# Northwestern---Round 4 vs. Samford GT

## 1AC

### 1AC---Plan

#### Plan: The United States federal government should prohibit anticompetitive business practices in the delegation of generic Top-Level Domains by the private sector.

### 1AC---Internet Freedom ADV

#### Advantage One is Internet Freedom---

#### ICANN, the body governing allocation of internet domain names, shifted its allocation of generic Top-Level Domains, or gTLDs, to allow companies to buy domain names that mirror their trademarks, allowing explicitly anti-competitive deal-making

Nelson Drake 18, J.D. from American University’s Washington College of Law and a B.A. in Political Science from Georgia College and State University, “Going Rogue: The National Telecommunications And Information Administration's Transfer Of IANA Naming Functions To ICANN”, 3 Admin. L. Rev. Accord 83, 2018, lexis

II. THE IANA TRANSFER AND WHY IT MATTERS

As noted above, one of ICANN's powers with respect to the DNS and the IANA functions is its ability to adjudicate disputes about the existence of trademark rights in a domain name via the UDRP. This power was relatively uncontroversial because the UDRP's standard for determining the existence of trademark rights mirrored the USPTO's. However, **ICANN's introduction of its new TLD program has created new problems** because it permits trademark owners to purchase TLDs that mirror their trademarks. This is an issue because the prevailing policy of both ICANN and the USPTO was that TLDs are, generally, generic. 69 For example, under the Legal Rights Objections (LRO) period of the TLD application process, most trademark owners are unable to prevent the delegation of a TLD that matches their trademark. 70 These LRO decisions have since been supported by courts intent on maintaining the current policy. As a result, **plaintiffs have been unable to successfully bring a case against ICANN regarding the delegations of gTLDs.**

A. Image Online Design and the Trademark Perspective

The non-trademarkability of gTLDs was a primary issue in the case *Image Online Design, Inc. v. Internet Corp. for Assigned Names and Nos.*, which revolved around the delegation of the ".web" gTLD. 71 Image Online Design (IOD) is the operator of a registry for the ".web" TLD on a non-authoritative DNS, which means that it is not readily searchable by users without preconfiguring  [\*95]  their web browser. 72 However, this reconfiguration can be problematic because alternative DNS roots are not authoritative for ICANN-delegated TLDs, which could result in domain names that are identical to those on ICANN's root and a "naming collision" as discussed in Part I. 73

IOD's claim stemmed from the fact that ICANN did not consider IOD's 2000 application, and when ICANN moved forward with the ".web" delegation process, IOD sued for trademark infringement under their registered and common law ".web" trademarks. 74 In its defense, ICANN argued that: (1) the .web would not cause confusion because TLD registry services are a different class of goods than those protected by IOD's registrations and (2) that TLD's are not subject to trademark protection because they are generic. 75 Ultimately, the court ruled in favor of ICANN and summarily dismissed all of IOD's trademark claims. 76

The IOD's claim under 15 U.S.C. § 1125(a)(1) 77 and its common law trademark was the most important part of the court's ruling. In its opinion, the court reiterated a long-held standard of trademark law that **"TLDs are not generally source indicators."** 78 The court further supported its ruling by citing the official policy of the USPTO that states "[g]enerally, when a trademark . . . is composed, in whole or in part, of a domain name, neither the beginning of the URL ('http://www.') nor the TLD have any source-indicating significance." 79 The IOD attempted to refute this portion of the ruling by pointing out that the USPTO altered its position to require consideration of "any potential source-indicating function of the TLD. 80 In response, the court stated that the **only marks available for protection as a TLD are famous**  [\*96]  **marks**, such as .apple for Apple, Inc., and that some marks would continue to remain generic even if they are famous. 81 In the court's view, ".web" fell under the latter category because it would indicate a genus of a type of website available on the World Wide Web and not a particular company or manufacturer. 82

Because of the court's decision in Image Online Design, **corporate stakeholders are susceptible to competitive harm if ICANN uses its powers unfairly**, particularly if the harm is propagated at the behest of another stakeholder. The effects of this limitation are particularly acute considering the ICANN's own regulatory policies, which take a similar position on the existence of trademark rights in gTLDs moving forward. 83 Both the UDRP and LRO, ICANN's current dispute resolution policies intended to protect the rights of trademark owners, reiterate the common proposition that gTLDs are generally ineligible for trademark protection. 84 However, both panels governing these decisions have articulated that this general rule may have an exception. 85

While this may indicate that the perception that gTLDs are generic is shifting, in application both policies strongly indicate that trademarkability is the exception, not the rule. The LRO decisions, for instance, demonstrate that to successfully assert legal rights in a gTLD, the trademark owner must either be particularly famous or be able to point to facts indicating bad faith on the part of the applicant. 86 While the UDRP has indicated a departure from this rule, panel decisions are **not subject to precedent.** This means that trademark owners should not expect any consistency between panel decisions, and that these decisions will be extremely fact specific.

B. The Consequences of Image Online Design

The presumably generic gTLDs, the uncertainty of how this rule will be applied, and the amount of fame a trademark owner must possess to state a claim have **created an environment where only the largest private stakeholders can successfully assert a violation** of their trademark rights against ICANN in court. Even then, the success of these claims remains in doubt, especially if ICANN's decisionmaking becomes clouded by undue influence from other stakeholders. For example, in a matter involving Amazon, [\*97]  ICANN denied delegation of the ".amazon" gTLD for reasons of "public policy" following strong objections by Brazil. 87 After failing to have the decision changed using ICANN's appeal processes, Amazon challenged ICANN's decision and requested an independent review that found **ICANN caved to pressure from the Brazilian government and**, more concerningly, attempted to abuse its internal processes to the detriment of Amazon. 88

#### Anti-competitive allocation of gTLDs exponentially increases internet privatization and decks internet freedom

Daniela Spencer 14, J.D. candidate at the UC Berkeley School of Law, “Trademark Law: Much Ado About Nothing: ICANN's New gTLDs,” 2014, lexis

C. ICANN's Section 1 Antitrust Violations

Since there are currently a small number of gTLDs, critics have alleged that ICANN is hindering competition not only among registries, but also among consumers. 120 Since ICANN has unlimited contracts with registries, critics allege that ICANN is assisting in an agreement amongst registries to restrain trade, which is illegal under Section 1 of the Sherman Act. 121 Consumers have limited choices among existing registries, especially since many of them are not open to the public. As such, they are limited to using registries like VeriSign, which are well known and open to the public.

As of September 2013, fifty-three percent of all registered websites had the gTLD of .com, owned by VeriSign. The next highest percentage of websites (5.7 percent) were registered under the TLD of .net, which VeriSign  [\*880]  also owns. 122 In 2006, the Ninth Circuit found that ICANN awarded VeriSign the contract for .com without any bidding. 123 As such, one private company is essentially controlling close to sixty percent of the market with collusion from ICANN. 124

There is no indication that there are any alternative products or possible substitutes to the favorite .com gTLD. 125 Additionally, unlike in a standard market, where the product is relatively elastic and responds to changes in price, in this system, sellers have little incentive to offer low prices in a market where demand is inelastic.126 ICANN has no incentive to discourage or prevent individual registry operators like VeriSign from charging high prices because consumers have nowhere else to turn. In the last few years, the demand for .com has increased, as demonstrated by its growing percentage of use while the prices have stayed stable. 127

 [\*881]  However, despite its prima facie appearance of restricting competition, the agreement between VeriSign and ICANN does not actually restrain commerce in the relevant market. Consumers do not choose .com due to a conspiracy between VeriSign and ICANN to reduce access to other gTLDs, but rather due to outside pressures to use .com. 128 As such, even the advent of hundreds of new gTLDs would not produce an appreciable or effective increase in competition. Despite its claim, ICANN's new program probably will not increase competition in any meaningful way. 129

D. Potential for Other Antitrust Violations Due to gTLDs

In a hearing to the House of Representatives in 2011, Federal Trade Commission chairman Jon Leibowitz said, "We worry that if ICANN goes broadly and doesn't ensure accuracy, it's going to be exponentially worse. There is going to be a burden on businesses, which will have to defensively register. We see a lot of cost but not a lot of benefit."130 Currently, there are a number of worries that big name players will monopolize the Internet. Donuts, Inc. 131 has applied for 307 gTLDs, Neustar has applied for 234, Google has applied for 101, and Amazon has applied for seventy-eight. 132 John M. Simpson, the director of Consumer Watchdog's Privacy Project, wrote to the chairman of Senate Commerce, Science, and Transportation Committee:

If these applications are granted, large parts of the internet would be privatised. It is one thing to own a domain associated with your brand, but it is a huge problem to take control of generic strings. Both Google and Amazon are already dominant players on the internet. Allowing them further control by buying generic domain [\*882] strings would threaten the free and open Internet that consumers rely upon. 133

#### Extinction---internet freedom solves every impact

Tony Blair 21, Former prime minister of Great Britain and founder and executive chairman of the Tony Blair Institute for Global Change, “The Progressive Case for Universal Internet Access: How to Close the Digital Divide by 2030,” 3/2/21, https://institute.global/policy/progressive-case-universal-internet-access-how-close-digital-divide-2030

Today, the internet is the beating heart of the world. And just as the roads, railways and canals provided the arteries for commerce in the Industrial Revolution, today’s network infrastructure is the circulatory system on which much of modern life depends. Without it, the ramifications of Covid-19 would have been far more severe.

That we have been able to use the internet to mitigate the impact of the pandemic is a small relief, but the Covid-19 crisis has emphasised the importance of everyone being connected in the future. Eradicating extreme poverty, solving the global education crisis, building better health-care systems and responding to pandemics effectively all require connectivity. For low-income countries, being largely excluded from the exponential potential of the internet means that they cannot transform their nations. It is extraordinary that today half the world remains offline.

Closing the digital divide by 2030 should be one of the primary global policy priorities. Accelerating internet expansion will drive economic growth and enable progress and – as this report from my Institute demonstrates – the benefits of investment vastly offset the costs. It outlines the urgent action required on stimulating demand, regulatory reform and greater global coordination, and how a new digital coalition needs to be formed to transform opportunity and access for billions of people.

But prioritising internet access is not only about poverty alleviation. During these past years of isolationist and unilateralist policymaking by Western governments, China has been taking a more dominant role in developing economies. It has been investing in digital hardware infrastructure, taking an active role within international bodies and influencing the standards and values that underpin the internet.

This requires strong global leadership. Collaborating with China, as well as competing. Stewarding the right global coalitions around investment to achieve universal internet access. Leadership with the vision, commitment and confidence to establish the internet for a prosperous and inclusive global society.

We’ve lost our way on this in recent years, but an open and connected world will be the lifeblood for our future growth. It’s time that we make it a reality.

#### Corporate control undermines internet connectivity and interdependence

Julius Genachowski & Lee C. Bollinger 13, Former Chairman of the U.S. Federal Communications Commission; President of Columbia University, “The Plot to Block Internet Freedom,” Foreign Policy, 4/16/13, https://foreignpolicy.com/2013/04/16/the-plot-to-block-internet-freedom/

The Internet has created an extraordinary new democratic forum for people around the world to express their opinions. It is revolutionizing global access to information: Today, more than 1 billion people worldwide have access to the Internet, and at current growth rates, 5 billion people — about 70 percent of the world’s population — will be connected in five years.

But this growth trajectory is not inevitable, and threats are mounting to the global spread of an open and truly "worldwide" web. The expansion of the open Internet must be allowed to continue: The mobile and social media revolutions are critical not only for democratic institutions’ ability to solve the collective problems of a shrinking world, but also to a dynamic and innovative global economy that depends on financial transparency and the free flow of information.

The threats to the open Internet were on stark display at last December’s World Conference on International Telecommunications in Dubai, where the United States fought attempts by a number of countries — including Russia, China, and Saudi Arabia — to give a U.N. organization, the International Telecommunication Union (ITU), new regulatory authority over the Internet. Ultimately, over the objection of the United States and many others, 89 countries voted to approve a treaty that could strengthen the power of governments to control online content and deter broadband deployment.

In Dubai, two deeply worrisome trends came to a head.

First, we see that the Arab Spring and similar events have awakened nondemocratic governments to the danger that the Internet poses to their regimes. In Dubai, they pushed for a treaty that would give the ITU’s imprimatur to governments’ blocking or favoring of online content under the guise of preventing spam and increasing network security. Authoritarian countries’ real goal is to legitimize content regulation, opening the door for governments to block any content they do not like, such as political speech.

Second, the basic commercial model underlying the open Internet is also under threat. In particular, some proposals, like the one made last year by major European network operators, would change the ground rules for payments for transferring Internet content. One species of these proposals is called "sender pays" or "sending party pays." Since the beginning of the Internet, content creators — individuals, news outlets, search engines, social media sites — have been able to make their content available to Internet users without paying a fee to Internet service providers. A sender-pays rule would change that, empowering governments to require Internet content creators to pay a fee to connect with an end user in that country.

Sender pays may look merely like a commercial issue, a different way to divide the pie. And proponents of sender pays and similar changes claim they would benefit Internet deployment and Internet users. But the opposite is true: If a country imposed a payment requirement, content creators would be less likely to serve that country. The loss of content would make the Internet less attractive and would lessen demand for the deployment of Internet infrastructure in that country.

Repeat the process in a few more countries, and the growth of global connectivity — as well as its attendant benefits for democracy — would slow dramatically. So too would the benefits accruing to the global economy. Without continuing improvements in transparency and information sharing, the innovation that springs from new commercial ideas and creative breakthroughs is sure to be severely inhibited.

To their credit, American Internet service providers have joined with the broader U.S. technology industry, civil society, and others in opposing these changes. Together, we were able to win the battle in Dubai over sender pays, but we have not yet won the war. Issues affecting global Internet openness, broadband deployment, and free speech will return in upcoming international forums, including an important meeting in Geneva in May, the World Telecommunication/ICT Policy Forum.

The massive investment in wired and wireless broadband infrastructure in the United States demonstrates that preserving an open Internet is completely compatible with broadband deployment. According to a recent UBS report, annual wireless capital investment in the United States increased 40 percent from 2009 to 2012, while investment in the rest of the world has barely inched upward. And according to the Information Technology and Innovation Foundation, more fiber-optic cable was laid in the United States in 2011 and 2012 than in any year since 2000, and 15 percent more than in Europe.

All Internet users lose something when some countries are cut off from the World Wide Web. Each person who is unable to connect to the Internet diminishes our own access to information. We become less able to understand the world and formulate policies to respond to our shrinking planet. Conversely, we gain a richer understanding of global events as more people connect around the world, and those societies nurturing nascent democracy movements become more familiar with America’s traditions of free speech and pluralism.

That’s why we believe that the Internet should remain free of gatekeepers and that no entity — public or private — should be able to pick and choose the information web users can receive. That is a principle the United States adopted in the Federal Communications Commission’s 2010 Open Internet Order. And it’s why we are deeply concerned about arguments by some in the United States that broadband providers should be able to block, edit, or favor Internet traffic that travels over their networks, or adopt economic models similar to international sender pays.

We must preserve the Internet as the most open and robust platform for the free exchange of information ever devised. Keeping the Internet open is perhaps the most important free speech issue of our time.

#### Internet connectivity prevents global war

Dr. Asma Iqbal & Muhammad Rafi Khan 21, Assistant Professor of Political Science, Government Graduate College for Women Samanabad; Lecturer/Research Officer at Minhaj University Lahore, “Power and Interdependence with Internet,” Pakistan Social Sciences Review, Vol. 5, No. 1, pgs. 1142-1153, 3/30/21, https://pssr.org.pk/issues/v5/1/power-and-interdependence-with-internet.pdf

Interdependence

Reflecting a softer image of power and extending its domains to global social structures, interdependence is a multidimensional term, that gained traction with the emergence of the concept of globalization. It refers to a state, or a condition, that compels two or more actors to seek cooperation. For such cooperation, the absence of enmity is not a requirement. There are many examples of interdependence between fierce enemies, like Pakistan and India, China and India, and Russia and the US. The goals of this interdependence are to fulfill domestic and international deficiencies for national interest, and sometimes, international interest. The presence of Russia and the US in the Security Council, where both take decisions together in international interest, and can also veto any move for their own or their ally’s national interest.

The world today has mostly been eradicating the threats of war and becoming increasingly interdependent. Their actions are mostly based on the cost- benefit ratio. For instance, if a state must choose between war and trade and applying the statistical models for a complete understanding of both before deciding, the trade will supersede in choice over the war in most cases. That is why even enemies are doing trade, while the war of words also gains traction. This is because the cost of war is higher, and the benefit of trade is higher. The democratic peace theory and the McDonald Peace theory exist in almost the same domains, where political relationship and economic connectivity, both are eradicating scenarios of a possible war.

As an effective tool of soft power, the interdependence has shattered the isolation of introverted peoples and merged them with vibrant, dynamic, and socially linked societies. It relies on multidimensional mediums to avoid conflicts, increase connectivity, and inculcates multilateralism. Among these, the Internet is the most obvious, effective and resourceful medium that “frees us from geographic fetters and brings us together in topic-based communities that are not tied down to any specific place. Ours is a networked, globalized society connected by new technologies” (Dentzel, 2014).

The internet, coinciding with matters related to power, is a world of unknown depth. It is the most effective tool of connectivity in this modern world. It can also be designated as a doorway between traditional unilaterality and a multilateral world. It boosted interdependence and opened new horizons of connectivity and cooperation. Therefore, the virtual age has cut the distances short and challenged the hardships of the physical world with a counterbalance, depicted in the figure below.

#### Internet privatization is increasing and displaces responsive and legitimate governance

Marietje Schaake 21, International policy director at Stanford University’s Cyber Policy Center, “Big Tech is trying to take governments’ policy role,” 1/27/21, https://www.ft.com/content/7f85a5ff-326f-490c-9873-013527c19b8f

Both events demonstrate an ever-growing trend: technology companies think they should be deciding public policy, not governments.

It is not just social media platforms, either. These days, all kinds of businesses set rules for how technology affects people’s lives. Encryption standards, for example, determine the extent of national security. Facial recognition systems deny the right to privacy.

Since all of society is touched by such digitisation, this puts companies in the position of policymakers — but without the governance mandate, independent oversight or checks and balances deemed vital in a democratic process.

In fact, tech groups’ governance powers are encroaching on the role of the state at ever greater speed. Minting digital currencies, verifying digital identities, even building cyberweapons — it is all under the direction of boardrooms, not parliaments.

One consequence of this private sector digitisation is that governments have, in effect, outsourced cyber security and personal data protection to companies — companies that do not always have duties of disclosure.

We witnessed as much in the hacking of SolarWinds’ networking software, to distribute malware. Had it not been for cyber security firm FireEye, we may never have learnt of the intrusions on companies and many US institutions. Software made by the likes of SolarWinds and Microsoft forms the backbone of digital operations globally, yet a decision to forgo proper security safeguards by SolarWinds was taken without anyone noticing. There are too few processes to ensure the public interest is systematically safeguarded.

