"Security versus Freedom" on the Internet: Cybersecurity and Net Neutrality1

Marvin Ammori
Keira Poellet

SAIS Review, Volume 30, Number 2, Summer-Fall 2010, pp. 51-65 (Article)

Published by The Johns Hopkins University Press

SAIS Review vol. XXX no. 2 (Summer–Fall 2010)

"Security versus Freedom" on the Internet: Cybersecurity and Net Neutrality[1]

Marvin Ammori & Keira Poellet

As we live in an increasingly networked world, cyber-threats have become much more prevalent. The United States has promoted network neutrality and the virtues of an uncensored Internet abroad. However, new laws are being proposed which allow Internet Service Providers (ISPs) to arbitrarily block or discriminate against potentially dangerous websites. This has resulted in a challenge to the freedoms and privacy highly valued by Americans and could potentially harm America's legitimacy as a leader of open Internet across the globe. Under such an environment, what should be done to create effective and responsible policies which can not only guarantee national security, but also preserve the freedoms of Internet users?

Through the centuries, political theorists have weighed trade-offs between security and freedom, often seeking to ensure both. Today, policymakers are weighing this classic trade-off in the context of cutting-edge network technologies like the global Internet. This article focuses on one example. Policymakers seek both to secure networks from cyber-threats, including cyber/espionage, attack, and crime, and to ensure open access to information. The State Department has stated that advancing Internet freedom around the world is central to our foreign policy—subject to ensuring cybersecurity. The United States' domestic telecommunications regulator, the Federal Communications Commission (FCC), has proposed "network neutrality" or "open Internet" rules forbidding Internet Service Providers (ISPs), such as AT&T, Comcast, and Verizon, from interfering with the online choices of users. Under the rules, they can not block or discriminate against particular online technologies and websites. But some technologies and websites are security threats, so ISPs should be encouraged to help address those threats by blocking or discriminating against them. So an open Internet exception for cybersecurity has been proposed. But this exception should not swal-

Marvin Ammori is a legal scholar and advocate expert in cyberlaw, the First Amendment and telecommunications policy. Ammori is a founding faculty member of University of Nebraska-Lincoln's Space & Telecom Law LLM program and spent the summer of 2010 as a Visiting Scholar at Stanford Law School's Center for Internet & Society. Keira Poellet is a Law LLM Student at the University of Nebraska. She was formerly a Deputy Staff Judge Advocate at the U.S. Air Force and adjunct instructor at Embry-Riddle Aeronautical University.

low the rule: some ISPs have claimed a right to block competing, legitimate technologies in the name of ensuring users' "security."

Neither the FCC nor the White House has provided the necessary details to mediate this potential conflict between Internet freedom and cybersecurity. The FCC has proposed a cybersecurity exception to its network neutrality rule,[2] and President Obama states he will ensure that his cybersecurity policies will not conflict with the FCC's network neutrality rule,[3] but neither proposes details or even a framework for determining those details.

This article aims to fill that gap. It argues that the key challenge arises from the presence of dynamic, rapidly changing threats coupled with a lack of trust among key stakeholders. In light of this dynamic yet distrustful environment, this article proposes a resolution—one which is common to constitutional law—of emphasizing not rigid substantive rules but inclusive institutional processes, organized with checks and balances, for flexibly adapting rules to dynamic technological developments.

This article is organized in three parts. First, it lays out this nation's policies for cybersecurity and for Internet freedom. Next, it discusses the tension between the two policies and proposes a framework for thinking about resolving that tension. Finally, the paper looks at current and proposed law and proposes some modifications to mediate this tension.

United States Policy Favors Both an Open Internet and a Secure Internet

The current administration has announced that both cybersecurity and network neutrality are key national goals.

Ensuring Cybersecurity

Cybersecurity is a presidential-level policy goal. In January 2008, President George W. Bush issued a still-classified national security and homeland security directive to launch the nation's Comprehensive National Cybersecurity Initiative (CNCI).[4] The following year the administration issued the Cyberspace Policy Review summarizing a 60-day review of cybersecurity policy. The Review set out initial near-term and mid-term action items for securing cyberspace. Central to the plans was anchoring leadership for cybersecurity within the White House, particularly by appointing a coordinator for cyber issues who would answer to both the National Economic Council and the National Security Council. The military secures its own networks under the leadership of the recently-launched United States Cyber Command, whose commander is dual-hatted as the head of the National Security Agency. The Department of Homeland Security has the lead on securing federal government networks.[5] Finally, private companies secure their own networks. But insecurities in one network can affect another; for example, military and government services often share the same public-Internet infrastructure as private companies, and rely on private web services that may be attacked or compromised. Further, cyber attacks routed through insecure private networks can attack military networks, and vice versa. As a result, these dif-

ferent authorities have to work together to assure each other's security.

