important respects, the Internet club looks not only less like a commons than it once did, but also less like a single club.

Rules increasingly circumscribe user behavior online, and pockets of the Internet now allow access only to members – with highly variable requirements for membership, ranging from unverified assertions that a user is above a certain age or resides in a particular place (often employed to restrict access to various kinds of entertainment content), to contractual arrangements on a fee-for-service basis (such as paywalls on major newspaper websites), to requirements that the user be a member of a particular offline ('meatspace') organization such as a corporation or government.

Generalizing about decision-rules for Internet governance requires caution, given that decision-making is distributed among a number of different bodies including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C). In addition, a number of private actors including network operators, information intermediaries, and content providers also perform governance functions. However, two broad trends are discernible. At least within existing governance bodies, decisions are made on the basis of an aspiration toward consensus among self-selecting groups composed primarily of technologists. Furthermore, to the extent authority emerges, it does so on the basis of technical expertise and the force of the better argument.[27]

Finally, the role of private actors is worthy of independent emphasis. Modern global governance involves an array of non-state actors, but such actors rarely perform regulatory oversight and enforcement functions. Moreover, the delegation of such roles to market-based actors raises fundamental questions of legitimacy pertaining to the appropriate boundaries between the public and private spheres.[28] Information intermediaries and network operators are increasingly exercising authoritative decision-making functions over a range of policy areas, sometimes at the behest of the state and at other times as a result of state inaction.[29]

The hybrid, distributed Internet governance regime contains a number of rule-setting venues. Decisions made in one venue by one group of stakeholders can have a potentially large impact on other constituencies not represented in the decision-making process, and individual end users necessarily belong to multiple such groups. The combination of overlapping club memberships and significant potential for negative externalities is conceptually significant. In particular, it suggests that the Inter-

net is best understood as a set of nested clubs. From its beginning, the Internet consisted of an interconnected network of networks. This fundamental architectural reality immediately evokes the concept of a set of clubs, since networks (whether physical or social) are not necessarily or uniformly open with respect to membership.

This view of the Internet as a set of rule-governed clubs is consistent with the scholarship of no less an advocate for online freedom than Creative Commons founder Lawrence Lessig. Lessig has argued that "the invisible hand of cyberspace is building an architecture that is quite the opposite of its architecture at its birth. The invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible." He is further insistent on the importance of recognizing that "the software and hardware (i.e., the 'code' of cyberspace) that make cyberspace what it is also regulate cyberspace as it is." This code "is never found; it is only ever made, and only ever made by us."[30] Notwithstanding Lessig's clear normative preference for open access to ideas and other cultural resources, he clearly recognizes that such open access is variable and contingent on social factors, including rules expressed in the form of code.

At the most basic level, Internet users are members of the club of people with Internet connections. However, they are also members of smaller clubs composed of people who access the Internet via a particular ISP, and of people who access the Internet from a particular country. It is impossible for an Internet user to avoid membership in any of these three kinds of clubs. Beyond this minimal baseline, users are typically also members of other clubs based on their personal identities and interests. These clubs function as fora for the representation of stakeholder views as well as for the creation, interpretation, and application of rules governing the Internet. They thus set conditions of possibility for a complex social and technical system. If the composition of the clubs or the ways in which they govern the behavior of their members changed, this would amount to changes in the ways in which users govern and experience the Internet.

Conclusion: Implications for Internet Governance. Understanding the Internet as a set of clubs rather than as a commons has important implications for Internet governance. First, it highlights the need to think carefully about potential externalities generated by attempts to update and apply rules for Internet governance. Court rulings, government policies, new technical standards promulgated by a particular decision-making authority, and particular enforcement actions may have unintended effects for citizens of other states, or for other Internet stakeholders. For example, a Pakistani effort to block domestic access to YouTube in 2008 led inadvertently to a global interruption in routing requests to the website.[31]

It is vital to enshrine a global commitment on the part of all stakeholders to 'do no harm' to the broader operation of the Internet. No individual club should regulate its internal matters in a fashion that prevents access to, or inter-

feres with, the operation of the Internet for other users. When such externalities occur, it is vital that they be redressed as quickly as practicable. This requires the creation of reporting systems and the acceptance of a 'responsibility to troubleshoot.' Given the uneven distribution of technical capacity to perform such work, it also means an important role for international cooperation on technical assistance and education, at least for the foreseeable future.