That is why laws need to be updated fast. This is not about “regulating the internet” but rather about upholding existing principles, such as democracy — online or offline. And it is surely an erosion of democracy when the agency of an elected government is reduced proportionately to the pace with which private companies are empowered.

For technology groups wondering how they can avoid being accused of failing to protect democracy — as social media platforms have of late — there is a simple solution. Before the ink is dry on new rules granting regulatory oversight of digitised processes, such as search algorithms, companies can embrace the rule of law today.

Aligning with democratic and human rights principles can be done now.

The world over, the power of technology companies is becoming ever more apparent. That is why we must not limit our assessment of potential harms to democracy to just social media platforms or search firms. They may be the services that are most visible to internet users, but they are not the only ones in need of scrutiny. The privatisation of governance in the digital world is now a systems problem.

After the US Capitol riots of January 6, there is a growing awareness of the power of companies in providing a platform for the stagers of a coup. It should make us even more wary of that other coup: the privatisation of governance across the digital world.

#### Extinction---shoring up the US model of public governance is key

Joseph S. Nye 17, University Distinguished Service Professor at the Harvard Kennedy School of Government, January/February 2017, “Will the Liberal Order Survive?,” Foreign Affairs, https://www.foreignaffairs.com/system/files/pdf/anthologies/2017/b0033\_0.pdf

The order will inevitably look somewhat different as the twenty-first century progresses. China, India, and other economies will continue to grow, and the U.S. share of the world economy will drop. But no other country, including China, is poised to displace the United States from its dominant position. Even so, the order may still be threatened by a general diffusion of power away from governments toward nonstate actors. The information revolution is putting a number of transnational issues, such as financial stability, climate change, terrorism, pandemics, and cybersecurity, on the global agenda at the same time as it is weakening the ability of all governments to respond.¶

Complexity is growing, and world politics will soon not be the sole province of governments. Individuals and private organizations—from corporations and nongovernmental organizations to terrorists and social movements—are being empowered, and informal networks will undercut the monopoly on power of traditional bureaucracies. Governments will continue to possess power and resources, but the stage on which they play will become ever more crowded, and they will have less ability to direct the action.¶

Even if the United States remains the largest power, accordingly, it will not be able to achieve many of its international goals acting alone. For example, international financial stability is vital to the prosperity of Americans, but the United States needs the cooperation of others to ensure it. Global climate change and rising sea levels will affect the quality of life, but Americans cannot manage these problems by themselves. And in a world where borders are becoming more porous, letting in everything from drugs to infectious diseases to terrorism, nations must use soft power to develop networks and build institutions to address shared threats and challenges.¶ China is unlikely to surpass the United States in power anytime soon.¶

Washington can provide some important global public goods largely by itself. The U.S. Navy is crucial when it comes to policing the law of the seas and defending freedom of navigation, and the U.S. Federal Reserve undergirds international financial stability by serving as a lender of last resort. On the new transnational issues, however, success will require the cooperation of others—and thus empowering others can help the United States accomplish its own goals. In this sense, power becomes a positive-sum game: one needs to think of not just the United States’ power over others but also the power to solve problems that the United States can acquire by working with others. In such a world, the ability to connect with others becomes a major source of power, and here, too, the United States leads the pack. The United States comes first in the Lowy Institute’s ranking of nations by number of embassies, consulates, and missions. It has some 60 treaty allies, and The Economist estimates that nearly 100 of the 150 largest countries lean toward it, while only 21 lean against it.¶

Increasingly, however, the openness that enables the United States to build networks, maintain institutions, and sustain alliances is itself under siege. This is why the most important challenge to the provision of world order in the twenty-first century comes not from without but from within.

#### Privatization enables large-scale attacks on critical infrastructure

Marietje Schaake 20, International policy director at Stanford University’s Cyber Policy Center, “The Lawless Realm: Countering the Real Cyberthreat,” November/December 2020, https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

THE WEAKENED STATE

For centuries, states enjoyed a monopoly on the use of force. Thanks to the asymmetric power facilitated by digitization and the proliferation of cyberweapons, that monopoly has slipped out of their grasp. Yes, many democratic countries—including the United States—have developed powerful tools to deploy in cyberspace, setting up sophisticated surveillance systems and launching attacks on adversaries. At the same time, developed countries wrestle with a private sector that exercises disproportionate power in the technological sphere, gobbling up data and taking on some key functions of the state, such as the protection of critical infrastructure.

Private companies both build the architecture of the digital world and largely govern its flows of data. They are often the victims of cyberattacks. But they are complicit in these attacks when they fail to protect databases and lose the personal information of their customers and clients. Worse, some companies are even developing and selling new technologies to adversaries around the world. Authoritarian (and several democratic) governments hire the services of hackers and buy commercially sold systems of digital surveillance and control. For instance, a U.S. company called Sandvine is alleged to have supplied the government of Belarus with the technology it used this past summer to shut down its citizens’ access to much of the Internet during antigovernment protests. Nonstate actors, such as militias or criminal gangs, can wreak disproportionate havoc through cyberattacks, hurting much more powerful states, companies, and international organizations.

Authorities often have a tough time understanding cyberattacks and identifying their perpetrators. As a result, attackers frequently act with impunity, using clever tactics and benefiting from a legal vacuum: there are few mechanisms that guarantee international cooperation and coordination in discovering and bringing to justice cyberattackers. “False flag” operations—in which actors conceal their identities and try to pin the blame on others—are common in the digital world. An intrusion directed from the other side of the world can be executed in milliseconds, almost invisibly. The speed of digital innovation outstrips the ability of states to prevent cyberattacks, hold perpetrators to account, and pass the necessary laws on encryption standards, data protection, and product liability (to hold manufacturers or sellers responsible for the goods they make or trade).

States are also unable to control private companies whose actions may imperil public safety; indeed, in some cases, a state finds itself dependent on just such a company. Earlier this year, a breach of a database belonging to the facial recognition company Clearview AI revealed that the firm was selling its technology and databases not just to vetted law enforcement agencies but also to a host of private companies. The breach showed how a private company can secretly share information about citizens without their consent and without transparency, as well as how such a company can be susceptible to hostile actors. And yet law enforcement agencies are increasingly reliant on the work of technology firms such as Clearview AI.

Society’s growing reliance on digitally connected devices creates more general vulnerabilities. A canny and willing attacker can exploit a software-powered fridge in a home or a street lined with data-collecting sensors in a smart city, finding multiple entry points to bring down a broader system. It is enough of a challenge for defense departments and intelligence services to man the ramparts and keep a lookout for such sophisticated adversaries. But the frontlines are now ubiquitous thanks to the pervasiveness of digital technology, and so doctors in hospitals, professors in university labs, and human rights activists in repressive countries—all must now contend with cyberthreats.

Such civilian targets are not always well prepared for this fight. Public institutions often employ poorly protected digital systems even when they process sensitive information. A clinic, for example, cannot be blamed for hiring an additional surgeon instead of a cybersecurity expert. A public university might choose to invest in computers for students but not acquire the more expensive protections to ensure that those new computer systems are safe. And an election board might decide to modernize electoral processes by installing voting machines and dispensing with paper ballots, without knowing the proper safeguards or having the means to invest in the requisite protections. Such well-intentioned efforts are understandable on their face, but they conspire to make societies vulnerable.

AIDING AUTHORITARIANS

The imbalance between the public and the private sector in democratic countries is obvious in another dangerous arena: the sale of cyberweapons to authoritarian regimes. Few laws limit how companies can trade in digital surveillance, blocking, and intrusion systems. Syria is a troubling case in point. As it wages civil war, the government of Bashar al-Assad has used operations in cyberspace to hit both adversaries abroad and opponents within the country. Hackers belonging to the so-called Syrian Electronic Army (which claimed to be acting independently of the Syrian government) gained visibility around the world for defacing the websites of Western media companies, such as The New York Times and the BBC, and for hacking the website of the U.S. Marine Corps. These brief propaganda victories were far less significant than the government’s digitally enabled attacks on domestic opposition figures and human rights defenders during the peaceful protests of 2011. That year, the Syrian government used sophisticated digital technology to collect communications between dissidents, which it then exploited to incriminate and detain the activists.

That one of the most violent regimes in the world engaged in such repression is not surprising; what is shocking is that European companies helped. The Assad government depended on technology and expertise from AREA, an Italian company. AREA sold technology to Syrian authorities that allowed them to monitor communications across the country, collecting and scanning Facebook posts, Google searches, text messages, and phone calls for key words or connections between particular individuals. The ensuing roundup of dissenting civilians led to torture and deaths.

Syria is not alone in receiving technological support from abroad for the purpose of domestic repression. Over the past few decades, companies based in Western countries have designed, marketed, and sold similar technology to a number of other authoritarian governments, including those of Egypt, Iran, Saudi Arabia, and the United Arab Emirates. When democratic countries fail to curb the sale of aggressive hacking systems by companies within their own borders to illiberal governments, they are undermining the worthy ambitions of their foreign policies. But the problem doesn’t seem to be going away. Some estimates predict that annual global sales of these systems will rise to hundreds of billions of dollars by 2021. China is now aggressively entering this market, too; it already is the global driver in developing and exporting technologies that enable repression, including facial recognition technology and predictive policing systems.

These technologies in the hands of nonstate actors is also a concern: such actors can [devastate] ~~cripple~~ far more powerful states, organizations, and companies through cyberattacks. In 2015, a hack of JPMorgan Chase compromised 83 million accounts; four individuals were eventually arrested. In 2017, “Rasputin,” a hacker who appeared to be operating alone, broke into databases of U.S. universities and government institutions, apparently hoping to sell access to the information. Earlier this year, a 17-year-old from Florida and two other hackers managed to take over 130 prominent Twitter accounts, including those of former U.S. President Barack Obama and former U.S. Vice President Joe Biden, and posted messages that convinced people to send money to a particular Bitcoin account. The hackers could have used that account access for far more sinister goals, including attempting to escalate geopolitical conflict or crash stock markets.

Some individuals with such exceptional skills sell their talents to the highest bidder. Among the most notorious companies hiring hackers is DarkMatter. This cybersecurity company, based in the United Arab Emirates, has hired former intelligence officials from the U.S. National Security Agency and the Israel Defense Forces, creating what amounts to a private intelligence service and blurring the lines of agency between companies and states. Such companies with top-grade skills may attract unsavory clients, including authoritarian regimes and even terrorist groups.

Democratic states have struggled to regulate the digital world and the market for cyberweapons, but some technology companies are beginning to take action. WhatsApp, through its parent company, Facebook, filed a lawsuit last spring against the NSO Group, an Israeli mobile surveillance company. The suit alleges that NSO covertly exploited a vulnerability in WhatsApp to illegally extract information from the phones of users. Facebook argues that NSO’s actions were unlawful. NSO is also the target of a lawsuit filed in Israel in 2018 by a Saudi dissident who claims that Saudi authorities used the company’s technology to spy on his communications, including those with Jamal Khashoggi, the journalist who was murdered in Turkey by Saudi operatives that same year. Forty-five countries are thought to be using the same NSO product, including democracies such as Mexico and Spain.

MAKING THE RULES

It shouldn’t be left to private companies and courts to determine the legitimacy of products and services that have the potential to compete with state intelligence services. Democratic countries must extend norms and rules to ensure safety in the digital world. Just as nations agreed to international laws governing the conduct of war and nuclear weapons, so, too, must they establish agreements to fend off threats in cyberspace. Perpetrators of cyberattacks have remained unaccountable for too long. Democratic governments especially need to take a number of steps to rebalance the power between states and private companies, which play too large a role in the digital world.

#### That goes nuclear, even if it fails

Vladimir Orlov 20, Founder & Director of the PIR Center, President of the Trialogue Club International, Head of the Center for Global Trends and International Organizations at the Diplomatic Academy, Ministry of Foreign Affairs of the Russian Federation, Co-Founder and Academic Supervisor of the International Dual Degree MA Program in Nonproliferation and Global Security Studies, MGIMO University, Professor at MGIMO University, author (or coauthor) of more than a dozen books and monographs and more than three hundred research papers, articles, and essays, publishes his views in Russian and foreign periodicals, “‘No Holds Barred’ and the New Vulnerability: Are We in for a Re-Run of the Cuban Missile Crisis in Cyberspace?,” SSRN Scholarly Paper, ID 3538078, Social Science Research Network, 02/14/2020, papers.ssrn.com, doi:10.2139/ssrn.3538078

Not hundred per cent of the dialogue has been frozen, fortunately. Certain informal, mostly offthe-record, meetings of US and Russian experts on cyber agenda continue taking place, both through Track 2 and Track 1.5. One of the most intellectually stimulating meetings, with frank exchanges, took place in Vienna in December 2018. The report produced after the meeting stressed “the significant risk […] that cyber-attacks could conceivably lead to a military escalation that may further trigger a nuclear weapons exchange, a fact that became more explicit with the adoption of the current Nuclear Posture Review. This issue gets complicated given that third parties may have the capabilities to invoke a cyber conflict between Russia and the United States. Whether a country or a non-state actor, they could put the two countries on the verge of an armed conflict by attacking critical infrastructure of either of them and making it look as if the aggressor were the other one”[22]. However, one should have no illusion: such informal meetings may be fully fruitful only when their reports and policy recommendations are utilized by the governments. And for that, a warmer climate in bilateral relations is a must. So far, we see exactly the opposite: mercury falling to freezing levels.

Risk of cyber clashes growing into a chaotic global cyber war has been emphasized by the UN Secretary-General Antonio Guterres in his Agenda for Disarmament: “Malicious acts in cyberspace are contributing to diminishing trust among States… States should implement the recommendations elaborated under the auspices of the General Assembly, which aim at building international confidence and greater responsibility in the use of cyberspace.[23]” However, as the members of the US-Russian Track 1.5 working group on strategic stability recently concluded, “without a constructive dialogue on cyber issues between the United States and Russia, the world would most likely fail to agree on any norms of responsible behavior of states in cyber space”[24].

Do we really have to survive a cyber equivalent of the Cuban Missile Crisis to realize the importance of achieving some kind of agreement on cyber issues, and on the broader agenda of international information security?[25] Or is that kind of talk plain old alarmism?

I don’t want to sound a fatalist, but I am even less keen on sounding like an ostrich that’s buried its head in the sand. We cannot ignore the obvious: whether the world’s most powerful actors like it or not, the world is sliding to another major crisis like the one in 1962. The cyber war is already raging. There are no rules of engagement in that war. The uncertainty is high. The spiral of tension is getting out of control. The cyber arms race is gaining momentum. And there are no guarantees that the next crisis will be controllable, or that it will result in a catharsis as far as international information security regulation is concerned. There’s no telling what will happen once the cyber genie is out of the bottle.

### 1AC---Multistakeholder Governance ADV

#### Advantage Two Is Multistakeholder Governance---

#### Two internal links---

#### First---Norms---the plan uniquely fosters ICANN accountability by establishing its presence within international human rights norms

Monika Zalnieriute 19, Research Fellow and Lead of 'Technologies and Rule of Law' Research Stream at the Allens Hub for Technology, Law, & Innovation, Faculty of Law, UNSW Sydney, Australia, “From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Case of Internet Governance and ICANN,” 21 Yale J. L. & Tech. 278, 2019, lexis

While profitability might not necessarily be the only reason driving corporations and private bodies to adopt human rights policies, it is nonetheless widely accepted to be the most influential. When human rights and profitability conflict, the latter will often prevail. This is well illustrated by the infamous  [\*316] strategic alliance between IBM and Nazi Germany, as well as by the recent complicity of U.S. tech giants, such as Microsoft and Google, in restricting free speech in countries like China. In the case of the latter, even an enormous public outcry has not been enough to reverse agreements made by Google to return to China to expand its customer base. While Google's commitment to human rights were questioned by many people, even a special "China search database" does not seem to prevent Google from branding itself as a defender of "Internet freedom."

Similarly, market forces have not been favorable for human rights protection within ICANN so far, not least because ICANN is not a traditional corporation--it is a non-profit corporation, which has no direct customers in the traditional sense, nor does it really compete with any other organization for market share in the assigned names and numbers of the Internet. Therefore, it seems unlikely that ICANN will pay attention to calls by human rights advocates, such as the CCWP-HR, to embrace its CSR obligations and to respect human rights by adopting new or modifying existing policies to ensure that they comply with human rights standards. ICANN does not have to worry that domain name registrants will no longer purchase domain names, because it is essentially a non-profit global policymaking monopoly that does not have any customers or competitors. It is precisely this non-profit status which has thus far successfully insulated ICANN from societal and regulatory pressure.

Given the lack of a profit motivation on the part of ICANN, it is difficult to see why a non-profit body managing global Internet  [\*317] resources and operating solely in the public interest should be subjected to a lower standard for human rights protection than a public body would be. Indeed, the discussion in Section II supra demonstrates that ICANN has qualities that are much more similar to those of public organizations and transnational policymaking networks than those of transnational for-profit corporations. Increasing involvement in ICANN by states--which are bound by both national and international human rights law obligations--points to the increasingly public dimension of this unique international body. This increasingly public dimension, in turn, suggests that the human rights duties of such a quasi-governmental international body must go well beyond those required of business corporations. While for corporations, it may seem reasonable to accept that there is a narrower scope of human rights obligations when compared to states, the narrower scope of obligations appears not as relevant when considering non-profit corporations such as ICANN, which operate solely in the public interest. Indeed, this unique status and operation for the public interest render ICANN's duties to respect human rights much stronger, because its social mission is not complicated by motivations for profit. Therefore, ICANN's human rights duties should be stronger than those of a standard for-profit corporation.

C. Public Confidence and CSR

As a non-profit organization, ICANN might uphold "soft commitments" and CSR not because of competition in the market, but rather to increase public confidence in its operations and create a better public image. Other factors beyond profit considerations, such as public "naming and shaming" and pressure by regulatory bodies and civil society, might therefore be more effective.

Thus far however, public confidence and public image have not proven to be strong factors for ICANN in embracing its CSR to respect human rights. A potential reason for this is that ICANN  [\*318] is not a widely known organization, and many people are unaware of the human rights implications of its activities. Pressure by NGOs or by data privacy commissioners and authoritative intergovernmental organizations (such as the EU Commission or Council of Europe ), have been ineffective in preventing ICANN from adopting certain policies that seem to strongly contradict human rights law. For example, an outcry from human rights activists over the .gay top level domain name has not motivated ICANN to pay more attention to the rights of freedom of expression and freedom of assembly of the LGBTI community. Similarly, dozens of letters to ICANN from the EU data protection authorities and various NGOS over violations of data privacy rights in the WHOIS policy and in the Registrar Accreditation Agreement of 2013 have seemingly done little to bother ICANN, in terms of any decrease in public confidence or in trust from regulatory authorities. Moreover, ICANN's main accountability mechanism of independent  [\*319] arbitration, which can be used to challenge its decisions, has been employed only once since 2005.