Cybersecurity threats are real and constant. Today's most serious threats do not come from the proverbial bored lone hacker in high school but from sophisticated organized crime syndicates and, perhaps, nation states. For example, when Google recently made headlines by announcing its servers had been subject to corporate espionage, apparently directed from Chinese sources, nobody suspected teenage hackers were behind the attack.

Today's most serious threats do not come from the proverbial bored lone hacker in high school but from sophisticated organized crime syndicates and, perhaps, nation states.

Cybersecurity threats can be classed into three broad categories: (1) espionage (accessing government, financial, or corporate information); (2) attacks (denial of service attacks, sabotage of electrical grids, air traffic controls, or military command communications); and (3) other crimes (identity theft, fraud, and other crimes). Attempted espionage is a persistent threat; military, governmental, and corporate records are constantly subject to intrusion.[6] On the other hand, "attacks" involve attempts not just to access and steal valuable information, but also to damage or interfere with computer systems. For example, denial-of-service attacks are common, and aim to deny someone's ability to use a server, computer, or other network resources. Distributed denial-of-service (DDOS) attacks generally involve thousands of computers, which generally overload a network resource like a server with requests for information. As a result of the requests, legitimate users are unable to access the company's site. To analogize to the phone network, a DDOS would resemble hundreds of people calling a company just to tie up the lines and keep legitimate callers from getting through to place orders or seek help. With DDOS, rather than convincing hundreds or thousands of people to go to the same website, actors use a virus or worm to infect thousands of computers, and then later give those compromised computers orders to request information at the same time from the same target site. Such a network of infected, controlled computers is often called a "botnet." Distributing spam often works the same way; however, the botnet computers have orders to send unwanted emails instead of bombarding servers with requests.

As a result of malware like viruses and worms, the weapons of bad actors are often our own computers, with a substantial number of compromised computers residing in the United States.[7] Criminals sometimes deploy DDOS attacks for extortion, as companies subject to such attacks have been willing to pay to stop the attack.[8] Other times, cyber attacks are deployed for military objectives. In 2008, the Russian government and closely affiliated criminal networks were allegedly responsible for cyber attacks on Georgian government sites in the days leading up to Russia's land assault on Georgia.[9]

While cybersecurity may be improved through simple distributed measures, such as convincing network users to chose passwords properly (and not to share them) and dissuading software companies from "shipping [products] now, patching [security] later,"[10] ISPs can also independently add a layer of cybersecurity protection. Simply put, technically, ISPs can monitor traffic patterns across a wide number of connected computers, something that individual users cannot do (unless those users are sophisticated enough to create or join virtual networks for cybersecurity, as few are).[11] By monitoring those traffic patterns, an ISP can determine if many individual users are requesting information from the same servers, and thus engaged in an apparent DDOS. Or, an ISP can determine if certain computers are constantly sending emails, and therefore part of a spamming botnet. Understanding which computers are involved in attacks or spamming, the ISP can then disconnect those computers from the network or can monitor all the data sent from the computers and block the apparently attacking or spamming data. ISPs are often hesitant to take these actions because there will be false negatives, where people are wrongly identified as part of a botnet, which could result in liability or, simply, angry customers.[12]

As a matter of policy, some have argued that ISPs should play an important role in cybersecurity for several reasons. First, ISPs can help address the technical aspect of some attacks.[13] ISPs can identify spamming computers and botnets, because of access to traffic data, and address them. Second, ISP involvement can be cost-efficient. Compared to individuals and smaller web companies, ISPs would have economies of scale for cybersecurity, in terms of hiring staff and investing in technologies. It would likely be less expensive in terms of time and resources, at least in some circumstances, to address a known problem through ISP network filtering, rather than by requiring all individual users to take the time to upgrade their antiviral software or download a particular patch. Third, ISPs can more easily identify threats that users would not identify. A user may not even know his or her computer is part of an active botnet because botnets are often designed to operate "silently" in the background of an infected computer. Meanwhile, ISPs monitor traffic patterns, so they can identify computers silently sending spam or DDOS requests. Fourth, and somewhat related, ISPs sometimes have better security incentives than users. If, thanks to a worm or virus, a user's computer accidentally joins a compromised computer army for DDOS or spam, that user has little incentive to stop the DDOS or spam affecting *other people's* computers. This represents a misalignment of incentives, well-known to economists as a "negative externality." The user does not bear the costs imposed by others when his or her computer spams or attacks other computers. In contrast to the user, the ISP may sometimes have a greater incentive to address the infection, if only to conserve network bandwidth otherwise going to spam and false requests on its own network.