The principle that governance of the Internet should 'do no harm' also requires the integration of human rights concerns into decision-making processes by state and non-state actors. As the Internet becomes more central to every aspect of public life, care will need to be taken to ensure that hard-won progress on human rights is not undermined by the deployment of new technology. Doing so will not be easy. Given the importance of the Internet as a communications platform, rights of privacy and free expression are obvious areas of risk. Ensuring these rights requires thinking explicitly about the rules for the three most basic types of clubs: the club of all Internet users; the clubs comprised of each individual ISP and its clients; and the clubs of national users. Maintaining the global reach and interoperability of the Internet, and thus maximizing its value to humanity, requires ensuring that access to these clubs remains open to all, and that their restrictions on member behavior do not exceed the minimum requirements of public safety. The performance of particular governments in domestic contexts and with respect to the creation of negative externalities at the international level is likely to be highly uneven over the foreseeable future; however, Internet technology remains sufficiently new that attitudes remain malleable. Educational campaigns and citizen engagement may prove effective in encouraging governments to moderate their worst impulses.

Thinking of the Internet as a commons directs attention away from pressing issues toward a largely non-existent problem of preventing overuse.

The nested clubs approach outlined here also suggests the importance of subsidiarity (the principle that political authority should reside at the most local level consistent with effectiveness) to Internet governance.[32] At one level, this is simply a recognition of the web of existing Internet governance institutions as well as the relevance of national law and regulation to Internet-related issues. More fundamentally, however, it is a recognition that the vibrancy of any club over time depends on its ability to respond effectively and legitimately to its members' desires. This highlights the need to augment fora that enable discussion and potential revision of shared understandings about online rights and duties at each level of the set of nested clubs that comprise the Internet. At the domestic level, privacy

watchdogs and consumer protection agencies are promising candidates for these tasks. Internationally, mechanisms are relatively underdeveloped; however, the Internet Governance Forum may provide a helpful exception. ICANN's consultative mechanisms, including the Governmental Advisory Committee, may also play a useful role.[33]

Both aspects of the 'do no harm' principle pertain centrally to the theme of protecting universal access that underlies Internet commons arguments. Even if the Internet was a commons, this focus on rule-making would prove consistent with the main finding of Ostrom's work – namely, that common pool resources are managed most effectively when users create and apply social rules governing their use. In order for such rules to enjoy legitimacy, and thus generate effective compliance, it is helpful to make them in close social proximity to users. Thus, treating the Internet as a series of nested clubs is not only more empirically accurate, it is also a superior approach to protecting the characteristic of the Internet most valued by proponents of commons arguments.

Thinking of the Internet as a commons directs attention away from pressing issues toward a largely non-existent problem of preventing overuse. It also tends to encourage sensationalist thinking about an ostensibly 'inevitable' tragedy at the expense of more constructive efforts to do the hard work of international law and diplomacy, which are the key tasks of rule-making, interpretation, and application that truly matter. In particular, commons arguments risk creating paralysis by 'globalizing' Internet governance decisions as a matter of principle. In practice, Internet governance can often be done more effectively, and arguably more legitimately, at the 'club' level.

NOTES

1 Maj. Gen. Mark Barrett, Dick Bedford, Elizabeth Skinner and Eva Vergles, "Assured Access to the Global Commons," Supreme Allied Command Transformation (Norfolk: NATO, 2011), Internet, http://www.act.nato.int/mainpages/globalcommons (date accessed: 17 November 2012).

2 Bill Davidow, "The Tragedy of the Internet Commons," *The Atlantic*, 18 May 2012, available at http://www.theatlantic.com/technology/archive/2012/05/the-tragedy-of-the-internet-commons/257290/ (date accessed: 13 May 2013).