Therefore, public accountability and the informal multistakeholder structure of ICANN have had a limited effect in actually holding the organization to human rights values. Public confidence might, however, become increasingly important, as ICANN is in the process of the IANA transition and is no longer supervised by the U.S. government, with ICANN declaring in its own words that it is "officially accountable to the global multistakeholder community."

D. Voluntary Commitments and CSR as "Social Branding"

A widespread practice by private actors of upholding CSR norms solely for the purpose of increasing public confidence has led some scholars to argue that CSR policies have been captured by business interests and commodified, as these policies are often used as marketing or social branding tools. In the case of ICANN, such CSR commodification does not relate to the promotion of its products (as it does not sell any), but rather to the strengthening of its institutional image in the global Internet governance regime as a relevant, transparent, and accountable institution that respects human rights. While ICANN is a non-profit, quasi-governmental corporation, its income is generated from numerous for-profit entities, such as registries and registrars that it contracts with. Thus ICANN perhaps could be indirectly compared to what some scholars describe as "market-oriented NGOs." These are sponsored by  [\*320] businesses but aim to be associated with civil society organizations; they "disseminate and actualize corporate-inspired versions of 'social responsibility.'" An example of a market-oriented NGO is the International Chamber of Commerce (ICC).

Some have convincingly argued that a powerful platform for "corporate-inspired versions of social responsibility" was created by the UN Guiding Principles. For example, the organization Rights and Accountability in Development (RAID) uses empirical evidence collected during the five years since the adoption of the UN Guiding Principles to argue that corporations endorse the UN Guiding Principles because they "offer companies a way to manage human rights risks, thereby protecting their business reputation, insuring against claims, and managing problems to avoid their escalation. Ultimately, like any other risk management process, it is an approach which protects profits by reducing costs."

E. CSR as a Risk and Information Management Tool

Empirical research by RAID further suggests how corporations might adopt company-based grievance mechanisms to overcome barriers to accessing judicial review, while at the same time introducing numerous controls to monopolize information, such as legal waivers and confidentiality clauses. This essentially channels victims through a review mechanism of the company's own making, which is centrally devised and controlled.

This is relevant for ICANN, as its institutional structure is based on contractual agreements and memoranda of understanding, and is filled with numerous legal waivers and confidentiality clauses. Lack of compliance with human rights laws is often  [\*321] well hidden behind the numerous legal actions and waivers between ICANN and various parties. For example, as mentioned in Section II supra, ICANN is seeking injunctions to ensure that accredited registrars keep collecting and revealing personal information in WHOIS, as required under its contracts, which contravenes the EU data protection framework under the GDPR. Similarly, the incompatibility of the Registrar Accreditation Agreement (RAA) agreement with the EU data protection law is managed via the so-called "data retention waiver" system, exempting several registrars from the specified data retention requirements, so that they can comply with EU data protection law.

It is not yet clear how such "legal management" systems will be impacted (if at all), once the human rights Bylaw comes into effect. The Impact Assessment Evaluation of the new Bylaw by the ICANN staff states, "The area where ICANN will be most impacted is in bringing in tools so that the policy development takes into account human rights considerations." Does this mean that ICANN will adopt ex ante human rights impact assessments for each policy it is developing, and will not simply try to manage incompatibility ex post? It would be naive to expect that when implementing the human rights Core Value, ICANN would act fundamentally differently from other transnational corporations, and without resort to legal management mechanisms, such as the waivers which it has readily employed in the past.

 [\*322]  F. Would Regulatory and Punitive Action Help?

Given the limited ability of multistakeholder accountability mechanisms to hold ICANN to its self-imposed human rights commitments, regulatory action against private actors in Internet governance might provide lessons for holding ICANN accountable for its human rights commitments. In this regard, a relationship between influential Internet platforms and EU regulators (such as the EU Commission and the Article 29 Working Party) could provide such lessons for ICANN, as well as for the business and human rights movement more generally. In particular, Google's market dominance saga and Facebook's Cambridge Analytica scandal suggest that private actors will rarely change their policies and procedures unless threatened with direct legal and punitive actions by influential institutions, such as the EU Commission or the U.S. Department of Commerce, for disregarding and violating fundamental rights norms.

#### ICANN accountability cements international support for multistakeholder internet governance

Megan Stifel 17, Founder and Chief Executive Officer of Silicon Harbor Consultants, “Maintaining U.S. Leadership on Internet Governance,” 2/21/17, Council on Foreign Relations, Digital and Cyberspace Policy Program, https://www.cfr.org/report/maintaining-us-leadership-internet-governance

Challenges for Multistakeholder Governance

The reformed multistakeholder internet governance approach faces significant challenges. The sophistication of cybercrime continues to increase, as does the use of computer attacks for espionage, disruption, and influence by states. In October 2016, unknown actors used thousands of unsecured devices to launch a massive attack that limited many users’ access to Twitter, Amazon, and other major websites. Left unchecked, these growing threats and other technical vulnerabilities could ~~cripple~~ [destroy] the internet. Developing economies are only now beginning to grapple with these challenges as increasing numbers of their citizens go online. If the multistakeholder model is seen as ineffective in addressing the vulnerabilities that enable cybercrime, or being completely peripheral to the issue, developing economies could question its legitimacy and seek answers in the multilateral system.

In addition, authoritarian governments, many of which are increasing their efforts to control internet activity within their own borders, continue to challenge multistakeholder models of governance. These countries cherry-pick multilateral and other standards organizations to find those most likely to promote a state-centric approach to governance. Recent efforts to create a technical standard to catalogue all devices connected to the internet failed, but it can be expected that China, Russia, and others will find new opportunities to promote other standards that could frustrate innovation.

There are also worries that ICANN, the operator of the IANA functions, will abuse its authority and ignore the interests of internet users. In the past, ICANN has been accused of ignoring the views of governments, prioritizing private sector interests, and mismanaging its finances. ICANN recently implemented enhancements to address these and similar concerns. Nevertheless, ensuring that ICANN remains accountable will be critical to demonstrating that the multistakeholder approach works. It will also act as a bulwark against Russian and Chinese efforts at greater intergovernmental control over the internet.

#### Externally---ICANN responsiveness spills over globally, securing a rights-based framework throughout digital governance

Andi Wilson Thompson 17, Senior policy analyst at New America’s Open Technology Institute, “Protect the Free and Open Internet,” 1/19/17, New America, https://www.newamerica.org/weekly/protect-free-and-open-internet/

ICANN: The Internet Corporation for Assigned Names and Numbers (ICANN) is a little-known non-profit organization that helps manage the “inner workings of the internet.” Put simply, ICANN maintains a complex system of naming and numbering that directs people to the right website. The U.S. has had a veto over ICANN decisions since its creation—a responsibility it has never exercised—but the Department of Commerce recently completed the long-awaited process of relinquishing that role. ICANN has matured and can now function as an independent organization. This transition led to strong statements by President-elect Trump, who accused the U.S. of “surrendering control of the internet to foreign powers.” In reality, as our paper points out, the change will make it easier to fight for internet freedom around the world by removing the common complaint that the U.S. is in charge. Given Trump’s critical statements, there is concern that he could take steps to derail the progress that the United States has made toward more global internet governance. We strongly recommend that the incoming administration strengthen mechanisms that ensure the independence, accountability, and transparency of ICANN’s decision-making processes, and work with the private sector and other governments to build independent and accountable financial support mechanisms for diverse global participation.

Rebecca MacKinnon, director of the Ranking Digital Rights project (incubated at New America), said it best during the launch event for these recommendations: Internet freedom starts at home. Domestic policy influences international policy, U.S. policy influences global policy, and threats to internet freedom in the United States embolden governments that are looking to limit the access of their citizens to a free, open, and secure internet. The Trump administration has a duty to assert its unique leadership on policy issues, including those above, and to continue the decades-long, bipartisan support that internet freedom policy has previously held. Further, it must take steps to protect, promote, and strengthen freedom online—at home and around the world—through policies that align with our long standing international commitments to uphold human rights and the rule of law while also strengthening our economy and protecting us from threats to national security.

#### Solidifying human rights as a foundation for internet norms stops nuclear war AND builds capacity to respond to future existential threats

Dennis Pamlin 15, Entrepreneur and Founder of 21st Century Frontiers, Senior Associate at Chinese Academy of Social Sciences, Visiting Research Fellow at the Research Center of Journalism and Social Development at Renmin University, Advisor to Centre for Sustainable Development at Confederation of Indian Industries, Stuart Armstrong, DPhil from Oxford University, James Martin Research Fellow at the Future of Humanity Institute at Oxford University, “Global Challenges, 12 Risks That Threaten Human Civilization: The Case for a New Risk Category”, Global Challenges Foundation, February, https://api.globalchallenges.org/static/wp-content/uploads/12-Risks-with-infinite-impact.pdf

2. Whether poor governance will result in a collapse of the world system.

3. How mass surveillance and other technological innovations will affect governance.

4. Whether there will be new systems of governance in the future.

5. Whether a world dictatorship may end up being constructed.

1. Global coordination between nations is essential for building a good global governance system – but also essential for building a bad one.

2. Global poverty is one of the important problems that are being only partially solved by current policies. In turn, it can contribute to global instability, worsening likely governance outcomes.

3. Smart sensors and mass surveillance can contribute to new systems of governance, but also to large-scale dictatorships.

4. The global system of governance consists of the UN and a wide variety of bilateral or multilateral agreements and norms, constructed mainly according to national self-interests. Thus significant improvements to global governance are currently possible.

5. General mitigation efforts against governance disasters are tricky – most mitigation efforts are the results of governance decisions! However, some efforts can be made – for instance, an increase in recognised human rights across the globe could militate against certain pernicious governance directions. These efforts are of a very different nature to mitigating other risks.

6. Some groups may deliberately seek to construct a world dictatorship, either through self-interest or because they believe it would be the best design for global governance.

7. Undesirable world systems (such as global dictatorships) could result from a worsening of global governance.

8. Many value systems do not distinguish between action and inaction, so a global system that didn’t positively encourage human flourishing would be almost as pernicious as one that blocked it.

9. Global pollution is a problem requiring solutions at the global governance level.

10. Climate change is a problem requiring solutions at the global governance level.

11. Various ethical systems have desirable goals that could be achieved in theory, but would not be achieved under suboptimal governance.

12. It would be a tragedy if absolute poverty were to endure over the generations to come, especially if this outcome were avoidable.

13. A collapse of the world system, for any reason (including revolution) is the most direct way a governance disaster could result in mass casualties.

14. Governance decisions taken at the global level have a high potential to cause disruptions to the world’s political and economic systems.

15. Bad governance at the global level may not be susceptible to improvements and could cause problems for a considerable amount of time.

16. Technological innovations could allow completely new models of government, but could also facilitate surveillance dictatorships.

17. Global instability could result in more pernicious systems of governance, as well as an increased failure to solve important problems.

18. New systems of governance could be developed, using modern communication technology for instance.

19. The political landscape after a disaster will be important in determining whether governance disasters could cause civilisation collapses or mass casualties.

20. How to compare enduring poverty, actual casualties, and repressive governance is a question of values and not just of direct comparison of lives lost.

– Research

In this paper Nick Bostrom, the director of the Future of Humanity Institute, lays out the case for making existential risk reduction a global priority. Existential risks (Xrisks) are the highest category of negative impact in this report, those that threaten the entire future of humanity. The policy implications of the paper are:

– Existential risk is a concept that can focus long-term global efforts and sustainability concerns.

– The biggest existential risks are anthropogenic and related to potential future technologies.

– A moral case can be made that existential risk reduction is strictly more important than any other global public good.

– Sustainability should be rethought in dynamic terms, as aiming for a sustainable trajectory rather than a sustainable state.

– Some small existential risks can be mitigated today directly (e.g. asteroids) or indirectly (by building resilience and reserves to increase survivability in a range of extreme scenarios) but it is more important to build capacity to improve humanity’s ability to deal with the larger existential risks that will arise later in this century. This will require collective wisdom, technology foresight, and the ability when necessary to mobilise a strong global coordinated response to expected existential risks.

– Perhaps the most cost-effective way to reduce existential risks today is to fund analysis of a wide range of existential risks and potential mitigation strategies, with a long-term perspective.

If this paper is right, a general lack of focus on existential risks by governments and other agents can be considered a governance disaster in itself.

19-Apr-13: Multidimensional poverty index diminishes in 18 out of 22 analysed countries 563 – Event

Of 22 countries for which the Oxford Poverty and Human Development Initiative analysed changes in MPI (Multidimensional Poverty Index) poverty over time, 18 reduced poverty significantly.

This confirms other studies, by the World Bank564 and others:565 poverty reduction is possible, and has been successfully implemented in many countries.

05-Jun-13: Guardian leaks NSA spying programme 566

– Initiative

A significant event was the revelation by Edward Snowden of the extent of the NSA’s surveillance programme. This included the mass recording and mining of data across the United States and the interception of foreign politicians’ data.

The revelations caused great controversy567 and raised questions about the NSA’s surveillance oversight.568 The episode established that discrete mass surveillance – an important component of potential totalitarianism – was already possible using current technology and political organisation.

– Policy

To reduce poverty in the future, it is important to maintain and extend past trends in poverty mitigation. The United Nations’ Poverty-Environment Initiative (PEI), launched in 2008, has had a number of success stories from Uruguay570 to Malawi.571 Due to increased demand from member states, the programme has been extended for another five years, 2013-2017, and may add countries such as Myanmar, Mongolia, Indonesia, Albania, Peru and Paraguay. Such programmes demonstrate that the bureaucratic/policy side of poverty reduction is supported by an international infrastructure with a strong emphasis on assessments. The effect of such approaches on overall poverty will depend on the interplay between these policies and the other side of poverty reduction: economic growth572 and trade.573

“We have some idea what might happen if, in the face of other pressing global challenges, we divert our focus from making systemic improvements in public health and veterinary services — and that prospect is frightening.” The World Bank 574

global risks

4. Relations between global risk and their potential impacts between global risks

4.1 General relations Two things make the understanding of the relation between the global risks particularly important.

1. Impacts: The global risks are interconnected in different ways. Often the situation can be described as a set of dominoes: if one falls, many others follow. Even small impacts can start a process where different challenges interact. Higher temperatures due to global warming can result in the spreading of pandemics which increase tensions between countries, and so on.

2. Specific measures to address a risk: Global risks often require significant changes in our current society, from how we build cities to how food is produced and provided. Such significant changes will result in situations where measures to reduce the risk in one area affect the probability and/or the impact in other areas. Depending on the measure chosen to reduce the risk, and other complementary measures, the effect can be positive or negative.

Relations between global risks is an area where surprisingly little work is being done. Most research focuses on individual or closely related groups of challenges. Organisations working on global challenges are almost always working on individual risks. The initial overview below is based on individual studies where different relations are analysed, but no work has been identified where the relations between all twelve challenges have been analysed.

A risk that is natural to start with is future bad global governance, as all other global challenges exacerbate governance disasters,575 and all other global challenges can potentially be exacerbated by governance disasters.

A well functioning global governance system is therefore a key factor to address global catastrophic risks. Conversely, avoiding governance disasters improves all risks, as better institutions are better able to mitigate risks. Governance disasters directly increase the problems of climate change (through a lack of coordination between countries), the risk of nuclear war (by stoking conflict between nuclear powers) and global system collapse (by weakening global responses to systemic risks). All risks exacerbate global system collapse, by putting extra stress on an interconnected system.576 Conversely, a resilient governance system is better able to cope with all risks, and a collapsed global system is more vulnerable to all risks.

#### Second---Foreign Capture---lack of domestic antitrust enforcement over ICANN incentivizes foreign actors to fill the gap---that causes litigation to discredit the body and prompts a shift to state-based multilateral governance

Szóka et al. 16, Berin Szóka is President of TechFreedom; Brett Schaefer is the is Jay Kingham Senior Research Fellow in International Regulatory Affairs at The Heritage Foundation; Paul Rosenzweig is a Visiting Fellow at The Heritage Foundation and formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security, “ICANN Transition is Premature,” 9/8/16, http://docs.techfreedom.org/TF\_White\_Paper\_IANA\_Transition.pdf

To the extent that’s true, those who worry that ICANN may be subject to capture and used in anticompetitive ways actually should worry about the Transition, not necessarily because the Transition changes the legal analysis over whether ICANN can be sued, but because if U.S. antitrust law can’t provide an effective remedy (or deterrent), one could legitimately worry that the Transition means giving up the leverage the U.S. has now: the possibility of putting the IANA contract out for re-bid (to an organization other than ICANN) if ICANN misbehaves.

And what about foreign antitrust law? Foreign courts are, in general, not only more willing to allow suit against state actors but also to discount pro-competitive justifications and, frankly, to allow firms to bring suits against their rivals. So it’s entirely possible that, while U.S. antitrust law might under-enforce, ICANN could be vulnerable to antitrust suit in other jurisdictions.

One might think the two would balance out, and that foreign courts would allow valid suits that might fail in the U.S. for whatever legal reason. Maybe. But there are so many potential antitrust suits that could be brought. While they’d all, no doubt, be framed as protecting consumers, some may really have narrow corporate agendas or broader political agendas.

China and Russia have made no secret of their push to gain greater control over Internet governance. And there’s every reason to think they would use antitrust as a weapon to that end. It wouldn’t be hard for them to find (or create) plaintiffs to carry their water. Again, it’s hard to say exactly what the suits would look like, but it’s clear what their basic objective would be: to portray ICANN as a cartel dominated by, in particular, American companies. The fact that U.S. courts might have tossed out such suits would simply help with the political framing. The goal would be to say that the Transition isn’t enough, that Internet governance should be transferred to the ITU, where it would be “democratically accountable” (i.e., dictated by governments).

#### It’s likely---there’s a coming push to displace ICANN and dislodge its model

David Ignatius 21, Associate editor and columnist for The Washington Post, “Russia’s plot to control the Internet is no longer a secret,” 5/4/21, Washington Post, https://www.washingtonpost.com/opinions/2021/05/04/russias-plot-control-internet-is-no-longer-secret/

Russia’s campaign to control the Internet isn’t just a secret intelligence gambit any longer. It’s an explicit goal, proclaimed by Russian President Vladimir Putin as a key element of the Kremlin’s foreign policy.

Putin complained during his annual address to the Russian federal assembly on April 21 that the United States and other western countries are “stubbornly rejecting Russia’s numerous proposals to establish an international dialogue on information and cybersecurity. We have come up with these proposals many times. They avoid even discussing this matter.”

Asking for “international dialogue” takes some nerve, coming from the world’s biggest cyberbully — a country that notoriously meddled in the 2016, 2018 and 2020 U.S. elections, and has engaged in similar Internet mischief throughout the world. Controlling the “information space,” as the Russians sometimes call it, has long been an intelligence priority for Moscow.