Nonetheless, the economics literature points to many reasons why ISPs often underinvest in security. The ISPs, like other private actors, follow their own economic incentives to secure their own networks. In keeping with the reality of negative externalities, ISPs have little incentive to block spam

going to other networks because outgoing spam is, by definition, someone else's problem.[14] In addition, consumers may complain over false positives, for example, when their computers are quarantined from the network or a favorite application is blocked because the ISP wrongly determines a security problem.[15] As a result of ISPs underinvesting in security, some have proposed to impose requirements on ISPs, such as liability for outgoing attacks from computers on the ISP's networks.[16]

Ensuring the Open Internet

President Obama, the Democratic congressional leadership, and members of the FCC have all repeatedly voiced their support for network neutrality.[17] While campaigning for the Presidency, Obama promised he would "take a backseat to no one" in his support for network neutrality.[18] In early 2009, Congress tied stimulus funds for broadband networks to the imposition of network neutrality conditions on the receiving ISPs.[19] Later, in September of 2009, Obama's FCC Chairman, Julius Genachowski, proposed a network neutrality rule and continues to accept public comment on all aspects of the rule, including the security exception.[20]

The motivation for a non-discrimination principle is to ensure a level playing field among speakers (e.g., news sources, bloggers, Twitter users) and innovators on the Internet. For this reason, a proposed rule forbidding ISPs from discriminating among different websites and applications is central to the FCC's proposed network neutrality framework. If an ISP (like AT&T) could discriminate against FoxNews.com and in favor of a competitor, like CNN.com, or against Skype and in favor of Google Voice, then that ISP would be choosing the online winners and losers in speech and innovation—a choice better left to individual consumers. By influencing speech and the marketplace decisions of users in this way, ISPs would impede robust speech and slow down economic innovation.[21]

If an ISP (like AT&T) could discriminate against FoxNews.com and in favor of a competitor, like CNN.com, or against Skype and in favor of Google Voice, then that ISP would be choosing the online winners and losers in speech and innovation—a choice better left to individual consumers.

Beyond domestic policy, Secretary of State Clinton has announced that ensuring an open Internet is now a major foreign policy objective.[22] In making the announcement, Secretary Clinton criticized governments around the world for censoring social networks and blogs. In addition, censorship impedes American companies' ability to compete fairly in international trade, something the censorship of Google results highlights.[23] Crafting a foreign policy to address censorship is more complicated than it seems. Nations may require ISPs to censor, may encourage such censorship,

and, at any rate, grant ISPs considerable discretion in determining what to censor and what not to censor. As a result, some characterize Chinese censorship as being "outsourced" to ISPs determining what specifically to block.[24] From the perspective of democratic debate, it matters little whether censorship comes from governments or from ISPs with close relationships to governments. As a result, the U.S. must favor global network neutrality. According to the Secretary's top advisor on using technologies to further our diplomatic efforts, in favoring global network neutrality, the United States would lose credibility if it allowed its own ISPs domestically to interfere with users' choices.[25] So domestic network neutrality advances our foreign policy goals.

In response to the present administration's claims, the largest ISPs make two relevant arguments. First, ISPs argue that network congestion during times of peak congestion is most appropriately addressed through internal network management, rather than by "overinvesting" in increased capacity to meet those rare peak moments. Network neutrality advocates concede that congestion-management is acceptable, but only so long as ISPs manage congestion in an *application-neutral* way. That is, for network neutrality advocates, ISPs cannot target and discriminate against certain applications.[26] For example, an application-neutral policy might take the following form: if a user consumes disproportionate bandwidth, his or her overall capacity could be limited, but the user chooses which applications to use with that capacity.

Second, ISPs argue that even if application-neutral management makes sense for congestion management, it makes no sense for security. The point of effective security is to discriminate against some content (such as spam) and applications (such as worms and DDOS attacks). Network neutrality advocates generally agree here; their interest is to ensure that users are able to access legal, consumer-requested services on a level playing-field.

Yet, for several reasons, ISPs cannot be completely trusted to target Internet traffic based upon a security justification. A recent doctorate dissertation, on the role of ISPs in mitigating botnet activity, explains:

> ISPs might be tempted to use [a system to monitor and block traffic] as an opportunity to classify user traffic for their own revenue-generating applications (i.e., targeted advertisement). . . . In extreme cases, they might use their newly acquired powers to disconnect users or traffic that they do not wish to carry, e.g., by labeling it malicious or risky. (This concern touches on a current debate regarding the network neutrality principle.)[27]

A real world example of ISPs' incentives to mischaracterize anticompetitive behavior as network management is the famous example of Comcast, in 2007, when it admitted to interfering with legitimate peer-to-peer transfers, including those used by competitors, but claiming that its application-specific interference was necessary to manage congestion. Comcast could have similarly attempted to justify its application-specific interference based on the security threat from peer-to-peer applications, as some blocked applications, no doubt, would have contributed to security threats. Yet, network

neutrality advocates would argue for some check on ISPs to ensure their "management" for security does not generate overly burdensome effects on legitimate content and applications.