3 Dominic Basulto, "The 'Doomsday' Virus and the Tragedy of the Internet Commons," *Washington Post*, 6 July 2012, available at http://www.washingtonpost.com/blogs/innovations/post/the-doomsday-virus-and-the-tragedy-of-the-internet-commons/2012/07/06/gJQALQuoRW_blog.html (date accessed: 13 May 2013).

4 The mission of the Internet Society can be found at http://www.internetsociety.org/who-we-are/mission (date accessed: 13 May 2013).

5 Internet commons arguments are further identifiable in academic literature; for one example, see JoAnne Holman and Michael A. McGregor, "The Internet as Commons: The Issue of Access," *Communication Law and Policy* 10.3 (2005): 267-289.

6 Garrett Hardin, "The Tragedy of the Commons," *Science* 162, no. 3859 (1968): 1243-1248.

7 Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge: Cambridge University Press, 1990).

8 It is important to disentangle the argument that the Internet is not a commons from the debate over intellectual property rights in a digital age, from debate about the merits of NATO's contention that the cyber domain should be understood as a commons for purposes of securing military access, or from debate about any other substantive issue of Internet governance. Whether the Internet is a commons is ultimately an empirical question about whether it meets the definition of a commons in the public goods literature. The implications of the answer to this empirical question is a matter for additional debate; this article briefly engages such debates in order to demonstrate the ways in which the answer to the empirical question matters for (but does not determine) policy debates.

9 Elinor Ostrom, "Tragedy of the Commons," in *The New Palgrave Dictionary of Economics*, 2nd ed., Steven N. Durlauf and Lawrence E. Blume, eds., (Basingstoke: Palgrave, 2008).

10 Recent Distributed Denial of Service (DDoS) attacks on the company Spamhaus targeted Internet Exchange Points (IXPs) and resulted in significant service degradation for a large number of users. John Markoff and Nicole Perlroth, "Attacks Used the Internet Against Itself to Clog Traffic," *New York Times*, 27 March 2013, Internet, http://www.nytimes.com/2013/03/28/technology/attacks-on-spamhaus-used-internet-against-itself.html?hpw&abra=test&_r=0 (date accessed: 13 May 2013).

11 Paul Klemperer, "Network Goods (Theory)," in *The New Palgrave Dictionary of Economics*, 2nd ed., Steven N. Durlauf and Lawrence E. Blume, eds., (Basingstoke: Palgrave, 2008).

12 On China's 'Great Firewall' see Ronald Deibert et al, eds., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge: MIT Press, 2012). On Iranian Internet censorship see Simurgh Aryan, Homa Aryan and J.A. Halderman, "Internet Censorship in Iran," *Proc. 3rd USENIX Workshop on Free and Open Communications on the Internet*, Washington D.C., August 2013, Internet, https://jhalderm.com/pub/papers/iran-foci13.pdf.

13 See Nicholas Watt and Charles Arthur, "Cameron Cracks Down on 'Corroding Influence' of Online Pornography," *The Guardian*, 22 July 2013, Internet, http://www.theguardian.com/technology/2013/jul/22/david-cameron-crackdown-internet-pornography.

14 Christopher Williams, "How Egypt Shut Down the Internet," *The Telegraph*, 28 January 2011, Internet, http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html (date accessed: 14 May 2013); Stephanie Wang, "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma, *OpenNet Initiative Bulletin*, 2007, Internet, https://opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf (date accessed: 14 May 2013). On Syrian attempts to control Internet access, see Nicholas Thompson, "Why Did Syria Shut Down the Internet?" *The New Yorker*, 8 May 2013, Internet, http://www.newyorker.com/online/blogs/comment/2013/05/why-did-syria-shut-down-the-internet.html (date accessed: 14 May 2013).