Russia is waging its cyberdiplomacy offensive on two fronts: First, the United Nations has embraced Russia’s proposal to write a new treaty governing cybercrime, to replace the 2001 Budapest convention that Moscow rejected because it was too intrusive. And second, Russia is lobbying for its candidate to head the U.N.’s International Telecommunications Union (ITU) and use it to supplant the current private group, known as ICANN, that coordinates Internet addresses.

These international regulatory battles sound obscure, but they will help determine who writes the rules for Internet communications for the rest of the 21st century. The fundamental question is whether the governance process will benefit authoritarian states that want to control information or the advocates of openness and freedom.

Secretary of State Antony Blinken stressed on Tuesday the importance of this contest. “There are relatively few items that are ultimately going to have a greater impact on the lives of people around the world than the ITU post. It may seem dry and esoteric, but it’s anything but. And so we’re very, very actively engaged on this front,” Blinken said in an email message, elaborating on comments he made to me during an April 7 interview.

Russia outlined its ITU game plan in unusually forthright comments by Ernst Chernukhin, the foreign ministry’s special coordinator for political use of information and communications technology. He spoke on April 21, the same day Putin made his speech.

“The optimal option . . . would be transferring Internet management prerogatives specifically to the ITU, as it is a specialized U.N. body, which has the needed expertise on these issues,” Chernukhin said. “This strategic objective may be achieved by electing or promoting the Russian candidate to the position of the ITU Secretary-General in the 2022 elections . . . and by holding the 2025 anniversary U.N. Internet Governance Forum in Russia.”

Russia’s candidate for ITU secretary-general is Rashid Ismailov, a former deputy chief of the Russian communications ministry and a former executive at the Chinese telecommunications company Huawei. In announcing Ismailov’s candidacy on April 7, Maxim Parshin, the current deputy minister, underlined Moscow’s governance takeover plan: “We believe it is important to define an entity, within the U.N. framework, that would develop and implement legal norms and standards in the field of Internet governance. We think that the ITU could become such an entity.”

The Biden administration’s candidate for the ITU post is Doreen Bogdan-Martin, an American telecommunications expert who’s currently director of the ITU’s development bureau. The State Department, which has sometimes been lackadaisical in such international regulatory contests, is campaigning aggressively for Bogdan-Martin, and officials hope she’ll have sufficient support in Africa, Europe, Latin America and elsewhere to win the post. The election will take place at an ITU gathering late next year in Romania.

Internet technical governance today is managed by ICANN, which stands for Internet Corporation for Assigned Names and Numbers. This gathering of engineers and other experts was founded in 1998 to supervise domain names for the Defense Department’s ARPANET system, and it operated under a contract with the Commerce Department until 2016, when it went fully private.

The American roots of the Internet seem to both upset Putin and fuel conspiratorial talk. The Russian leader said during a 2014 interview translated by RT that the Internet “first appeared as a special CIA project . . . and the special services are still at the center of things.” Dmitry Medvedev, Russia’s former president, complained in a February interview: “The Internet emerged at a certain time, and undoubtedly the key rights to control are in the United States.”

Russia is ready to rumble over the rules that will shape the future of Internet communications. Fortunately, the Biden administration seems determined to fight back hard to maintain fair and open rules.

#### Multistakeholder governance is key to fend off authoritarian takeover but overzealous governmental intervention backfires

Joe Kane & Milton Mueller 18, Graduate research fellow at the Mercatus Center; Professor at the Georgia Institute of Technology School of Public Policy, “U.S. government should not reverse course on internet governance transition,” Brookings Institute, 2/7/18, https://www.brookings.edu/blog/techtank/2018/02/07/u-s-government-should-not-reverse-course-on-internet-governance-transition/

ICANN is an imperfect organization with politics and problems of its own. But the transition led to dramatic improvements in ICANN’s accountability and corporate governance. The relevant alternatives at this point are leaving IANA stewardship in the hands of ICANN or, if legally possible, transferring it back to the U.S. government. There are no perfect solutions here, only tradeoffs. Accepting stewardship by ICANN is still preferable to reverting to the NTIA, which would bring injurious consequences for global internet freedom. For those who value global internet freedom, the former is the only option.

The internet protocols are used globally, rendering internet governance a matter of global concern. A free and open internet run by the private sector and relatively free of geopolitics was the reason for delegating authority over IANA to ICANN in the first place.

As global commerce and civil society become increasingly reliant on the internet, committing to private governance, rather than government or intergovernmental control, is more critical than ever. If the U.S. wants to be a legitimate force in combating authoritarian regimes who seek greater control over the internet, it must hold fast to its principle of multi-stakeholder governance by non-state actors, and it must be able to keep moderate countries from abandoning the ICANN regime and embracing governmental control.Reversing the IANA transition would tell the world that we want governments to be in charge of the internet—and China and Russia would not hesitate to assert their respective claims.

The issue here is as much about rhetoric as it is about substance. The IANA functions themselves do not directly impinge on whether authoritarian governments gain more influence over the internet, but how the United States reacts to the transition will nudge diplomatic debates one way or another. If the U.S. government is seen to be grasping at more control over the internet, countries that would otherwise be on the fence might support a greater role for intergovernmental bodies in internet governance.

On the other hand, going through with the transition has improved the United States’ negotiating position. By committing to private governance of the internet, it has been and will be able to augment its credibility in arguing against more government control. Attempting to reverse the transition would undermine whatever influence the U.S. has gained since it took place.

This problem is now especially acute because of this November’s Plenipotentiary Conference of the UN’s International Telecommunication Union, a body that has notoriously sought to establish intergovernmental control over the internet in the past. Authoritarian governments want nothing more than to paint the U.S. as a hypocrite that touts internet freedom while secretly grabbing the controls. How far they seek to go at this year’s conference will partly depend on how far the U.S. goes in attempting to reverse the IANA transition and how many moderate-country votes they can swing to their side.

Of course, it might be that Redl’s promised “panel of experts” was a political ploy. It may never materialize or, if it does, it may return a verdict consistent with his original answer at the confirmation hearing, that “it’s very difficult to put the genie back in the bottle.” Either way, both Redl and Cruz should look ahead to address real internet governance threats from authoritarian governments, like an expanded role for the ITU and ICANN’s Government Advisory Committee, rather than trying to undo the privatization of the IANA functions.

We have been living in a post-transition world for over a year now, and nightmare scenarios of Russia and China somehow being empowered by this change have yet to materialize. Trying to undo the transition only makes these harmful outcomes more likely.

#### A transition fractures global ICT interoperability

* ICT: information and communications technology

Isabella Wilkinson 21, Research Associate at Chatham House’s International Security Programme, “Digital standards are key for protecting democracy,” 5/17/21, https://www.chathamhouse.org/2021/05/digital-standards-are-key-protecting-democracy

Geopolitical tensions in digital technical standards

And it could not have come at a better time. China has proposed a ‘new IP’ within key standards development organizations (SDOs) such as the International Telecommunications Union (ITU), dubbed by one expert as ‘the most important UN agency you have never heard of’.

Proposals for a decentralized internet infrastructure threaten global ICT interoperability and have serious consequences for human rights: China’s proposals may facilitate the implementation of its social credit scheme. And since the launch of its Belt and Road Initiative (BRI), and 2035 Standards Strategy, Chinese proposals to reshape standards have gained momentum, as well as some support from its trusted trade partners.

To complicate matters further, ITU secretary general Zhao Houlin is known to favour China-backed proposals and, with US candidate Doreen Bogdan-Martin likely pitted against Russia’s Rashid Ismailov in the ITU 2022 plenipotentiary, stakes have never been higher. Ismailov is a former Huawei executive and, for Russia, the ITU presidency offers a unique opportunity to champion its vision for closed, nationally-controlled internet; for example, by supplanting ICANN, the current group coordinating internet addresses.

But these threats run deeper than just Russia and China. Globally, there are a diversity of regimes with long-term, vested interests in shaping standards for their own benefit, willing to throw their weight behind China’s proposals. Like-minded democracies must urgently rethink their approach to standards – and a multi-stakeholder strategy could offer a solution.

What more stakeholders bring to the table

To assist G7 partners in their preparation for the Ministerial Declaration, experts at the Chatham House-DCMS workshop (held on 3 March 2021) recognized that multi-stakeholderism encourages coalition-building, nurtures local and cross-border innovation, and bolsters shared normative commitments to safeguarding the transparency, openness and interoperability of ICTs.

For years, industry has dominated efforts to shape digital technical standards, with everyday tech items and their standards, such as USB specifications, developed by coalitions of ICT companies. But new challenges demand new approaches. ICT giants offer technical expertise and digital leadership experience, but it is time to broaden the field.

Governments have always played a role in standards development, with the power to identify policy issues, facilitate partnerships, and provide financial incentives, but the G7 declaration signals a reimagining of government responsibilities vis-à-vis industry’s leadership. At a national level, governments can lead strategic coordination and invest in capacity-building for non-state actors, while internationally, governments can encourage coalitions between stakeholders.

The G7’s declarations on ICTs are steps in the right direction, as are national standards strategies such as Germany’s Standardisation Roadmap on AI, and the UK’s focus on standards in the Integrated Review. But non-state actors also have a legitimate, urgent role to play. In the past, knowledge gaps, financial barriers, and a lack of incentives have prevented sustained engagement from civil society and academia in SDOs.

These actors bring much to the table, such as technical expertise, existing networks, and under-represented voices, such as young adults and children. Plus, they already raise awareness about the importance of certain standards, and serve as barometers for their societal impact.

It may be easy to forget that the SDOs themselves are also stakeholders, setting the tone for inclusion, coordination, and engagement, so their leadership and norms matter. US Secretary of State Anthony Blinken noted there are ‘relatively few items that are ultimately going to have a greater impact on the lives of people around the world’ than the ITU leadership race.

Why multi-stakeholderism matters

From a technical standpoint, the more perspectives involved in determining technical interoperability, the better – especially with the onset of disruptive technologies such as quantum and AI which are likely to have a wide, societal impact. Building deeper knowledge-sharing networks between academia and SMEs can generate resilient standards that reflect policy principles.

But more importantly, multi-stakeholder approaches build cross-sector and cross-border coalitions rooted in normative commitments to open, democratic societies and enhancing shared prosperity. Meaningful engagement on standards with a variety of stakeholders at national and regional levels is even more urgent for technologies with far-reaching societal impacts – such as smart cities and autonomous vehicles – to avoid societal harms.

By championing open, transparent, consensus-based multi-stakeholderism in standards-setting, states bring home more than just majority votes on key proposals. Changing ICT culture by institutionalizing multi-stakeholderism and diverse representation would generate good practices which can be replicated in areas such as the UN cybercrime treaty deliberations proposed by Russia to supplant existing agreements, and negotiations on responsible state behaviour in cyberspace.

There is a long way to go, as states still need to develop effective outreach mechanisms and invest in coordination at all levels, and there are clear trade-offs between stakeholder inclusion and the efficiency of expert groups.

But faced with some states’ aspirations to shape the internet, telecoms, and emerging technologies, like-minded states interested in protecting open, democratic societies cannot afford to adopt a siloed approach to digital technical standards. Multi-stakeholderism is both urgent and necessary – before it is too late.

#### Global ICT interoperability prevents extinction from disease, food, and environmental collapse

N. Kishor Narang 20, Research Advisor at the Institute of Informatics and Communication at the University of Delhi, Member of the Academic Council at D Y Patil International University, Member of the Academic Committee at Electronics & ICT Academy at National Institute of Technology, ““Protecting the Planet with Standards” ... Mentor’s Musings on the World Standards Day 2020.”, LinkedIn, 10/14/2020, https://www.linkedin.com/pulse/protecting-planet-standards-mentors-musings-world-day-narang

It has been observed that the technologies developed by human beings in the last two to three centuries have had a major impact on the earth’s climate and our nature’s equilibrium. Some believe that we have reached a point of no return. This can have a huge impact on life on earth, especially on the human species.

However, while technology has been responsible for most of it, technology also seems to have a solution for it.

The COVID-19 pandemic, a humanitarian challenge, has caused widespread disruption in the global business community. The issues involved in the pandemic are both nuanced and complex. Global business dynamics are going to witness a sea change in the coming times.

The COVID-19 crisis has upended urban life, as we know it. Cities are on lockdown, and the once bustling streets of Paris, New York, London, Rome, Bombay and more now sit virtually empty. Technology and Standards have been critical to the way cities and society have coped with the crisis. Online delivery companies have been essential for getting food and supplies to residents, while their restaurant delivery counterparts have helped keep restaurants up and running during the lockdown. Urban informatics has helped track the virus and identify infection hot spots. As cities begin to reopen, digital technologies are being leveraged to better test and trace the virus as well as to ready urban infrastructure, like airports, public transportation, office buildings, and businesses, to open back up safely.

Safety in the interconnected world - As organizations across the world ramp up their operations and strive to serve their consumers, they are also faced with increased cyber security threat. Cybercriminals can exploit the weaknesses and vulnerabilities to exploit the connected devices and the network itself. This presents a challenge to the cybersecurity teams who must learn to evolve with the evolving threat perception.

As work from home increases, users who don’t have the same quality of security ecosystem as at their offices are finding themselves to be the targets of directed phishing, smishing, vishing and ransomware attacks. Home Wi-Fi systems usually suffer from a low degree of protection and are presenting opportunities for hackers. Since more and more people are working from home, there is a fear that the ever-increasing number of IoT devices in the household are easy targets for hackers, who can use them as gateways to undermine the security of the larger systems they connect to.

Managing disruption during a global pandemic - The current health crisis which has gripped the world can be seen as an inflection point between Digital Transformation and businesses. It has also impressed upon various stakeholders to invest more robustly in digital technologies. It is also a challenge to the security planners who have to guard against security threats and also ensure business continuity. Hospitals must have emergency backup systems which ensure seamless continuity of operations and databases. Rogue nations and intelligence agencies who attempt attacks on healthcare facilities must be warned of immediate consequences.

The question most people would ask is – What do STANDARDS have to do with all this?

Although most people do not realize it, standards and the methods used to assess conformity to standards are absolutely critical. They are essential components of any nation's technology infrastructure—vital to industry and commerce, crucial to the health and safety of citizens, and basic to any nation's economic performance. About 80 percent of global merchandise trade is affected by standards and by regulations that embody standards.

Standards enable us to pre-solve complex problems.

International standards enable and provide society with efficient ways to get work done while maintaining the safety of producers who create and provide goods and services, as well as the end-users receiving the benefits from these goods and services. International Standards are an important instrument for global trade and economic development. They provide a harmonized, stable and globally recognized framework for the dissemination and use of technologies. Standards provide people and organizations with a basis for mutual understanding, and are used as tools to facilitate communication, measurement, commerce and manufacturing. Standards are everywhere and play an important role in the economy by facilitating business interaction.

Standards: details of "Mega" importance - The topic of standards and the challenge of effective standards development can bewilder, by immersing the uninitiated in a blizzard of details. To some degree, this is unavoidable. After all, standards are details. They specify characteristics or performance levels of products, processes, services, or systems.

Standards are becoming increasingly important due to several intensifying trends:

· the pace of technological innovation is quickening;

· trade volumes are growing faster than national economies; and

· business operations are globally distributed.

There is extreme pressure for the standards community to reckon fully with the realities of the brutally competitive, extremely fast-paced global economy. This is because standards are necessary complements of modern products, processes, and services. Standards can:

· promote industrial and market efficiency;

· foster international trade;

· lower barriers to market entry;

· diffuse new technologies; and

· protect human health and the environment.

Hence, it is critical to achieve worldwide use of International Standards and Conformity Assessment Services that ensure the safety, efficiency, reliability and interoperability of electrical, electronic and information technologies, to enhance international trade, facilitate broad electricity access and enable a more sustainable world.

Standardized protocols and regulatory controls will allow seamless sharing of information and data between various devices. This will help in managing security breaches and dealing quickly with them. Adoption of universal standards will result in faster and more efficient response to any future disaster or pandemic.

Since Standardization is a collective churning, deliberation & collaboration process, we need to moderate, as well as, expand our individual thoughts on any subject to make it acceptable globally.

Innovation and technology development are accelerating. Strategic plans and roadmaps are needed to help ensure that the market is suitably served with best practices that is pertinent to the goals and context of this very large market.

Standards support our need to balance agility, openness and security in a fast-moving environment. Standards provide us with a reliable platform from which we are able to innovate, differentiate and scale up our technology development. They help us control essential security and integrate the right level of interoperability. Standards help ensure cyber security in ICT and IoT systems.

The world has never been as competitive as today, yet cooperation is a must to deliver solutions for increasingly complex systems. No technical committee and no standards organization are able to single handedly develop all the Standards that are needed. We all need to work together.

Given the scale, moving forward cannot be successfully, efficiently, and swiftly accomplished without standards. The role of standards to help steer and shape this journey is vital. Standards provide a foundation to support innovation. Standards capture tacit best practices and standards set regulatory compliance requirements.

Covid-19 has brought us face to face with systemic problems, we have long chosen to ignore collectively: Inequalities, environmental degradation, hunger, poverty, oppression, and the digital divide. In this age of technological progress, many of us are tempted by the promising thought of quick technological fixes to these deeply-ingrained issues. But technology alone will not save us. We must put the well-being of people, communities, and the planet back at the centre. We need to ask ourselves: What are the futures we want to create? What do we value? What kind of world do we want to live in?

The socioeconomic disruption caused by COVID-19 will be a lasting one and poses a challenge to planners and leaders globally; a number of fundamental changes in policy and mindset are necessary. As we have already witnessed, because of interconnected trade and business, any future pandemic may spread rapidly globally and infect millions. Some countries may be less geared to tackle the crisis than others. But with challenges come opportunities. Marrying Human Intelligence and labor with Disruptive Technologies to find solutions is the way to go. Necessity is the mother of inventions and hopefully, public-private partnerships can lead to many new innovations. Without a collaborative approach, any global approach to deal with any future pandemic will be compromised. And, Standards shall play a crucial role in providing INTEROPERABILITY, SAFETY, SECURITY, RELIABILITY and last but not the least a comprehensive TRUST in the minds of procurers, users and citizens.

This pandemic has catapulted two diametrically opposite paradigms to the focus of the mankind – ‘Sustainability’ and ‘Digitalization'.

Facing the global pandemic, multiple nations have seen lockdowns, changed social interactions and challenging isolations. But in these testing times, nature has been our constant friend. From our windows to the world, we have been comforted by nature’s presence all around us — we have been delighted by the birdsong we can now hear. We have finally seen the sheen on the wings of a delicately fluttering butterfly, the industriousness of ants as they march by, the green-gold of trees as they sway in a magical breeze, the pink glow of dawn, the night’s coverlet of stars.