In addition, ISPs may block legitimate applications unintentionally. A clear distinction between congestion management and security management may not exist in practice. In real time, at light speed, network engineers cannot always determine if a sudden, particularized spike in demand comes from a DDOS targeting particular sites or from actual consumer interest. For example, when Michael Jackson died, engineers would have seen a sudden spike in requests, from millions of computers, going to news sites. Consider also a new video technology, one that achieves sudden popularity for a weekly show. Engineers may confuse consumer demand for an attack and end up treating the consumer interest like a DDOS. As a result, the ISP has accidentally engaged in application-specific behavior violating the network neutrality rule—with application-specific management of a consumer application. While this is just one example where the distinction between congestion and security is more apparent than real, it could be a common one.

Finally, ISPs' interventions can sometimes lead to greater insecurity. ISPs once partnered with a company run by spyware founders to spy on DNS queries, to capture the information, and to sell the information for targeted advertising, which many found problematic from a security perspective;[28] this company had 30 U.S. customers covering 10 percent of Internet users, and the activity resulted in heated Congressional hearings.[29] Many more ISPs resolve mistyped DNS requests to an ISP-advertiser landing page, which has been criticized for introducing major vulnerabilities.[30]

Tension Between an Open Internet and Cybersecurity

Because of the potential need for ISPs to engage in application-specific targeting of security threats, the tension between network neutrality and cybersecurity is well-recognized in government policy and is referenced in both the FCC network neutrality proposal and the *Cyber Policy Review*.

In order to resolve the tension, authorities must address both dynamic threats and a lack of trust among key partners. These threats are dynamic because bad actors adopt new technologies quickly, which results in a rapid-fire technological arms race between good and bad actors.[31] At the same time, parties lack trust in one another across almost every relationship. First, the public distrusts the government—an American tradition of sorts. For example, groups have complained about cybersecurity proposals granting the President emergency authority to designate and control particular networks in times of war or emergency.[32] The "warrantless wiretapping" controversy, in which many believe that the Bush Administration ordered the National Security Agency to overstep then-current laws, may have increased public distrust for government cybersecurity efforts.[33] Further, ISPs may not trust the government, as many ISPs generally disfavor government regulatory mandates, some of which may impede efficiency and reduce profits. ISPs

also likely fear a public relations backlash for working too closely with government—for example, many experienced some backlash over "warrantless wiretapping."[34] Similarly, many civil liberties groups do not trust the ISPs. This distrust arises partly from the FCC's conclusion in 2008 that the nation's largest landline ISP, Comcast, was not perfectly candid with the public and the agency in the FCC's most important network neutrality case to date.[35] Moreover, just this year, another ISP, RCN, admitted to engaging in similar conduct to Comcast's, having not disclosed the conduct until caught.[36] Consequently, consumer groups and technology companies currently suspect ISPs of managing traffic in undisclosed ways. Not surprisingly, these same groups would likely fear that ISPs could secretly use their "security" tools to disadvantage targeted applications.

Meanwhile, the government cannot trust the public or ISPs—at least not entirely. The public network includes both (few) actors who deliberately engage in malicious activities, and (many) others whose computers are infected and unknowingly malicious. As discussed, ISPs will rationally mitigate threats affecting their own self-interest, but ISPs have little incentive to mitigate the outgoing threats to competitors. Government cannot trust outcomes produced by this kind of market.

Of course, these parties can work on building trust among one another—including a public education plan to make the public better understand and trust governmental cybersecurity efforts. But trust-building will likely not be enough. Each party will end up following some iteration of the Reagan maxim: "trust, but verify." As a result, this dynamic threat environment will remain subject to some distrust among the relevant parties.

The pairing of these challenges renders policy making more complicated. In a static environment, parties lacking trust could specify rules for unchanging security threats. Yet, in a dynamic environment, threats change quickly, making specified rules quickly obsolete. Conversely, in dynamic environments with trust among parties, responsibilities may be divided between parties and broad discretion may be granted to each party. When relationships are characterized by distrust, however, parties are unlikely to grant such vast discretion, and, as a result, neither the government nor the ISPs will possess the flexibility to address dynamic threats.