15 On SOPA, and the companion "Protect IP Act" considered by the United States Senate, see Mark A. Lemley, David S. Levine and David G. Post, "Don't Break the Internet," *Stanford Law Review Online* 64 (2011): 34-38, Internet, http://www.stanfordlawreview.org/online/dont-break-internet (date accessed: 9 July 2013).

16 Davidow, "The Tragedy of the Internet Commons."

17 Joseph A. Schumpter, *Capitalism, Socialism and Democracy* (New York: Harper, 1975).

18 Davidow, "The Tragedy of the Internet Commons."

19 Basulto, "The 'Doomsday Virus' and the Tragedy of the Internet Commons."

20 Barrett, et al, "Assured Access to the Global Commons," 34.

21 Ibid., 35.

22 Ibid., 38.

23 Electronic Frontier Foundation (2010), "Unintended Consequences: Twelve Years Under the DMCA," Internet, https://www.eff.org/wp/unintended-consequences-under-dmca (date accessed: 9

July 2013).

24 Konstantinos Komaitis, "Internet Society Issues Paper on Intellectual Property on the Internet" (Reston VA: Internet Society, 2013), Internet, http://www.internetsociety.org/doc/internet-society-issues-paper-intellectual-property-internet (date accessed: 9 July 2013).

25 Please see special issue of the journal *International Organization*, especially Kenneth W. Abbott, Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter and Duncal Snidal, "The Concept of Legalization," International Organization 54, no. 3 (2000): 410-419; and, for a critical view, see Alexander Wendt, "Driving with the Rearview Mirror: On the Rational Science of Institutional Design," *International Organization* 54, no. 3 (2000): 1019-49.

26 International Telecommunication Union, "ICT Services Getting More Affordable Worldwide," Internet, http://www.itu.int/net/pressoffice/press_releases/2011/15.aspx#.UaT700D_l8E (date accessed: 14 May 2013).

27 This is essentially a case of governance by epistemic community. On epistemic communities, see Peter M. Haas, "Introduction: Epistemic Communities and International Policy Coordination," *International Organization* 46, no. 1 (1992): 1-35.

28 On the role of private actors in governance see Virginia Haufler, *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy* (Washington DC: Carnegie Endowment for International Peace, 2001); and Morten Ougaard, "Private Institutions and Business Power in Global Governance," *Global Governance* 14, no. 3 (2008): 387-403. These issues are salient in the context of the international financial system; for more information please see Geoffrey R.D. Underhill and Xiaoke Zhang, "Setting the Rules: Private Power, Political Underpinnings, and Legitimacy in Global Monetary and Financial Governance," *International Affairs* 84, no. 3 (2008): 535-554.

29 The role of such intermediaries has been addressed by the OECD. Organization for Economic Cooperation and Development (2010), "The Economic and Social Role of Internet Intermediaries," Internet, http://www.oecd.org/sti/ieconomy/44949023.pdf (date accessed: 14 May 2013).

30 *Lawrence Lessig, Code, Version 2.0* (New York: Basic Books, 2006), Internet http://www.codev2.cc/download+remix/Lessig-Codev2.pdf, p. 4-6.

31 Brad Stone, "Pakistan Cuts Access to YouTube Worldwide," New York Times, 26 February 2008, Internet, http://www.nytimes.com/2008/02/26/technology/26tube.html?_r=0 (date accessed: 14 May 2013).

32 On the principle of subsidiarity, see Andreas Føllesdal, "Survey Article: Subsidiarity," J*ournal of Political Philosophy* 6, no. 2 (1998): 190-218.

33 The suitability of ICANN, at least in its current form as the delegated authority of the U.S. government for management of the Internet root, is unclear. Recent revelations about the nature and extent of American monitoring of global Internet traffic have already further politicized questions of Internet governance. Though it is important to note ICANN has not, as yet, been implicated in these revelations, its legitimacy is at considerable risk of collateral damage so long as the principal-agent relationship with the US government persists.

34This phrase is taken from Jutta Brunnée and Stephen J. Toope, *Legitimacy and Legality in International Law: An Interactional Account* (Cambridge: Cambridge University Press, 2010).