However, alongside appreciating nature’s beauty, we must also understand the lesson it is offering us now. The Covid-19 pandemic has been brought about by humanity disturbing nature’s ecological cycle. Similarly, climate change is being driven by humanity’s exploitation of nature as a captive resource — our constant need to consume more and more is consuming the very planet we call our home. As global temperatures, driven by greenhouse gas emissions, rise, we see the science manifest before our eyes. There is no eliding the truth of melting glaciers now, or rising oceanic levels, increasing land desertification, droughts and unseasonal storms. If we persist in damaging the environment in this way, scientists state, the pandemic may look small compared to the impacts of climate change.

This pandemic is a way of the Earth saying she has had enough of years of exploitation and excesses and needs restoring. Then again, it can be seen through another moral lens. It is evident that the pandemic is a counterstrike to our collective human consciousness that has been corrupted by indifference and culpability in sufferings across the world.

We may not yet know how this story ends, but we already know for sure that this pandemic has brought the greatest reversal of our times, turning the world along with its wisdom on its head… This is our freak chance to unlearn and learn. Let’s not blow it. So, why not re-visit our history and re-learn. Maybe we shall get an opportunity to re-calibrate our approach for defining and developing our future ways of leading lives… And, we still have a chance. Indeed, nature has given us an epochal opportunity to transform ourselves. Such transformation is possible at multiple levels.

Be it a drop in pollution & GHG emission or self-healing of the Ozone layer; the last few months have amply demonstrated the resilience of Mother Nature by reversing the damage mankind has done to the planet’s climate in last many decades due to sheer arrogance and complacence. It is now evident that widespread adoption of nature-inspired solutions will catalyse a new era in design and business that benefits both people and the planet. Let’s make the act of asking nature’s advice a normal part of everyday inventing. We can create solutions inspired by nature that even address the United Nations ‘Sustainable Development Goals’ (SDGs).

We need to develop sustainable solutions for a balanced ecosystem by empowering people to learn and apply nature-inspired strategies in design. We need to develop repositories of resources and launch design challenges where people learn by practicing, provide comprehensive support for bringing solutions to market, and create a conducive environment & platform for a global network of innovators. In short, together, we need to learn about, teach, and practice a radically different way to build our world.

We need to change how we think about technology and innovation. Rather than allowing technological advancement to steer our narratives, innovation and technology should help us build bridges between the worlds we inhabit now and the ones we imagine for tomorrow.

#### Splintering ICT interoperability causes de-globalization, hostile economic blocs and hot and proxy wars that go global

Dr. Nouriel Roubini 19, PhD in Economics from Harvard University, BA from Bocconi University, Former Professor of Economics at New York University's Stern School of Business, Chairman of Roubini Macro Associates, “The Global Consequences of a Sino-American Cold War”, Project Syndicate, 5/20/2019, https://www.project-syndicate.org/commentary/united-states-china-cold-war-deglobalization-by-nouriel-roubini-2019-05

Regardless of which side has the stronger argument, the escalation of economic, trade, technological, and geopolitical tensions may have been inevitable. What started as a trade war now threatens to escalate into a permanent state of mutual animosity. This is reflected in the Trump administration’s National Security Strategy, which deems China a strategic “competitor” that should be contained on all fronts.

Accordingly, the US is sharply restricting Chinese foreign direct investment in sensitive sectors, and pursuing other actions to ensure Western dominance in strategic industries such as artificial intelligence and 5G. It is pressuring partners and allies not to participate in the Belt and Road Initiative, China’s massive program to build infrastructure projects across the Eurasian landmass. And it is increasing US Navy patrols in the East and South China Seas, where China has grown more aggressive in asserting its dubious territorial claims.

The global consequences of a Sino-American cold war would be even more severe than those of the Cold War between the US and the Soviet Union. Whereas the Soviet Union was a declining power with a failing economic model, China will soon become the world’s largest economy, and will continue to grow from there. Moreover, the US and the Soviet Union traded very little with each other, whereas China is fully integrated in the global trading and investment system, and deeply intertwined with the US, in particular.1

A full-scale cold war thus could trigger a new stage of de-globalization, or at least a division of the global economy into two incompatible economic blocs. In either scenario, trade in goods, services, capital, labor, technology, and data would be severely restricted, and the digital realm would become a “splinternet,” wherein Western and Chinese nodes would not connect to one another. Now that the US has imposed sanctions on ZTE and Huawei, China will be scrambling to ensure that its tech giants can source essential inputs domestically, or at least from friendly trade partners that are not dependent on the US.

In this balkanized world, China and the US will both expect all other countries to pick a side, while most governments will try to thread the needle of maintaining good economic ties with both. After all, many US allies now do more business (in terms of trade and investment) with China than they do with America. Yet in a future economy where China and the US separately control access to crucial technologies such as AI and 5G, the middle ground will most likely become uninhabitable. Everyone will have to choose, and the world may well enter a long process of de-globalization.

Whatever happens, the Sino-American relationship will be the key geopolitical issue of this century. Some degree of rivalry is inevitable. But, ideally, both sides would manage it constructively, allowing for cooperation on some issues and healthy competition on others. In effect, China and the US would create a new international order, based on the recognition that the (inevitably) rising new power should be granted a role in shaping global rules and institutions.

If the relationship is mismanaged – with the US trying to derail China’s development and contain its rise, and China aggressively projecting its power in Asia and around the world – a full-scale cold war will ensue, and a hot one (or a series of proxy wars) cannot be ruled out. In the twenty-first century, the Thucydides Trap would swallow not just the US and China, but the entire world**.**

#### Proxy wars spill over, draw-in outside powers, and escalate to World War III

David Kampf 20, Senior PhD Fellow at the Center for Strategic Studies at The Fletcher School, MA in International Affairs from Columbia University, BA in Political Science from Bates College, “How COVID-19 Could Increase the Risk of War”, World Politics Review, 6/16/2020, https://www.worldpoliticsreview.com/articles/28843/how-covid-19-could-increase-the-risk-of-war

And by focusing solely on interstate wars, the optimists miss half the story, at least. Wars between states have declined, but civil wars never disappeared—and these internal conflicts could easily escalate into regional or global wars.

The number of conflicts in the world reached its highest point since World War II in 2016, with 53 state-based armed conflicts in 37 countries. All but two of these conflicts were considered civil wars. To make matters worse, new studies have shown that civil wars are becoming longer, deadlier and harder to conclusively end, and that these internal conflicts are not really internal. Civil wars harm the economies and stability of neighboring countries, since armed groups, refugees, illicit goods and diseases all spill over borders. Some 10 million refugees have fled to other countries since 2012. The countries that now host them are more likely to experience war, which means states with huge refugee populations like Lebanon, Jordan and Turkey face legitimate security challenges. Even after the threat of violence has diminished in refugees’ countries of origin, return migration can reignite conflicts, repeating the brutal cycle.

A Yugoslav Federal Army tank.

Perhaps most importantly, recent research indicates that civil wars increase the risk of interstate war, in large part because they are attracting more and more outside involvement. In a 2008 paper, researchers Kristian Skrede Gleditsch, Idean Salehyan and Kenneth Schultz explained that, in addition to the spillover effects, two other factors in civil wars increase international tensions and could possibly provoke wider interstate wars: external interventions in support of rebel groups and regime attacks on insurgents across international borders.

Immediately after the Cold War, none of the ongoing civil wars around the world were internationalized. According to the Uppsala Conflict Data Program, there were 12 full-fledged civil wars in 1991—in Afghanistan, Iraq, Peru, Sri Lanka, Sudan, and elsewhere—and foreign militaries were not active on the ground in any of them. Last year, by contrast, every single full-fledged civil war involved external military participants. This is due, in part, to the huge growth in U.S. military interventions abroad into civil conflicts, but it’s not only the Americans. All of today’s major wars are in essence proxy wars, pitting external rivals against one another. Conflicts in Syria, Yemen and Libya are best understood not as civil wars, but as international warzones, attracting meddlers including the United States, Russia, Saudi Arabia, Turkey, Iran, France and many others, which often intervene not to build peace, but to resolve conflicts in a way that is favorable to their own interests. These internationalized wars are more lethal, harder to resolve and possibly more likely to recur than civil wars that remain localized. It is not that difficult to imagine how these conflicts could spark wider international conflagrations. Wars, after all, can quickly spiral out of control.

As Risks Increase, Deterrents Decline

To make matters worse, most of the global trends that explained why interstate war had decreased in recent decades are now reversing. The theories that democracy, prosperity, cooperation and other factors kept the peace have been much debated—but if there was any truth to them, their reversals are likely to increase the chance of war, irrespective of how long the coronavirus pandemic lasts.

Democracy is often considered a prophylactic for war. Fully democratic countries are less likely to experience civil war and rarely, if ever, go to war with other democracies—though, of course, they do still go to war against non-democracies. While this would be great news if democracy and pluralism were spreading, there have now been 14 consecutive years of global democratic decline, and there have been signs of additional authoritarian power grabs in countries like Hungary and Serbia during the pandemic. If democracy backslides far enough, internal conflicts and foreign aggression will become more likely.

Other theories posit that economic bonds between countries have limited wars in recent decades. Dale Copeland, a professor of international relations at the University of Virginia, has argued that countries work to preserve ties when there are high expectations for future trade, but war becomes increasingly possible when trade is predicted to fall. If globalization brought peace, the recent wave of far-right nationalism and populism around the world may increase the chances of war, as tariffs and other trade barriers go up—mostly from the United States under President Donald Trump, who has launched trade wars with allies and adversaries alike.

The coronavirus pandemic immediately elicited further calls to reduce dependence on other countries, with Trump using the opportunity to pressure U.S. companies to reconfigure their supply chains away from China. For its part, China made sure that it had the homemade supplies it needed to fight the virus before exporting extras, while countries like France and Germany barred the export of face masks, even to friendly nations. And widening economic inequalities, a consequence of the pandemic, are not likely to enhance support for free trade.

This assault on open trade and globalization is just one aspect of a decaying liberal international order, which, its proponents argue, has largely helped to preserve peace between nations since World War II. But that old order is almost gone, and in all likelihood isn’t coming back. The U.N. Security Council appears increasingly fragmented and dysfunctional. Even before Trump, the world’s most powerful country ratified fewer treaties per year under the Obama administration than at any time since 1945.

Trump’s presidency only harms multilateral cooperation further. He has backed out of the Paris Agreement on climate change, reneged on the Iran nuclear deal, picked fights with allies, questioned the value of NATO and defunded the World Health Organization in the middle of a global health crisis. Hyper-nationalism, rather than international collaboration, was the default response to the coronavirus outbreak in the U.S. and many other countries around the world.

It’s hard to see the U.S. reluctance to lead as anything other than a sign of its inevitable, if slow, decline. The country’s institutionalized inequalities and systemic racism have been laid bare in recent months, and it no longer looks like a beacon for others to follow. The global balance of power is changing. China is both keen to assert a greater leadership role within traditionally Western-led institutions and to challenge the existing regional order in Asia. Between a rising China, revanchist Russia and new global actors, including non-state groups, we may be heading toward an increasingly multipolar or nonpolar world, which could prove destabilizing in its own right.

Finally, the pacifying effect of nuclear weapons could be waning. While vast nuclear arsenals once compelled the United States and the Soviet Union to reach arms control agreements, old treaties are expiring and new talks are breaking down. Mistrust is growing, and the chance of an unwanted U.S.-Russia nuclear confrontation is arguably as high as it has been since the Cuban missile crisis.

The theory of nuclear peace may no longer hold if more countries are tempted to obtain their own nuclear deterrent. Trump’s decision to abandon the Iran nuclear deal, for one thing, has only increased the chance that Tehran will acquire nuclear weapons. It’s almost easy to forget that, just a few short months ago, the United States and Iran were one miscalculation or dumb mistake away from waging all-out war. And despite Trump’s efforts to negotiate nuclear disarmament with Kim Jong Un’s regime in Pyongyang, it is wishful thinking to believe North Korea will give up its nuclear weapons. At this point, negotiators can only realistically try to ensure that North Korea’s nuclear menace doesn’t get even more potent.

In other words, by turning inward, the United States is choosing to leave other countries to fend for themselves. The end result may be a less stable world with more nuclear actors.

If leaders are smart, they will take seriously the warning signs exposed by this global emergency and work to reverse the drift toward war.

If only one of these theories for peace were worsening, concerns would be easier to dismiss. But together, they are unsettling. While the world is not yet on the brink of World War III and no two countries are destined for war, the odds of avoiding future conflicts don’t look good.

The pandemic is already degrading democracies, harming economies and curtailing international cooperation, and it also seems to be fostering internal instability within states. Rachel Brown, Heather Hurlburt and Alexandra Stark argue that the coronavirus could in fact sow more civil conflict. If this proves accurate, the increase in civil wars is likely to lead to more external meddling, and these next proxy wars could soon precipitate all-out international conflicts if outsiders aren’t careful. With the usual deterrents to conflict declining around the world, major wars could soon return.

#### The plan is goldilocks---antitrust enforcement over the gTLDs regulates ICANN without undermining its authority

Nelson Drake 18, J.D. from American University’s Washington College of Law and a B.A. in Political Science from Georgia College and State University, “Going Rogue: The National Telecommunications And Information Administration's Transfer Of IANA Naming Functions To ICANN,” 3 Admin. L. Rev. Accord 83, 2018, lexis

CONCLUSION

Since it was created and commercialized, the Internet, and more specifically the domain name space, has been a place for free thought and open competition. This environment was successfully maintained through quasi-governmental regulation by ICANN in conjunction with the NTIA. This model was problematic as the United States became increasingly pressured to relinquish its oversight role. 139 This pressure led to the NTIA relinquishing its control over the IANA functions and transferring them to ICANN, which was already administering them on a day-to-day basis. 140 Following this transfer, **ICANN became uniquely positioned to control the DNS** through one of these functions, specifically the power to delegate gTLDs to  [\*106]  DNS registries in the authoritative root zone. 141 These functions **made ICANN both the judge and jury regarding the delegation of gTLDs.**

This transition also marks the beginning of an era in which **ICANN behaves like a regulatory agency** and creates the potential for abuse by ICANN and its Board. Potential abuses would be difficult to prevent because **ICANN has removed itself from U.S. courts** by requiring disputes to be handled through arbitration. 142 In addition, with respect to trademark owners, trademark law would be an ineffective deterrent because of the USPTO's position that gTLDs are generic and inherently incapable of denoting source. 143

Antitrust law, under **Section 1 of the Sherman Act** or the essential facilities doctrine, could effectively regulate ICANN's power **without undermining ICANN's authority to regulate the DNS.** First, ICANN is not immune from antitrust liability because its actions play an important role in Internet commerce. 144 ICANN is also not immune from liability because of its agreement with the NTIA. Instead, a reviewing court must determine whether the actions at issue were necessary to meet the needs of that agreement. 145 Second, a review of relevant case law shows that a court could find that agreements involving the delegation of gTLDs could constitute an illegal restraint of trade under Section 1 of the Sherman Act. 146 Finally, although it has not been attempted, this paper theorized that ICANN could also be found liable under the essential facilities doctrine provided that a plaintiff could prove the factors laid out in MCI v. AT&T. 147

In addition, though a court can stop the delegation of a gTLD, it cannot force ICANN to award the gTLD to the complaining party. This means that **an antitrust claim would only prevent stakeholders from abusing ICANN's authority, not usurping it.** Thus, ensuring that a U.S. court does not simply replace the NTIA in its oversight capacity. Furthermore, it would not open ICANN to unnecessary lawsuits from corporate stakeholders seeking to unnecessarily challenge ICANN's authority at every turn.

Overall, the Internet is entering a new era of DNS regulation. This era  [\*107]  was entered suddenly and haphazardly, but that does not mean that it will yield negative results. There are upsides to having DNS management out of the hands of the United States government, although they are not discussed here. It would be foolish to allow this transfer to occur without examining possible regulatory alternatives in the absence of a body capable of overseeing ICANN's use of its authority. Thus, this paper concludes that one form of **regulation** would be **through antitrust law** to **ensure that the DNS continues to be a place of open communication, commercialization, and innovation into the future.**

## 2AC

### T Substantial---2AC

#### Substantial means considerable in a given context

Prost 4 (Judge – United States Court of Appeals for the Federal Circuit, “Committee For Fairly Traded Venezuelan Cement v. United States”, 6-18, http://www.ll.georgetown.edu/federal/judicial/fed/opinions/04opinions/04-1016.html)

The URAA and the SAA neither amend nor refine the language of § 1677(4)(C).  In fact, they merely suggest, without disqualifying other alternatives, a “clearly higher/substantial proportion” approach.  Indeed, the SAA specifically mentions that no “precise mathematical formula” or “‘benchmark’ proportion” is to be used for a dumping concentration analysis.  SAA at 860 (citations omitted); see also Venez. Cement, 279 F. Supp. 2d at 1329-30.  Furthermore, as the Court of International Trade noted, the SAA emphasizes that the Commission retains the discretion to determine concentration of imports on a “case-by-case basis.”  SAA at 860.  Finally, the definition of the word “substantial” undercuts the CFTVC’s argument.  The word “substantial” generally means “considerable in amount, value or worth.”  Webster’s Third New International Dictionary 2280 (1993).  It does not imply a specific number or cut-off.  What may be substantial in one situation may not be in another situation.  The very breadth of the term “substantial” undercuts the CFTVC’s argument that Congress spoke clearly in establishing a standard for the Commission’s regional antidumping and countervailing duty analyses.  It therefore supports the conclusion that the Commission is owed deference in its interpretation of “substantial proportion.”  The Commission clearly embarked on its analysis having been given considerable leeway to interpret a particularly broad term.

#### gTLDs are ‘substantial’

Arif Ali 16, JD from the New York University School of Law, BA from Columbia University, Lawyer and Co-Chair of the International Arbitration Practice at Dechert LLP, “Accountability and Transition in ICANN’s New gTLD Program”, JD Supra, 8/18/2016, https://www.jdsupra.com/legalnews/accountability-and-transition-in-icann-17101/

Bringing accountability to the Internet Corporation for Assigned Names and Numbers (ICANN), the little known yet hugely significant global regulator of the Internet domain name system, is always a significant victory. ICANN is currently expanding new top level domain names (TLDs) beyond familiar TLDs such as .com and .edu to hundreds of new domain names under the new gTLD Program. These TLDs involve high-profile public interests and are valuable resources, with companies competing to pay tens of millions of dollars at auction to win the right to operate them.