For guidance, we can turn to America's greatest policymakers: the founding fathers. Madison, Hamilton, and others went to the Constitutional Convention to establish a constitutional framework for a young nation needing to address *dynamic* external and internal threats (ranging from the United Kingdom to the Whiskey Rebellion), despite deep popular *distrust* in one another—and in a centralized government. Facing both dynamic threats and wide distrust, they also had to balance security and freedom within a constitutional regime, and their solutions provide a particularly useful lesson on which we have often relied.

To address dynamism and distrust, we should employ both substantive safeguards, including somewhat general rules, and procedural safeguards, namely divided authority and checks and balances. This combination of substance and procedure would provide better flexibility, legitimacy, and

policy guidance than would overly-prescriptive rules and a process without diverse parties constantly checking one another.[37]

First, somewhat more general rules are preferable to more prescriptive rules. Rules could set out the general principle, clarify some "easy cases" or "expected cases" as either prohibited or encouraged—indicating, perhaps, that the security response should not overly burden legitimate traffic, as in the Comcast and DNS scenarios above—and then address the harder cases through ongoing policy making based on handling real threats and incorporating the lessons learned from those experiences. The benefit of this approach is to provide some guidance—in terms of both principle and particular, expected challenges—without overly constraining engineers' ability to address evolving and unexpected challenges. The primary drawback is the flip-side of the coin; many hard issues are punted to later and not decided *ex ante* in the rule. While this drawback is considerable, it is also largely unavoidable under any policy. In a dynamic environment, no other policy decision could better address this downside. A highly prescriptive rule cannot predict and address those hard issues, and might only serve to create an immediately ossified framework, which bad actors can work around.[38] Meanwhile, we can mitigate the primary drawback of unresolved hard issues by providing a credible process for addressing those hard issues when they come up.

Second, the checks and balances of divided authority will help create legitimacy, trust, and sound policymaking. In terms of legitimacy, even though parties may continue to distrust one another, they could easily come to trust a *process* that includes several parties. That is, in the words of James Madison, while they may distrust each others' ambitions, they may trust a process designed where "ambition counteracts ambitions."[39] Regarding trust among the parties themselves, a divided-authority process will require parties to exchange information, to take into account other viewpoints (if only to make more persuasive arguments), and to simply develop personal connections based on some measure of trust. This increased trust will help all parties work through new challenges. Finally, sound policymaking could benefit from diverse voices at the table. Decision-making often benefits from diversity of views,[40] and we can expect more diverse views from a group of actors coming from different backgrounds, expressing different institutional concerns, and exhibiting different expertise. The primary drawbacks include the potential for gridlock, slow decision making, and worse decisions based on "too many cooks in the kitchen" or compromise thinking. Yet, again, no solution is better, and these drawbacks can be mitigated. No solution is better because, without divided authority, only a few key players make decisions, resulting in a lack of legitimacy—which itself tends to result in parties ignoring and government under-enforcing a law. In addition, those parties excluded from the process may agitate to change the law, perhaps to focus on *ex ante*, substantive limitations, which have drawbacks we have already discussed.

The drawbacks in this area can also be mitigated. As long as we do not adopt flawed models encouraging gridlock (some would suggest, the

United States Senate and its filibuster rules), gridlock can be mitigated. A vote could decide the matter, and it could do so legitimately if parties feel the process is fair. Slower decision making is simply a fact of divided authority. The question here is whether divided authority would be so slow as to outweigh other benefits. This is an empirical question. But, again, it seems that so long as the process encourages decision making and not gridlock, the process will not be fatally slower than the alternative—a less inclusive decision making group.

Finally, some would argue that diverse contributors could lead to worse decision making. After all, "the engineers," especially those who know a network best, can handle the technological aspect of cybersecurity; contributions from debating lawyers and policymakers certainly will not improve the engineering decisions and will likely muddy them through non-engineering considerations and compromises. This objection is empirical, and evidence is unavailable. We tend to believe that often two minds are better than one,[41] and, as some have tried to demonstrate, that decision making benefits from deliberation.[42] More importantly, questions of cybersecurity and Internet freedom are not merely engineering decisions—they are also policy calls. We must make policy decisions—weighing individual freedom, economics, and public safety—when deciding how to resolve cybersecurity challenges. Moreover, few people are expert in all aspects of cybersecurity challenges. Some combination of expertise from across the legal, military, and technological fields is thus necessary to produce politically and technologically effective solutions.

Evaluating Proposals to Modify Current Law

In this section, based on the framework laid out above, we discuss some aspects of operative and proposed law. Proposed laws include the FCC network neutrality rule, aspects of the Cyber Policy Review, over forty proposed cybersecurity bills, and the operative "cybersecurity" law found in a law drafted long before the Internet was invented—the Communications Act of 1934.

First, the *Cyberspace Policy Review* merely notes that despite network neutrality objectives, delivery of emergency communications should be ensured. To do so, those communications may need technical priority (rather than mere "neutrality" with other communications), and ISPs must ensure that attacks do not render networks unusable, even for prioritized traffic. The *Cyberspace Policy Review*, because it is merely an initial report, provides no substantive guidance. It proposes, however, an important procedural safeguard: to "[d]esignate a privacy and civil liberties official to the NSC cybersecurity directorate." This official would institutionally represent the interests of civil liberties on the directorate and would come from a background reflecting a deep commitment to civil liberties and privacy. To this end, President Obama appointed Tim Edgar, previously of the American Civil Liberties Union, and long a fierce critic of the privacy and civil liberties aspects of government programs.

As might be expected, appointing this official strikes us as a sound way to balance the need for dynamic discretion with improving trust among parties. As part of the civil liberties portfolio, this official should consider network neutrality issues and coordinate with an FCC network neutrality official in designing White House-level policy on cybersecurity. In addition, this official should publish reports informing the public of substantive principles that have guided the official's analysis, much like an agency policy statement analyzing precedent to provide public guidance. These reports can be important both in terms of public transparency to foster greater trust among diverse groups, and to ensure consistent decision making over time.

Second, the FCC's network neutrality proposal lays out a process of adjudicating potential violations of network neutrality with minimal substantive guidance. The heart of the rule turns on the undefined term, "reasonable."[43] To provide some guidance, the FCC stated that its rule would not limit an ISP's "ability to deliver emergency communications or to address the needs of public safety or national or homeland security authorities, consistent with applicable law." The proposal similarly contemplates that an ISP can "prioritize certain types of traffic in the case of an emergency" for the benefit of first responders.[44] The FCC specified that ISPs could seek declaratory rulings in advance of deploying a technology or tactic.

None of these policies is explained in sufficient detail. The FCC does not describe who can determine when a communication is an emergency; can the ISP unilaterally decide or must a government agency be involved? At what level must the agency be involved, if at all? We suggest that a government agency be involved, that general policies be published for public transparency and involvement, and that the policy decision should be rendered at a fairly high level (while implementation would obviously fall to a delegated officer).

Further, we believe the FCC should draw inspiration from the White House and appoint a network neutrality official—at least for the next several years—to serve as a liaison as foundational questions are addressed.

Finally, who could file in the declaratory-ruling proceeding (third-parties?) and who could issue the rulings (the full Commission or a delegated official)? Again, we favor a more inclusive process, with transparency and the right of third-parties to weigh in; we argue these *policy* decisions ought not be delegated to specialized officials in the first instance.

Further, we believe the FCC should draw inspiration from the White House and appoint a network neutrality official—at least for the next several years—to serve as a liaison as foundational questions are addressed. This official could convene discussions among ISPs, the government and military, and network neutrality advocates. Along the same lines, several

industry participants have proposed a small, industry-only working group for network neutrality generally.[45] Whatever the merits of that proposal, a *broad* working group of industry, government, and users could prove helpful *specifically* on cybersecurity matters. This group could serve as advisors to the FCC official.

Moving from the White House and FCC, we turn to Congress. Congress has over forty proposed cybersecurity bills, and this article cannot address even a small subset of them. The most controversial aspects of these bills center on granting the president emergency authority to direct ISPs to close particular Internet links, as well as to commandeer parts of the network. Critics refer to this authority, not quite accurately, as an Internet "kill-switch." Interestingly, the operative law in our nation already has a "kill-switch," though it is a conditional one. The current legal framework for balancing cybersecurity and nondiscrimination is codified in the 1934 Communications Act, as amended, at 47 U.S.C. § 606. That section—"War Emergency—Powers of President"—grants the president broad authority to require priority for certain traffic and to confer ISP immunity for that priority during wartime. The president is also empowered to take control of wireless networks during war, threat of war, or emergency and to control wireline networks during war or the threat of war, but inexplicably not during an emergency.[46] The President's power to appropriate wireline communications expires six months after the end of war or threat of war, or earlier if designated by Congress in a joint resolution and it is subject to the provision of just compensation.

The most controversial aspects of these bills center on granting the president emergency authority to direct ISPs to close particular Internet links, as well as to commandeer parts of the network. Critics refer to this authority, not quite accurately, as an Internet "kill-switch."

In sum, the existing law creates a system of vast discretion and a number of checks and balances, not all of which are appropriate today. Some checks and balances go too far. For example, it seems absurd that, under limited conditions, the president cannot order prioritization during a national emergency.[47] In addition, the requirement of paying "just compensation" could require the government to pay unpredictable compensation, even when appropriating an attacked network may increase its value. Finally, current law treats wireline and wireless networks differently, granting the president more authority to appropriate wireless networks. The discrepancy may make sense: wireless networks may emit signals that interfere with government signals. Yet, Congress should reflect on the discrepancy, and perhaps tailor the presidential checks and powers to that particular wireless concern.