### Memo CP---2AC

#### Only notice and comment solves---regulatory capture over gTLDs ensures non-binding action is ignored---takes out the inducements plank

Fadi Chehade 14, President and CEO of expVC and former president of ICANN, “Domain Names Industry, ICANN, Regulatory Capture”, 9/29/14, http://www.expvc.com/2014/09/domain-names-industry-icann-regulatory.html

"... regulatory capture occurs because groups or individuals with a high-stakes interest [ICANN's high-stakes stakeholders--e.g., Registries, Registrars, and Registry service providers] in the outcome of policy or regulatory decisions can be expected to focus their resources and energies in attempting to gain the policy outcomes they prefer, while members of the public, each with only a tiny individual stake in the outcome, will ignore it altogether.[1] Regulatory capture refers to the actions by interest groups when this imbalance of focused resources devoted to a particular policy outcome is successful at "capturing" influence with the staff or commission members [i.e., ICANN groups, committees, Board of Directors] of the regulatory agency [ICANN], so that the preferred policy outcomes of the special interest groups are implemented..." (source: Wikipedia, supra)

Regulatory economics – Wikipedia: "... Countering, overriding, or bypassing regulation is Regulatory Capture where a regulatory agency created to act in the public interest, instead advances the commercial or special concerns of interest groups that dominate the industry that the agency is charged with regulating. The probability of regulatory capture is economically biased, in that vested interests in an industry have the greatest financial stake in regulatory activity and are more likely to be motivated to influence the regulatory body than dispersed individual consumers, each of whom has little particular incentive to try to influence regulators. Thus the likelihood of regulatory capture is a risk to which an agency is exposed by its very nature..."

This is a well-known flaw at the heart of multistakeholderism. To paraphrase George Orwell, within ICANN, all stakeholders are equal, but some are more equal than others. ICANN's high-stakes stakeholders with vested interests--e.g., domain name registry operators, service providers, and registrars--have "captured" the organization, dominate its decision-making, policies and outcomes, Board of Directors, and are generally over-represented throughout its organizational structure. The most effective counter to powerful commercial vested interests are governments, but in the case of ICANN, governments are relegated to an advisory capacity except for the United States government which still holds "ultimate power and authority" by virtue of its agreements and contracts with ICANN. As for domain name registrants, who are the actual customers or consumers of domain names (and who pay a fee to ICANN included as part of the registration fee for each domain name), they have almost no representation within ICANN--there is no "Registrants Group" within the ICANN structure (unlike the multiple groups who represent registries (one for gTLDs, one for ccTLDs, etc.) and registrars. Unsurprisingly, ICANN's record of protecting domain name registrants from price-gouging and other abusive registry and registrar practices is almost non-existent. So much for the multistakeholder model of Internet governance as practiced by ICANN.

A good example of ICANN's capture by the Domain Names Industry is ICANN's new gTLDs program where ICANN, ridden with conflicts of interest at its highest levels, subverted the wider public interest in favor of the high-stakes stakeholders' interests.

#### Antitrust guidance fails AND no follow on.

Bill Baer 20; October 1; Visiting Fellow in Governance Studies, former Assistant Attorney General for Antitrust at the U.S. Department of Justice and Director of the Bureau of Competition at the Federal Trade Commission, J.D. from Stanford University; Testimony Before the United States House of Representatives, “Proposals to Strengthen the Antitrust Laws and Restore Competition Online,” <https://www.brookings.edu/wp-content/uploads/2020/05/Bill-Baer-10.1.20-Testimony-to-House-Antitrust-Subcommittee.pdf>

So where do we go from here? One strategy has the antitrust enforcers developing new policy guidance in areas such as vertical mergers, standard essential patents, and high tech platforms to nudge the courts towards a less skeptical view of the need for assertive enforcement. The joint DOJ/FTC Horizontal Merger Guidelines have, as I noted earlier, over time increasingly been relied on by the courts as providing a framework for determining whether the combination of two rivals risks harm to consumers and to competition.

There are at least two reasons to doubt whether reliance on that strategy will be sufficient. First, it took years for the courts to embrace the soundness of the merger guidelines—indeed more than a decade. Can we afford to wait that long? Second, there is no guarantee that the courts will embrace that new guidance. The mindset that antitrust enforcers are more likely to be wrong than right, and that as a result, we should at all costs avoid the risk of over-enforcement, is pretty well-entrenched in antitrust jurisprudence. Absent some further direction from Congress, those biases are unlikely to change.

#### Guidance gets rolled back AND even the possibility wrecks certainty

Dr. Simon F. Haeder 20, Assistant Professor of Public Policy at Penn State University, PhD in Political Science from the University of Wisconsin-Madison, and Dr. Susan Webb Yackee, Director of the La Follette School of Public Affairs and a Collins-Bascom Professor of Public Affairs and Political Science at the University of Wisconsin-Madison, PhD in Political Science from the University of North Carolina at Chapel Hill, “Policies that Bind? The Use of Guidance Documents by Federal Agencies”, Journal of Health and Human Services Administration, Volume 43, Issue 2, Fall 2020, p. 90-91

Given these distinctions, there are significant advantages and disadvantages to using guidance documents as policy tools. For instance, as suggested above, guidance document development is often seen as a faster, more flexible, and less proceduralized approach to policymaking than notice and comment rulemaking (Gluck et al., 2015; Mantel, 2009; Shapiro, 2014). Some observers may interpret these factors as advantages because they allow agencies to respond more nimbly to changing political circumstances or technical and scientific innovations. Less benevolent explanations may see the speed, as well as the reduced participation requirements attached to guidance documents, as a means to shield public policy development from necessary political oversight and public participation. Similarly, the ease of issuing guidance may be seen as an advantage on the one hand by allowing presidents to unilaterally move policy in the face of gridlock. However, on the other hand, as the bathroom guidance example above suggests, future presidents can relatively easily rescind previous guidances. As a result, one of the “costs” attached to policymaking via guidance documents is that they can result in a more volatile regulatory environment and with less certainty and predictability for regulated entities. In contrast, it is much more difficult to rescind a notice and comment rule is because it requires an agency to go through the full regulatory process (Kerwin & Furlong, 2018). Another way to consider the advantages and disadvantages of policymaking via guidance documents is to look at the human capital expenditures attached to these tools. As Shapiro (2014, 582) writes, policymaking via notice and comment rulemaking is much more “costly.” Agencies have to develop a robust written record to establish a political and, oftentimes, scientific basis for new regulations (West, 1995). Thus, the notice and comment process—which is closely policed by the courts—is intense in terms of agency resources. In contrast, the guidance document development process often requires less in terms of a written record and justification (Romano, 2019). This may be seen as a benefit to some, but to others, who believe that agency policymaking ought to only take place when a fully developed evidentiary record undergirds that decision-making, it may be seen as problematic.

#### Or, struck down

Sam Kalen 8, Visiting Assistant Professor at Penn State University, “The Transformation of Modern Administrative Law: Changing Administrations and Environmental Guidance Documents”, Ecology Law Quarterly, 35 Ecology L.Q. 657, Lexis   
Since 2000, the D.C. Circuit's decisions have become less predictable. In 2000, the court sent a strong message to agencies that increased reliance on guidance documents might prove problematic. It delivered this message in Appalachian Power Co. v. EPA, where the court held that it could review and vacate a CAA guidance document, because the agency had failed to follow APA notice-and-comment rulemaking. [79](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n79) One commentator at the time predicted that life after Appalachian Power could prove interesting, as the court suggested that a host of EPA guidance documents might succumb to the same fate. [80](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n80) Appalachian Power involved EPA's issuance of one of many guidance documents necessary to help inform the administration of the CAA. In 1992, EPA issued regulations requiring that certain air permits contain requirements for "periodic monitoring" of emissions. [81](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n81) The regulations left a number of issues unresolved and created uncertainty about the insertion of periodic monitoring requirements in CAA permits. Released in 1998, EPA's "Periodic Monitoring Guidance" (PMG) document sought to address the ambiguities in  [\*679]  the 1992 regulations. [82](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n82) Petitioners argued that EPA had impermissibly attempted to prescribe substantive rules through the guise of a guidance document, which had not been adopted in accordance with notice-and-comment rulemaking. [83](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n83) EPA responded by objecting to any challenge, claiming that the court lacked jurisdiction to hear the case because the guidance document was not a final rule. [84](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n84) Early in the opinion, Judge Randolph foreshadowed the tenor of the court's decision. Before discussing the merits, he observed:   The phenomenon we see in this case is familiar. Congress passes a broadly worded statute. The agency follows with regulations containing broad language, open-ended phrases, ambiguous standards and the like. Then as years pass, the agency issues circulars or guidance or memoranda, explaining, interpreting, defining and often expanding the commands in the regulations. One guidance document may yield another and then another and so on. Several words in a regulation may spawn hundreds of pages of text as the agency offers more and more detail regarding what its regulations demand of regulated entities. Law is made, without notice and comment, without public participation, and without publication in the Federal Register or the Code of Federal Regulations. [85](http://www.lexis.com/research/retrieve?cc=&pushme=1&tmpFBSel=all&totaldocs=&taggedDocs=&toggleValue=&numDocsChked=0&prefFBSel=0&delformat=XCITE&fpDocs=&fpNodeId=&fpCiteReq=&brand=&_m=74ac310076c537f12e8efe5a5d3fc51f&docnum=1&_fmtstr=FULL&_startdoc=1&wchp=dGLbVzW-zSkAA&_md5=93e9632651372cfab6b3ead4cfe76412&focBudTerms=The+phenomenon+we+see+in+this+case+is+familiar.+Congress+passes+a+broadly+&focBudSel=all#n85)

#### Courts will ignore guidance

HLR 20 – Harvard Law Review, “Antitrust Federalism, Preemption, and Judge-Made Law”, Harvard Law Review, 133 Harv. L. Rev. 2557, June 2020, Lexis

This is not to say that the FTC and DOJ do not have significant impacts on the development of federal antitrust policy. For one thing, the agencies choose when to enforce antitrust laws, thus affecting the kinds of cases and controversies that the judiciary sees. But the Sherman Act and the Clayton Act offer private rights of action, and states may sue as parens patriae under Hart-Scott-Rodino, so the agencies' enforcement [\*2576] decisions cannot completely control the law's development. Many seminal antitrust cases were decided without an agency party. Granted, even in suits not brought by an agency, the agencies can have significant sway: the executive branch often acts as amicus curiae, and courts sometimes base their decisions directly on the government's amicus briefs. And the FTC and DOJ publish enforcement guidelines that courts have found highly persuasive, even though those guidelines are non-binding and meant mainly as an expression of enforcement policy. For example, the "Merger Guidelines are for all practical purposes the law on merger liability." That being said, other enforcement guidelines have been far less influential -- some "have been cited only a handful of times each." In the end, although amicus briefs and guidelines may often win over judges, it is judges who make final decisions, and who sometimes ignore agencies.

#### It won’t be publicized

Cary Coglianese 20, Edward B. Shils Professor of Law, Professor of Political Science, and Director of the Penn Program on Regulation at the University of Pennsylvania Law School, and Public Member and Chair of the Rulemaking Committee of the Administrative Conference of the United States, “Illuminating Regulatory Guidance”, Michigan Journal of Environmental and Administrative Law, 9 Mich. J. Envtl. & Admin. L. 243, Spring 2020, Lexis

Based on the search results, four of the fourteen agencies appear to have no applicable statutory or regulatory provision that imposes an agency-specific requirement to make guidance documents publicly available (EPA, FTC, NHTSA, SEC). The remaining ten agencies were found to have either a statutory or regulatory provision that spoke to guidance availability by their agency either generally or with respect to specific guidance documents. Few agencies were subject to general [\*279] legal obligations with respect to guidance. Beyond FDA, only one other agency--DOT--was found to be subject to a statutory provision addressing publication of guidance generally across the agency. Outside of FDA, only five other agencies were found subject to such regulatory provisions that were general in scope. A total of five agencies were identified to have a statutory provision that required publication of a specific guidance; for six agencies, a regulatory provision on a specific guidance was found. Overall, most of the provisions addressed specific guidance documents (50 out of 63), and regulatory provisions (42) outnumbered statutory provisions (21) by a two-to-one margin.

#### CP links more to politics---GOP hates guidance documents

Bloomberg 11 – “Backlash Against ‘Guidance as Rulemaking' Leads to Actions in Federal Court, Congress,” July 15, 2011, online: http://www.bna.com/backlash-against-guidance-n12884902458/

The decision comes as the Obama administration faces a backlash from industry, Republicans in Congress, and state regulators over what they say is its pursuit of policy initiatives through guidance in lieu of rulemaking. Critics are challenging a practice—particularly on the part of EPA and to a lesser degree the Interior Department—they see as establishing new mandates without proper notice and comment.

The Clean Air Act document aside, EPA in the past 14 months has issued guidance to curb the impact of surface coal mining on water quality, to clarify which waters merit protection under the Clean Water Act, and to outline the best available technologies to curb greenhouse gases.

Interior, meanwhile, issued two guidance documents in June 2010 in the wake of the explosion at the Deepwater Horizon drilling rig in the Gulf of Mexico that required oil and gas companies to implement safety and environmental measures for drilling operations.

‘Poster Child' for Regulatory Overreach

EPA's actions have drawn the wrath of House Republicans. Appropriations Committee Chairman Hal Rogers (R-Ky.), speaking at a July 6 markup of the EPA appropriations bill for fiscal year 2012, said the agency has been “running roughshod” over every sector of the U.S. economy.

“This agency is the poster child for this Administration's widespread regulatory overreach, having vastly overstepped the authority granted by this Congress,” Rogers said.

Guidance, as defined by the Administrative Procedure Act, is a document that clarifies how an agency and its delegated state permitting agencies will interpret a law, such as the Clean Water Act or the Surface Mining Control and Reclamation Act, or it conveys administrative procedures to its various offices. A rule, unlike guidance, is a legally binding document that is subject to notice and comment.

### China DA---2AC

### 2AC---Soft Power AO

#### The plan restores US soft power globally

Justin Sherman 21, Contributor at WIRED, focused on technology and geopolitics, “Weak US Privacy Law Hurts America’s Global Standing,” 7/20/21, https://www.wired.com/story/weak-us-privacy-law-hurts-americas-global-standing/

One of the greatest foreign policy challenges posed by weak US privacy law, though, is that Washington loses credibility on democratic tech governance by purporting to fight digital repression globally while allowing data-enabled abuses at home.

Many authoritarian governments spin this reality right into what-about-ism, in which everything is hypocrisy and there is no difference between democratic and authoritarian countries. The Kremlin, for example, routinely uses problems in American internet policy to suggest that internet openness is nonsense and to justify the Russian state’s internet repression. So, to be clear, the weakness of US privacy law does not mean there’s no hope (there is), nor that criticisms of authoritarian technology abuses are baseless (quite the opposite). Government surveillance in the US is also not the same as that in Russia or China.

But among many other digital harms allowed in the US, the lack of data controls on US firms undermines American soft power. As much as the US government condemns data surveillance practices overseas, American citizens are still unprotected from rampant corporate data hoarding and selling at home. This undermines Washington’s credibility. Politicians vaguely speak of zero controls on corporate data collection in China (inaccurate), while not acknowledging that the US has virtually no corporate surveillance controls whatsoever; the US government campaigns against Indian data localization rules and continues labeling the GDPR a trade barrier while not presenting a positive, democratic alternative for a “better” privacy law. All the while, companies and government organizations keep teaming up to surveil American communities with poor or nonexistent oversight.

If the US is going to forge a realistic, attractive, democratic model of technology governance—one it can use to entice internet “swing states” and hold up against Beijing's and Moscow’s digital abuses—it needs to be privacy-proactive. Otherwise, the US fails to live up to the democratic ideal by failing to protect its citizens, especially its most vulnerable, from unchecked corporate data collection and sale. It also risks feeding into a post-Snowden view in Europe and elsewhere that the US is merely repeating its 2010-era “internet freedom” agenda when it speaks in the language of techno-democracy.

Citizens’ ability to lead a safe and democratic life in the digital age matters in and of itself, but it also matters for American foreign policy. Congress needs to investigate and hold hearings on the ways that US tech firms might also undermine US national security through their data practices. The unregulated brokering of US citizen data on the open market is one place to start.

In a globally connected world, US foreign policy cannot succeed without safeguarding the data and the rights of American citizens at home.

#### Extinction---solves every impact

Margaret Seymour 21, 2020 Lt. Gen. Bernard E. Trainor USMC Veterans Fellow at the Foreign Policy Research Institute, “Building Soft Power Back Better?,” 3/19/21, https://www.fpri.org/article/2021/03/building-soft-power-back-better/

Focusing on economic strength, alliances, and institutions and exporting American values and ideals are good starts to restoring American soft power abroad—a critical component of American leadership. In fact, the post-WWII world order, and, more recently, the post-Cold War international system with the United States emerging at the sole superpower, was only possible through U.S. soft power. Historically, the United States has maintained its power and influence abroad, in part, due to its appeal. This appeal must be restored.

This is not a call for a post-Trump 180, the path away from soft power and towards a hard power-dominant foreign policy is decades-long. True reinvigoration is going to require not only a criticism of the past four years, but also deep introspection on President Biden’s own contribution to the trend as a senator and vice president. In other words, building a smart power approach to foreign policy is going to take more than simply rejoining a few international accords or hosting some impressive state dinners. Frankly, it’s going to take more time than this administration has, even with the possibility of a second term. But if we take Biden at his promise to serve as a transitional leader, we can certainly start rebuilding the foundation of a foreign policy approach that will serve generations of Americans and citizens abroad for decades.

This starts with rebuilding relationships. Based on Biden’s picks for high-level positions, it appears that he understands the power of relationships, choosing long-term confidants and establishment experts. Biden values trust and interpersonal history—and this approach must be applied to international relations.

President Biden campaigned on his personal relationships with key international leaders, which is critical, but the administration must also craft relationships with populations and other non-state actors. While the new administration understands the potential threat from non-state actions, it would be well-advised to also consider the potential opportunities in non-state groups and craft a national security strategy that acknowledges the growing power and role of such groups. For example, this strategy must include a prioritization of immigration and refugee programs, such as the Special Immigration Visa Program. While the Trump administration infamously decreased the levels of immigrants admitted under this program, the United States has arguably never fulfilled its responsibilities to the men and women who have assisted missions in Afghanistan and Iraq. Not only should the Biden administration reintroduce the Iraqi Special Immigrant Visa (SIV) Program, but it also should offer a permanent fix to the Afghan program as well as create a new program to reward our allies in the Syrian conflict. Such programs would establish the United States as a leader in refugee rights and protections. The success of future conflicts will be heavily reliant on the ability to gain and maintain the trust of civilian populaces. Without interpreters, translators, and other host-nation citizens, the success of U.S. missions abroad would and will continue to be threatened. More than that, failing to uphold promises to allies abroad threatens American legitimacy and standing in the international community.

In the new world order described by the administration, these wicked international problems “respect no borders or walls, and must be met with collective action.” While the COVID-19 pandemic has made the increasingly global nature of the international order abundantly clear, biological disease isn’t the first challenge to transcend borders. Counterterrorism, the threat of nuclear war, economic structures, and climate change all present challenges not to a single state or region, but to an entire international structure. These problems can only be addressed with global solutions.