Other checks, however, likely do not go far enough. The president should be precluded from unilaterally declaring an emergency, as declaring an emergency confers the power to appropriate Internet networks. Congress should play a role by at least providing certain requirements that must be met in order to be a "cybersecurity emergency." Indeed, the latest cybersecurity bills incorporate a very important limitation: requiring Congress to authorize the president to declare a cybersecurity emergency and appropriate Internet systems for more than 120 days.

As a result, existing and proposed law are on the right track, attempting both substantive and procedural safeguards, though both can be better tailored for the challenge.

Conclusion

Policymakers have long debated how to balance security and freedom in the Internet. Because the security threats are dynamic, discretion for government and ISPs is necessary, but that discretion should be checked with trust-ensuring procedural safeguards. This article takes a first step in proposing that policymakers incorporate both substantive and procedural checks to address these challenges—to keep our networks both free and safe.

Notes

[1] The views expressed in this article are those of the authors and do not reflect the official or unofficial policy or position of the United States Air Force, Department of Defense, or the U.S. Government. We thank David Solheim and Robb Topolski.

[2] Preserving the Open Internet; Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking, 24 FCC Rcd 13064, 13102, 13112, 13115-16 (2009).

[3] President Obama said, in discussing cybersecurity: "I remain firmly committed to net neutrality so we can keep the Internet as it should be—open and free." Barack Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," May 29, 2009, The White House. The President's Cyberspace Policy Review action plan items included to: "[d]evelop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality." *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 29, 2009, p. 38.

[4] National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (NSPD-54 / HSPD-23), discussed at The Comprehensive National Cybersecurity Initiative, The National Security Council: Cybersecurity, http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[5] The legal framework for cybersecurity depends partly on the bad actor (criminal or nation state), but defense often requires real-time response, long before the defender can attribute an attack to a particular source. See, e.g., The Council of Europe Convention on Cybercrime, Nov. 23, 2001, ETS No. 185, available at http:// conventions.coe.int/Treaty/EN/Treaties/Html/185.htm; Scott Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 27 *Berkeley J. Int'l L.*, 192, 193 (2009); Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," 37 *Colum. J. Transnat'l L.* 885, 894 (1999).

[6] William A. Owens et al., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities (Washington, D.C.: National Academies Press, 2009), at 227, 261.

[7] Byron Acohido, "U.S. Replaces China as Top Source of Malicious Servers," USA Today Technology Live, June 3, 2010.
[8] Fatal System Error: Interview with Joseph Menn, Kojo Nnamdi Show, June 22, 2010, http://thekojonnamdishow.org/shows/2010-06-22/fatal-system-error.
[9] Jon Swaine, "Georgia: Russia 'Conducting Cyber War,'" Telegraph (UK), August 11, 2008.
[10] Ross Anderson, "Why Information Security is Hard—An Economic Perspective," 17th Annual Computer Security Applications Conference (2001), at 2.
[11] Herdict, www.herdict.org.
[12] Jonathan Zittrain, The Future of the Internet and How to Stop It (2008), at page 166.
[13] I thank Robb Topolski for discussing some of the technical issues with me.
[14] John Dunn, "ISPs Reluctant to Filter Outbound Spam," Tech World, June 9, 2010.
[15] Hadi Asghari, "Botnet Mitigation and the Role of ISPs: A Quantitative Study Into the Role and Incentives of Internet Service Providers in Combating Botnet Propagation and Activity," (Thesis: Faculty of Technology, Policy and Management. Delft University of Technology), 2010.
[16] Asghari, "Botnet Mitigation," at 151-52 (and sources cited).
[17] Tim Karr, "Obama: Firmly Committed to Net Neutrality," Save the Internet.com Blog, May 29, 2009
[18] "Video: Barack Obama 'I will take a back seat to no one in my commitment to Net Neutrality,'" https://www.freepress.net/obama_net_neutrality.
[19] Leslie Cauley, "What's 'Broadband'? Billions in Stimulus Funds Are at Stake," USA Today, April 7, 2009.
[20] Preserving the Open Internet; Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking, 24 FCC Rcd 13064, 13102, 13112, 13115-16 (2009).
[21] Barbara van Schewick, Internet Architecture and Innovation (2010); Marvin Ammori, "Beyond Content Neutrality: Understanding Content-Based Promotion of Democratic Speech," 61 *Fed. Comm. L.J.* 273 (2009). Supporters of network neutrality, therefore, include both civic organizations (from the Christian Coalition to MoveOn and Free Press) and for-profit corporations (from Google to Zipcar to Union Square Ventures).
[22] Hillary Rodham Clinton, Secretary of State, "Remarks on Internet Freedom," Washington, DC, January 21, 2010.
[23] See, e.g., Tim Wu, "The World Trade Law of Internet Filtering," SSRN Working Paper, May 3, 2006.
[24] "Audio: Interview with Dr. James Mulvenon on China and Cybersecurity," Center for Strategic and International Studies, April 2, 2010.
[25] Marvin Ammori, "Net Neutrality at Home is Key to Promoting Freedom Abroad, Say White House, State Department," Huffington Post, November 24, 2009.
[26] For example, the FCC found that Comcast had essentially violated network neutrality policies for singling out and discriminating against peer-to-peer applications. In response, Comcast moved to a practice of managing individual usage.
[27] Asghari, "Botnet Mitigation," at 153.
[28] Robb M. Topolski, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," June 18, 2008.
[29] "NebuAd," Wikipedia, *http://en.wikipedia.org/wiki/NebuAd*. This page was fairly meticulously updated during the controversy to include all ISPs that partnered with, or ended partnerships with, the company.
[30] Ryan Singel, "You Don't Want ISPs to Innovate," *Wired: Epicenter*, June 24, 2010.
[31] *Cf.* William H. Lehr et al., "Scenarios for the Network Neutrality Arms Race," 1 *Int'l J. Comm.* 607 (2007).
[32] J. Nicholas Hoover, "Senators Say Cybersecurity Bill Has No 'Kill Switch,'" *InformationWeek,* June 24, 2010.
[33] Ellen Nakashima, "Telecom Firms Helped With Government's Warrantless Wiretaps," *Washington Post*, August 24, 2007.
[34] Ibid.

[35] In the Matters of Formal Complaint of Free Press and Public Knowledge Against Comcast Corporation for Secretly Degrading Peer-to-Peer Applications, Memorandum Opinion and Order, 23 FCC Rcd 13028, n.31 (2008) ("Comcast's statements in its comments and response to Free Press's complaint raise troubling questions about Comcast's candor during this proceeding."). One of the authors, Marvin Ammori, was a lawyer for Free Press on this case.
[36] Mehan Jayasuriya, "RCN Settlement Demonstrates the Perils of ISP Self-Regulation," Public Knowledge Policy Blog, April 20, 2010.
[37] This reasoning is not necessarily relevant for all aspects of the network neutrality debate. While ISPs sometimes describe applications as nefariously using too many network resources, applications have incentives to be efficient and to limit the bandwidth they consume. Moreover, the "threat" of innovative applications needing more capacity is one we generally solve cost-effectively in tech markets and even the ISP market with investments in more capacity. Technology generally becomes faster and cheaper every year, maintaining the affordability of investments in capacity. Though ISPs could possibly make more money by cutting investment costs in capacity, car manufacturers could make more money by skimping on safety or fuel-efficiency. As a matter of policy, we could decide that investments in capacity are necessary. At any rate, the general network neutrality challenge is different from the challenge of addressing cybersecurity in a network neutrality framework.
[38] While, in theory, the prescriptive rules could also be changed often, providing flexibility, the administrative and coordination costs of changing an FCC rule are fairly high. These costs would be lower with a framework designed specifically to have flexibility, and therefore fairly low-cost policy tweaking.
[39] James Madison, Federalist 51.
[40] Cass R. Sunstein, Why Societies Need Dissent (2003).
[41] *Cf.* Yochai Benkler, The Wealth of Networks (2005).
[42] Bruce Ackerman & James S. Fishkin, Deliberation Day (2004).
[43] Cecilia Kang, "Biggest Net Neutrality Boosters Question FCC Proposal," *Washington Post: PostTech*, November 2, 2009.
[44] Preserving the Open Internet; Broadband Industry Practices, GN Docket No. 09-191, WC Docket No. 07-52, Notice of Proposed Rulemaking, 24 FCC Rcd 13064, at 13112 (2009).
[45] Richard Whitt (Counsel for Google), Broadband Internet Technical Advisory Group Poised for Launch," *Google Public Policy Blog*, June 9, 2010.
[46] Of course, in 1934, the technology would require almost an "all-or-nothing" takeover of the communication lines, while today's technology could allow the president priority communications during an emergency without completing taking over all communications lines.
[47] Of course, the president would need to weigh many factors in exercising that power, should the president receive this power. For example, while emergency communications are better assured delivery, calls to and from loved ones may be dropped or delayed, causing anguish and panic in areas far from the emergency.