### Infrastructure DA---2AC

#### Won’t pass---Manchin won’t be persuaded

Hans Nichols 9/16, Political Reporter at Axios, “Scoop: Biden bombs with Manchin”, Axios, 9/16/21, https://www.axios.com/scoop-biden-bombs-manchin-b2b4acbd-24d0-40a3-ba6f-c0509e0e0224.html

President Biden failed to persuade Sen. Joe Manchin (D-W.Va.) to agree to spending $3.5 trillion on the Democrats' budget reconciliation package during their Oval Office meeting on Wednesday, people familiar with the matter tell Axios.

Why it matters: Defying a president from his own party — face-to-face — is the strongest indication yet Manchin is serious about cutting specific programs and limiting the price tag of any potential bill to $1.5 trillion. His insistence could blow up the deal for progressives and others.

Axios was told Biden explained to Manchin his opposition could imperil the $1.2 trillion bipartisan infrastructure bill that's already passed the Senate. Biden's analysis did little to persuade Manchin to raise his top line.

Manchin held his position and appears willing to let the bipartisan bill hang in the balance, given his entrenched opposition to many of the specific proposals in the $3.5 trillion spending package, Axios was told.

#### The plan is bipartisan

John D. Dingell 06, Former Democratic Representative from Michigan and longest serving member of Congress in history, “ICANN INTERNET GOVERNANCE: IS IT WORKING?”, House of Representatives Committee on Energy and Commerce, 7/21/06, https://www.govinfo.gov/content/pkg/CHRG-109hhrg31468/pdf/CHRG-109hhrg31468.pdf

ICANN continues to fall short in representing the interests of the broad Internet community. The last time, under your leadership, Mr. Chairman, this committee held a hearing on ICANN more than 5 years ago. Many serious questions were raised at that time. While ICANN has since made some progress in instituting reforms, several fairness, transparency and accountability issues and problems remain. Following the creation of the Internet in the U.S., ICANN was formed in 1998 as a global nongovernmental organization with guiding principles of stability, competition, bottom-up coordination and representation.

The Department of Commerce’s relationship with ICANN was under review at last year’s United Nations World Summit on the Information Society. With the bipartisan support of this committee and the Congress, attempts to shift Internet control away from the current framework were quelled. The international community instead reached consensus on maintaining a stable and secure Internet and continuing further dialogue on Internet governance. That said, we cannot allow U.S. interests to be put at risk by blindly ignoring ICANN’s flaws or failing to seek improvement for fear of global dissatisfaction. Indeed, I would worry that there may perhaps be more risk to us in ignoring than in proceeding to address this matter. As the Department negotiates an extension of the Memorandum of Understanding, further reforms must be sought. And the Memorandum of Understanding must be held up to the light for all to see and understand. ICANN remains far from a model of effective and sustainable self governance. It seems, however, to be a device which has a rich opportunity for prosperity and profit to some. Moreover, the Department should be sensitive that the manner in which the dot com registry contract is renewed bears on the integrity of ICANN and the Department itself.

#### But ICANN regs are apolitical and under the radar

Theo Lebryk 21, Yenching Scholar at Peking University Pursuing a Master's in China Studies, Graduated from Harvard University with a Joint Concentration in Social Studies and East Asian Studies and a Minor in Computer Science, Intern at the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies, “The Fight over the Fate of the Internet: The Economic, Political, and Security Costs of China’s Digital Standards Strategy”, China Focus, 4/21/2021, https://chinafocus.ucsd.edu/2021/04/21/the-fight-over-the-fate-of-the-internet-the-economic-political-and-security-costs-of-chinas-digital-standards-strategy/

Three months into Biden’s presidency, the new administration has already started to reverse many of Trump’s high profile exits from international institutions. The Biden administration has rejoined the Paris global climate accord and World Health Organization and looks poised to rejoin the UN Human Rights Council when it becomes eligible. While regaining America’s international stature may take some time, the Trump administration’s “Withdrawal Doctrine” appears to be more of a temporary blip than an important historical phenomenon.

However, there are important, albeit less flashy international arenas where the U.S. has lost ground to China, which transcend the Trump anomaly. Reversing China’s rise in these institutions cannot be accomplished with a simple executive pen stroke. Nowhere is this truer than the complicated world of digital standards and internet governance.

It is easy to think of the internet as simply working, but a great deal of work gets put into the standards, protocols, and rules which keep the World Wide Web running. In part because these debates are highly technical and seemingly apolitical in nature, internet governance institutions and standards development organizations often fly under the radar. In reality, considering how virtually every sector is increasingly reliant on the internet, the rules and standards of the Web have wide-ranging economic, political, and security implications.

The major digital innovations on the horizon – blockchain, 5G/6G, internet of things (IoT), AI – threaten to upend existing military, political, economic, and social paradigms. The direction of that impact is not predetermined. Blockchain, for instance, started with a promise of security, privacy, and independence, but has recently been put towards more Orwellian applications such as China’s social credit system. Internet governance institutions and standards organizations are becoming the battleground in determining how these digital technologies will be deployed and regulated.

The coming four years in internet governance will focus heavily on Huawei’s pitch to redesign the Internet, which it calls “New IP.” Huawei justifies this top-down redesign of the internet by arguing it is necessary to support these looming innovations. However, the political overtones of New IP are undeniable: if U.S. influence has eroded to the point where the proposal passes, it could create security backdoors for the Chinese government to exploit and codify Chinese censorship norms worldwide.

THE FREE INTERNET VS. CYBERSOVEREIGNTY

Having “invented” what eventually became the internet, the U.S. had a head start in determining the direction of the Web up until now. The U.S. government has generally supported a free, open internet while opposing censorship and excessive government regulation of the Web. The U.S. prefers to keep internet governance in the hands of multistakeholder organizations, where representatives from industry, academia, civil society as well as national governments have a say in decision making. By contrast, China supports multilateralism (national government-led governance, which is personified by the UN’s telecommunication arm, the International Telecommunication Union) and a more tightly regulated, censored internet. China’s general stance is that a national government should be able to control its domestic internet, which it calls “cybersovereignty.”

China has been pushing these norms for years, but only in recent years has it been able to pose a serious threat to U.S. interests. In recent years, America’s share of leadership and general participation in the ITU and ISO/IEC have dropped. In 2016, ICANN – the organization in charge of the Domain Name System (DNS) that therefore controls users’ ability to access URLs – left U.S. stewardship.

#### PC doesn’t solve OR deplete

Paul Waldman 20, Communication PhD at the University of Pennsylvania, Politics Columnist at the Washington Post. “Joe Biden has to move fast”, 12-2-20, https://www.washingtonpost.com/opinions/2020/12/02/joe-biden-has-move-fast/

As David Roberts of Vox observes: In 2009, Obama and his aides made the mistake of thinking that their major initiatives had to be rolled out one at a time in sequence, because he had a finite store of “political capital” that had to be spent carefully. But political capital is not something that exists apart from any particular issue; it isn’t a special sauce that has to be poured on a policy in order to make it palatable.

And with the parties as polarized and unified as they are, political capital has become all but meaningless. There may have been a time when a popular president possessed so much capital that a senator from the opposition party would feel compelled to support him on part of that president’s agenda, but that time is long gone. There is no account Biden can draw on to turn Republican “no” votes into “yes.”

So setting up a series of high-profile policy battles may be the opposite of what Biden should do. The unfortunate fact is that he may not have the opportunity to do much in the way of big legislation on health care or climate change or anything else, and if he has only executive power to work with, it makes it all the more urgent to move quickly.

Which means getting staff in place immediately and then unleashing them. The Revolving Door Project argues that Biden should give as much authority as possible to the agencies to let them dismantle their particular corners of the Trump legacy on their own, because the task “simply will not happen if approached sequentially or micromanaged” by a White House staff with limited bandwidth.

That means moving on every policy area all at once. There’s nothing to be gained by putting off any part of Biden’s agenda. Whatever he can do given the limits of his power, he should do as soon as possible, in a flood of policymaking.

Even if Democrats win both Georgia races and control the Senate, Biden should acknowledge that he likely has two years until the 2022 midterm elections to pass whatever legislation he can. Not only will Democrats probably lose one or both houses in the inevitable backlash (as happens to most presidents in their first midterm), the only possible chance at forestalling that result is to get results, as many as possible, that he can show the voters.

Republicans will complain that Biden is being partisan, uncompromising, taking a “my way or the highway” approach. It will be a strategy to convince everyone of the lie that Biden and Democrats might be able to find some way of winning them over, when in fact they’ll be implementing a strategy of total opposition.

If Biden follows them on that fruitless quest, he’ll be running in circles while crucial time passes and nothing gets done. The only option for him is to decide not to care about Republican whining and do what he got elected to do with all haste. The alternative is failure.

#### Federal spending decreases overall investment by trading-off with states and localities

D.J. Gribbin 19, Non-Resident Fellow at the Brookings Institution, Founder of Madrus, LLC, Former General Counsel of the U.S. Department of Transportation, “Three Reasons To Think Twice About An Infrastructure Bill”, Politico, 3/27/2019, https://www.politico.com/agenda/story/2019/03/27/infrastructure-funding-bill-000886/

In physics, Newton’s Third Law states that for every action there is an equal and opposite reaction. In policy, too, every action creates a reaction, albeit rarely equal or opposite. In fact, the challenge of policy is that reactions, while inevitable, are difficult to predict. When weighing federal expenditures on infrastructure, policymakers need to keep in mind that allocating more federal funds to infrastructure might backfire. Here are three ways that could happen:

The “coupon effect”

The prospect of federal funding can dampen state and local funding. While voters overwhelmingly support increased infrastructure spending, their strong preference is that someone else pay for it. This dynamic makes it difficult for state and local leaders (who own 90 percent of governmental infrastructure) to turn to their electorate and ask for a tax or fee increase if the federal government is offering “free” funding.

This dynamic can be called the “coupon effect.” Imagine if shoppers in the market for a new suit were told that there is a small likelihood they will receive a coupon for 80 percent off their next suit purchase. Consumers will rationally engage in what economists call strategic delay and postpone their purchase in the hope of receiving a coupon, even if the chance of getting the coupon is very small. Every time a consumer considers heading to the store and buying a suit, he will ask, “But what if a coupon arrives tomorrow?” As a result, many will continue to delay until their suits (or our infrastructure) become unacceptably shoddy and worn.

In my experience, the prospect of federal funding has this same impact on state and local leaders considering a tax or user fee increase to expand or improve the quality of their infrastructure. This dynamic was clearly apparent in Kentucky in 2014, for instance. That year, a candidate for the U.S. Senate encouraged the communities around the Brent Spence Bridge (connecting Cincinnati and Covington, Ky.) to oppose a toll increase, because if elected, she would get the federal government to pick up the $2.6 billion tab to replace the bridge. Her campaign successfully increased opposition to tolling. Yet five years later, the debate on how to fund the bridge is still unresolved, and the probability of full federal funding is still just about zero (notwithstanding the fact that the state is represented by the Senate majority leader, who is married to the Secretary of Transportation).

While further study needs to be done, the coupon effect could actually result in a net *decrease* in infrastructure funds, especially when coupled with the challenges of substitution; states and local governments receiving an influx of federal dollars frequently substitute the new federal dollars for funds previously allocated to infrastructure and transfer their dollars to other policy priorities. As a result, a dollar in new federal infrastructure spending does not necessarily result in an additional dollar available for infrastructure.

The current non-federal to federal ratio of infrastructure spending is 3:1. Thus, if a 30 percent increase in federal spending (along with celebrations that the coupon is in the mail) dampened by 11 percent non-federal spending increases, our nation would be left with a net national decrease in infrastructure funding.

#### Projects are slow---that accelerates short-term downturn

Ryan Bourne 17, MPhil in Economics from the University of Cambridge, R. Evan Scharf Chair for the Public Understanding of Economics at Cato, Former Head of Public Policy at the Institute of Economic Affairs – London, Former Head of Economic Research at the Center for Policy Studies, “Would More Government Infrastructure Spending Boost the U.S. Economy?”, Cato Institute Policy Analysis, Number 812, 6/6/2017, https://www.cato.org/policy-analysis/would-more-government-infrastructure-spending-boost-us-economy

Is Government Infrastructure Investment the Best Tool for Fiscal Stimulus?

Even if we accept that fiscal policy works as expected, a key question is whether infrastructure investment is the best mechanism for delivering a stimulus.

Keynesian economists frequently cite multiplier estimates suggesting government investment spending has significantly bigger effects than either tax cuts or government consumption spending.35 Yet much counterevidence is available. International Monetary Fund (IMF) analysis, for example, has found that government investment has largely indistinguishable multipliers from government consumption spending for open, flexible exchange rate countries or for highly indebted governments. In fact, a growing literature (primarily based on so-called narrative studies) suggests that tax-based stimulus programs may be more effective for short-term growth.36 More recent analysis also suggests that tax rate increases have far worse effects on output than public spending cuts in fiscal consolidation programs.37

One reason government investment spending might be an ineffective form of fiscal stimulus is that infrastructure projects have long lead times. Even if we accurately assess the “demand deficiency” of the economy, undertaking investment to coincide with a recession or slowdown is difficult. In the words of the IMF, infrastructure investments “require coordination among federal, state, and local governments and have to go through a long process of planning, bidding, contracting, construction, and evaluation.”38

Government-imposed constraints, such as land-use planning laws and environmental audits, often delay projects. President Obama realized that fact in relation to his stimulus program, acknowledging as far back as 2010 that “there’s no such thing as shovel-ready projects.”39 By the end of 2009, actual infrastructure spending was just 10 percent of that authorized for the year.40

Such delays can severely limit any positive effect of the spending and may even exacerbate the downturn. The expectation of productive government spending and hence higher living standards reduces work effort today, but if the project is delayed then that outweighs any positive effect on labor and output from the actual spending. In fact, the IMF attributes delays as a potential explanation to why President Obama’s stimulus package made much less of a dent on unemployment than expected. By the second quarter of 2010, President Obama’s economics team had expected the unemployment rate to have fallen to 7.5 percent. In fact, it was 9.6 percent.41 (Other factors might explain the difference between forecasts and outcomes, not least fiscal stimulus working less well than expected or the legacy effects of the financial crisis being more severe than believed.)

#### Fights are compartmentalized AND don’t spill over

Chad Pergram 18, Congressional Correspondent for FOX News Channel, 10/13/2018, “Amid Kavanaugh Cacophony, Congress Forges Bipartisan Agreements On Key Issues.” https://www.foxnews.com/politics/amid-kavanaugh-cacophony-congress-forges-bipartisan-agreements-on-key-issues

Step back from the Kavanaugh cacophony. Examine what lawmakers from both parties in both chambers accomplished in September and early October, with virtually zero fanfare.

Amid the turmoil, Congress approved the first revamp of national aviation policy in years. The Senate approved the final version of the legislation 93-6. This came after a staggering six extensions due to bickering and disagreement.

Then, Congress approved a sweeping, bipartisan measure to combat opioid abuse. The House okayed the package 393-8. The Senate adopted the measure 98-1.

And, there was no government shutdown. The House and Senate came to terms on two bipartisan bills which funded five of the 12 annual spending bills which operate the government. The sides agreed to latch an additional measure to one of the spending plans to fund the remaining seven areas of federal spending through December 7. President Trump briefly threatened to force a government shutdown if lawmakers didn’t include money for his border wall in the plan. But the President ultimately punted that battle until December. Democrats praised Republicans for keeping conservative “poison pill” riders out of the appropriations bills. That decision drew Democratic support for the measures.

The Senate approved a bipartisan water and infrastructure package.

McConnell hailed the bipartisanship which descended upon the Senate – even as the senators fought over Kavanaugh. Nearly in the same breath, McConnell derided boisterous, anti-Kavanaugh protesters outside the Capitol as a “mob.”

McConnell insisted this week he needed the Senate to clear a slate of 15 conservative judges to lower courts before he could cut senators loose for the midterm elections. McConnell and Schumer appeared at loggerheads. McConnell’s goal was clear: extract the confirmation of these nominees – or tether to Washington vulnerable Democratic senators from battleground states to keep them off the campaign trail.

Schumer knew McConnell would ultimately prevail on the nominees after the midterms. So the New York Democrat accepted McConnell’s ransom, permitting the Senate vote on a slate of nominees on Thursday night. Schumer also extracted a concession from McConnell: send senators home until November 13th.

One may wonder how lawmakers can find themselves in an imbroglio over a major issue like Kavanaugh – yet forge major bipartisan accords on other. Frankly, that’s just politics. Politics always elicits strange bedfellows. Successful lawmakers know they should compartmentalize their disputes. The enemy today may be your best ally tomorrow.

### AT: Cyber---2AC

#### There are still tons of gaps

David Smith 21, Vice President of Business Planning & Performance at National Grid, “The Grid in the Infrastructure Package – What’s In, What’s Out, What’s Next”, GridForward, 8/19/21, https://gridforward.org/the-grid-in-the-infrastructure-package-whats-in-whats-out-whats-next/

What’s Not In The Package

Demand-Side Flexibility

Demand response and wider demand side management capabilities are essentially not funded in the bi-partisan package. One section encourages utility demand side management considerations, but no real funding goes to bringing demand side resources on the grid. With the potential of FERC 2222 to bring aggregated demand side and distributed resources into markets, much more widely available and adopted controllable devices, and other market developments necessitating the type of resource coming on the grid, this is a bit striking.

Building Automation

Support to ensure that buildings have higher level controls and capabilities to respond to grid signals was also not in the package. See comments in demand side and DER integration above and below.

Distributed Resource Integration

It’s not a future state, but a current need, in which aggregated edge resources can provide significant value to the grid. Turning distributed assets (solar, storage, EVs, thermostats, generators, hot water heaters, and much more) into a resource requires new technology, evolved models, new partnerships and more. Support to help this transition is essential. When well established values can be equitably dispersed to owners and all grid customers (and for the benefit of the system itself), we will have reached a new milestone in the evolution of our energy system – the grid has not reached this place yet and investing to get there is critical.

Analytics & Digital Infrastructure

Real-time grid telemetry to better understand and optimize the dynamics of the system was essentially not in the package and is also not present in most parts of the grid. What’s the saying ‘you can’t manage what you don’t measure?’ Are there exciting things you can do with the roughly 70% of advanced meters that are now deployed? Absolutely! But additional investments are required to apply a suite of capabilities, largely powered by the cloud, to the grid and it’s time that we take them off the shelf and use them.

Renewable Energy

Remember that part of the grid that actually creates the energy we need to run our economy? There are a handful of minor areas of investment in targeted deployments and demonstrations here and there offering a few hundred million dollars. But this package does not help fund the build-out of clean energy resources, nor the grid capabilities to help facilitate it. Economics of resources like wind and solar in many jurisdictions are just so cost-effective that their additions have largely won out over recent years, but if we want a lower carbon society we have to dramatically expand renewable resources. And, importantly, we must build a grid that ensures affordable, reliable power gets to people and businesses when they need it. It seems that the reconciliation package may have central aspects to helping support the further build-out of clean energy resources, but if the IPCC report that came out this week didn’t wake you up to the needs I’m not sure what else may.

#### No cyber war or retaliation

Jasmine Rodet 18, Master’s Degree in Cyber Security, Strategy, and Diplomacy from the University of New South Wales, Cyber Security Program Manager at Fortescue Metals Group, “The Threat of Cyber War is Exaggerated”, 11/11/2018, linkedin.com/pulse/threat-cyber-war-exaggerated-jasmine-rodet/

For the regular person on the street, the term ‘cyber war’ is more likely to bring to mind the 1983 movie “WarGames” and the doomsday articles that appear regularly in the media about the ‘cyber battlefield’ and an impending World War III. This essay argues that the threat of cyber war is exaggerated and although it can, by definition, be stated that we are already in a state of cyber war, the impact on states is negligible compared to conventional war domains.

The argument is presented in 3 steps. The first step is to define cyber war and cyber weapons, referencing scholars and experts in the area of conventional war and the cyber domain. The second step is to explore who has been exaggerating the threat of cyber war and what their motivations might be. The third is to explore the evidence and quantify the probability and impact that cyberwar has had on states to date.

‘Cyber war’ is a term often used interchangeably in media with cyber-crime, cyber-attacks, cyber-conflict and cyber-incidents, creating confusion amongst the public and scholars alike. Clausewitz (1989, 75), in his book, On War, defines war as ‘an act of force to compel the enemy to do our will’. Rid (2012, 7) on the other interprets Clausewitz use of ‘force’ as meaning ‘violent’ force. According to Rid, if an act is not potentially violent, it is not an act of war. However, Stone (2013, 107) describes ‘cyber war’ as a politically motivated act of force, not necessarily lethal and not necessarily attributable. The definition by Powers and Jablonski states more simply that cyber war is the utilisation of digital networks for geopolitical purposes (Nocetti 2016, 464). Neither of the latter two definitions requires violence to qualify as cyber war. Under these definitions, the Stuxnet cyber-incident in 2010 and the Estonia incident in 2007 would constitute an act of cyber war, and as such we could say that nations have been at cyber war in the past and are likely to continue to engage in cyber war in years to come.

For this essay, I will use Stones definition to argue that even though states may engage in cyber war, the concept of cyber war is exaggerated. It seems that cyber war is deliberately exaggerated in the media and by politicians for financial and political gains. There are countless examples in the media and in politics of the exaggeration of the threat of cyber war and the language used plays a big factor in creating a sense of fear in the community.

The Four Corners report, Hacked, is a classic example where the reporter, Andrew Fowler describes the current situation in Australia as ‘… a secret war where the body count is climbing every day’ (Fowler 2013). The documentary reveals nothing violent or lethal about cyber incidents. The documentary is actually about hackers working from locations overseas, having targeted key Federal Government departments and major corporations in Australia.

In another example, NATO may be interpreted as exaggerating the threat of Cyber War when they invited Charlie Millar to present at their Conference for Cyber Conflict at the NATO Cooperative Cyber Defence Centre of Excellence in 2017. Millar is an independent security evaluator, and his presentation was titled ‘Kim Jong-il and me: How to build a cyber army to attack the US’. He later presented similar content at Def Con 2018. His presentation described the steps he would take to mount a cyber war, including the types of people he would engage, how much he would pay them, what his strategy would be and how much it would cost in total.

Who stands to gain from the exaggeration and hype? Logically, one group would be those that gain financially from the sale of cyber protective services and software. According to Valerino, 57% of technical experts surveyed said that we are currently in a cyber arms race and 43% said that the worst-case scenarios are inevitable (Valeriano and Ryan 2015). Translate this into sales and Gartner projects worldwide security spending will reach $96 Billion in 2018, up 8 Percent from 2017 and to top $113 billion by 2020 (Gartner 2017).

Additionally, there may be political motivations to exaggerate the threat of cyber war. Cyberspace is not well understood by the general public and fear is natural. In the US’s cyber security debate, observers have noted there is a tendency for policymakers, military leaders, and media, among others, to use frightening ‘cyber-doom scenarios’ when making a case for action on cyber security (Dunn 2008, 2).

There is some evidence to suggest that more recently in the political arena; we may be maturing in our understanding of the real threat of cyber war. The Tallinn Manual, an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare, was written at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence. It was first published in 2013 with the title ‘The Tallinn Manual on the International Law of Cyber War’. In 2017, it was re-released with the revised title ‘Tallinn Manual 2.0 on the International Law of Cyber Operations’. The change in title from ‘war’ to ‘operations’ signifies a more moderate use of language from NATO and is an acknowledgement that cyber incidents generally fall below the threshold at which International Law would declare them to be a formal act of war. Experience over the 4 short years from 2013 to 2017 has demonstrated that cyber incidents tend to have a low-level impact on the target state. As the book’s authors put it ‘the focus of the original Manual was on the most severe cyber operations, those that violate the prohibition of the use of force in international relations, entitle states to exercise the right of self-defence, and/or occur during armed conflict’ while the new version ‘adds a legal analysis of the more common cyber incidents that states encounter on a day-to-day basis and that fall below the thresholds of the use of force or armed conflict’ (Leetaru 2017).

To get a better sense if cyber war is exaggerated, we must also consider the probability of cyber war in the future. The probability of cyber war should be weighed up against the probability of conventional war. Where tensions are already high, for example, between North Korea and the US or Russia and Estonia, I would argue that cyber war is more likely than conventional war. This is due to factors including; cyber warfare is less costly than conventional warfare, states are less rational in their decision space in the cyber realm, states find cyber attribution very difficult to achieve so attacks can be undertaken covertly and cyber war is considered ‘a challenge’ and central to the hackers’ ethos (Junio 2013, 128). Further, Sanger describes in his book, The Perfect Weapon, cyber weapons (such as cyber vandalism, Distributed Denial of Service (DDOS), intrusions and advanced persistent threat (APT)) as the ‘perfect weapons’ for the following reasons;

They are cheap: When compared to Nuclear weapons, there are only a handful of nations globally that can afford the technology to create a nuclear weapon.

They are easily accessible: Unlike a Nuclear bomb that requires uranium, a highly protected metal, in the production process, a cyber weapon can be created with minimal investment and highly available IT infrastructure.

They can be dialled-up or dialled-down relatively easily. A ballistic missile, the force of the explosion cannot be adjusted as easily as a DDOS attack. A DDOS attack can be adjusted to last an hour, a few days or a few weeks.

They have a huge range in how they are used: Sabotage as with Stuxnet, Espionage as with the Chinese industrial spying on the US, North Korea’s infiltration of Sony, the Iranians attack on Las Vegas Sands Corp. casino operators.

The significant factor is that cyber weapons can and are being used every day for discrete, low-level cyber conflicts to undermine and disrupt rivals, but historically it has not progressed to open conflict, nor has it warranted a military response (Sanger 2018). Additionally, massive cyber operations would necessarily impact the civilian population and violate the immunity of non-combatants. The conditions of war dictate that this is “taboo” and to date, rival states have shown restraint in their use of cyber weapons for this reason (Valeriano and Ryan 2015). It appears that the threat that cyber weapons represent to national security is overstated and the threat of cyber war is overstated.

The US and likely other highly networked nations appear reticent about using cyber weapons for significant cyber conflict given their vulnerabilities. Ironically, NSA programs such as PRISM have made the US more of a target given the sheer volume of sensitive information stored in one place. Regardless of US defences, there is no way to make this information completely secure from intrusion, and as such, the very act of storing the information makes them more vulnerable.

Rid (2012) is among some academics who argue that cyber war has never and will likely never eventuate. The benefits of being on this side of the debate mean that public funding can be allocated away from offensive cyber security initiatives to other, potentially more important initiatives, such as public health and housing. The government is constantly under pressure to prioritise public spending and it is imperative that they have realistic, accurate projections regarding the risk of cyber war, the probability and the impact, to allow them to focus spending on the most important areas.

### DPA CP---2AC

#### DPA’s fail---Capture and delay

Neil Chilson 19, Former Chief Technologist, FTC; Senior Research Fellow, Technology & Innovation, Charles Koch Institute, "Creating A New Federal Agency To Regulate Big Tech Would Be A Disaster," Washington Post, 10/30/2019, https://www.washingtonpost.com/outlook/2019/10/30/creating-new-federal-agency-regulate-big-tech-would-be-disaster/.

Captured agencies don’t hold companies accountable; instead, they act to benefit the industry’s established players, disadvantaging newer firms and the public at large. In worst-case scenarios, such agencies can block new, disruptive competitors that threaten the established, regulated industry. The recent report from the Stigler Center holds up the Federal Communications Commission as an example of what a new Digital Authority could look like. But the FCC is a perfect example of the likely problems of an industry-specific regulator. At nearly every turn, with every new potentially disruptive communications innovation, the FCC (and its predecessor, the Federal Radio Commission) did the bidding of the best-connected incumbents. As former FCC chairman Michael Powell said, “[T]he history of the FCC is, when something happens that it doesn’t understand, kill it. We tried to kill cable. We tried to kill long-distance. When [MCI founder] Bill McGowan start[ed] stringing out microwave towers that threatened AT&T, the FCC tried to stop him. The FCC tried to kill cable because it was going to threaten broadcasting.” While it didn’t halt technological progress or competition, it often slowed it, occasionally by decades. For example, almost immediately after its creation, the Federal Radio Commission sided with industry players when it rejected the expansion of AM radio bands at the behest of existing commercial broadcasters. Later, the agency slowed the development of FM radio to protect AM radio manufacturers. It cracked down on early “community antenna television” (cable TV) to protect the broadcast television industry; conducted “beauty contests” to parcel out valuable broadcast licenses, sometimes to the politically connected (such as President Lyndon Johnson’s wife); and slowed approvals and imposed onerous regulations on satellite radio services to protect traditional radio stations. The FCC also transfers billions of consumer dollars between various telecommunication competitors in pursuit of several different connectivity goals — an exercise that brings everyone to Washington to petition the FCC for a share of the money. Thinking forward, the FCC’s history suggests that a single digital regulator would make it easier for existing companies to lobby for processes that restrict new competitors. Even regulations that are intended to promote competition could easily become barriers to new competitors. Similarly, new digital business models could be delayed or blocked by regulators who are too familiar with the existing way of doing things to imagine new pathways to success. Then there’s the question of price controls: Fixing prices with competitors is anticompetitive — unless the government is the one setting the prices. And where private price-fixing agreements are unstable (since it only takes one defecting party to ruin the agreement), government-mandated prices are conveniently government-enforced. A single digital regulator could provide a simple mechanism for guaranteed profits. Imagine a digital ad industry regulated like the FCC regulated the AT&T telephone monopoly for more than 40 years. So what is the alternative? As I noted earlier, regulators are less susceptible to the interests of individual companies and interests when they hear from a lot of different companies with a lot of different interests. Thus, generalist agencies that broadly regulate many industries are more resistant to capture. Further, agencies that primarily enforce laws (like the DOJ) are far less attractive targets for regulatory capture than those that mostly write rules (like the FCC). A company that manages to get in bed with the former might be able to dodge a lawsuit or put pressure on a competitor, but that pales before the possibility of influencing rules that reshape a company’s entire industry. In the United States, we already have an economywide enforcement agency: the Federal Trade Commission. Charged by Congress to promote competition and to protect consumers, the FTC has decades of experience addressing antitrust and consumer protection issues in the tech industry. Even now, it is pursuing investigations into digital companies under its current authority. And if new capabilities are needed to police digital companies, doesn’t it make sense to give such authority to an experienced agency that has been resistant to regulatory capture?

#### Wheeler is wrong

Lawrence J. Spiwak 21, President of the Phoenix Center for Advanced Legal and Economic Public Policy Studies. of the Phoenix Center for Advanced Legal and Economic Public Policy Studies, " A Poor Case for a ‘Digital Platform Agency’," Phoenix Center Perspectives, 21-02, 03/09/2021, pg. 3.

The Ability to Self-Define its Own Jurisdiction

Given the DPA’s eponymous title, the casual reader might assume that the DPA’s jurisdiction would be limited to large digital platforms such as Apple, Amazon, Google and Facebook. Not so.

The regulatory emphasis of the DPA is to impose a duty to deal upon those companies “deemed systemically important to society due to their economic dominance or essential nature.”21 “Systematic importance” centers around “whether network effects, economies of scale, economies of scope, power over data and similar factors have given certain companies excessive economic or social power, most often reflected by having a dominant position— bottleneck or gatekeeper control—over a key aspect of the digital market.” (Emphasis supplied.)22 (As a side, the Wheeler Proposal describes data as having “economics of scale,” but economies of scale are a property of a firm, not an asset.23)

There are two key aspects to “systematic importance” worth mentioning. First, the authors of the Wheeler Proposal contend that the DPA—and not Congress—should “determine what companies are systemically important in their social and economic impact.”24 As a general proposition, granting any regulatory agency such broad discretion to self-define what firms come under its jurisdiction based on a subjective standard of “systematic importance” is an invitation for mischief.25

Second, the only limiting principle to “systematic importance” is that “bottleneck or gatekeeper control” is required. The Wheeler Proposal bases its definition of “bottleneck or gatekeeper control” on the language used by the FCC in its 2015 Open Internet Rules (which is unsurprising given the authors’ professional history).26 Under such weak constraints (and given the preceding point that the DPA would have the ability to self-define which firms fall under its jurisdiction) it is entirely possible that members of the DPA would view their jurisdiction to reach far beyond “platforms” like Google, Facebook and Amazon, including core network providers such as AT&T and Comcast (who the FCC previously defined as “gatekeepers” in the 2015 Open Internet Order) as well as any other firm that operates as a “platform” (i.e., a firm in a two-sided market).27 Unquestionably, the authors of the Wheeler Proposal intend for the jurisdiction of their new DPA to be profoundly broad and encompass the entire Internet Ecosystem (and perhaps beyond).

## 1AR

### CP---1AR

#### Empirics prove ICANN capture

Kevin Ohashi 19, Head writer at Review Signal, “The Case for Regulatory Capture at ICANN”, Review Signal, 6/24/19, https://reviewsignal.com/blog/2019/06/24/the-case-for-regulatory-capture-at-icann/

Conclusion

The public interest is at best being represented, in majority, by people tied up in potential conflicts of interest in the given matter. At worst, it looks like special interest groups for VeriSign and The Internet Society(ISOC)/Public Interest Registry have captured multiple groups at ICANN and are trying to use it to line their organizations' pockets.

This appears to be a case study in regulatory capture. Beyond public outcry, there appears to be very little stopping ICANN from simply pushing through these contracts despite overwhelming evidence that the average internet user isn't in favor of these changes. There is virtually no meaningful argument in favor of removing price caps, unless you accept that it would be administratively easier for an organization with hundreds of millions of dollars in the bank. There is a bizarre free market argument that falls apart when you realize the cost of lock-ins for using a domain name and creating a web presence on any domain. .ORG is a thirty million dollar subsidy to the Internet Society (via PIR) which outsources, via competitive bid, the actual registry services. And they want the ability to charge more, at the expense of every other non profit. Their interests strongly align with VeriSign, who most likely see .ORG as the last hurdle before getting .COM and .NET to have price caps removed and increase their bottom line even more in their non competitive monopoly contract.

The only step left before these changes go into effect, that I am aware of, is board approval. I think it probably will go through unless there is a tremendous amount of attention brought to the issue. I'm not only concerned about price caps on .ORG, but structurally the only people who can invest so much time and money participating in ICANN are the organizations which stand to financially gain the most. Who is representing the public interest? Registry groups appear to have a strong voice within the ICANN community. Finally, I also worry about potential conflicts of interest at the board level, which has twenty members. Five ICANN board members were or are connected to ISOC (1,2,3,4,5). One is a former board member of PIR as well. I hope they recognize their responsibility to do what is right for everyone and not the select few registry operators in this instance.

#### It gets rolled back

Jack M. Beermann 3, Professor of Law and Richard L. Godfrey Faculty Research Scholar – Boston University School of Law, “Presidential Power in Transitions”, Boston University Law Review, December, 83 B.U.L. Rev. 947, Lexis

B. Nonlegislative Rules and Executive Orders

As noted above, there was no surge at the end of the Clinton presidency in the issuance of interpretive rules although there appears to have been an increase in some documents, such as guidances, that do not require notice and comment proceedings. 163 The reason for this may be very simple: in general, the APA requires the same process for revoking or revising a rule as is followed in its adoption. Therefore, a new administration can revoke or replace a prior administration's interpretive rules and policy statements simply by publishing notice in the Federal Register. Because interpretive rules and policy statements are not very durable, the outgoing administration may not find it worthwhile to take the trouble to issue them just so the incoming administration can revoke them a few days or weeks later.

#### Or ruled invalid

Stephen M. Johnson 12, Associate Dean and Professor at the Walter F. George School of Law at Mercer University, B.S. and J.D. from Villanova University, LL.M. from the George Washington University School of Law, “In Defense of the Short Cut”, University of Kansas Law Review, 60 U. Kan. L. Rev. 495, March 2012, Lexis

I. INTRODUCTION

Congress frequently gives administrative agencies a choice of several different tools - including legislative rulemaking, nonlegislative rulemaking, and adjudication - to interpret and apply the statutes that they administer. When Congress gives agencies a choice, courts rarely second-guess the agencies' choice of policymaking tool. Rarely, that is, unless the agency chooses to interpret a statute through nonlegislative rulemaking.

In theory, an agency should be able to announce an interpretation of a statute through a policy statement, interpretive rule, or other form of nonlegislative rule - often referred to more generally as "guidance documents" - without incurring the costs or delay of notice-and-comment rulemaking. As long as the agency does not treat that policy decision as binding and justifies the decision when applying it to a concrete factual situation, there should be nothing legally objectionable about the agency's action.

Nevertheless, regulated entities

and regulatory beneficiaries frequently challenge nonlegislative rules before the agency applies them, arguing that the policy decisions are really legislative rules and thus invalid because they were adopted without notice-and-comment procedures. In response, courts have fashioned a variety of unworkable [\*496] tests to distinguish between legislative and nonlegislative rules, and they have frequently struck down nonlegislative rules by characterizing them as invalid legislative rules that the agency should have promulgated through notice-and-comment procedures.

### DA---1AR

#### Manchin and Synema block it AND thumpers

Kevin McLaughlin 9/13, Journalist at The Information, “Kevin McLaughlin: Stop Biden's $3.5 trillion boondoggle – Manchin shows moderate Dems how to survive midterms”, Fox News, 9/13/21, https://www.foxnews.com/opinion/stop-biden-trillion-manchin-moderate-dems-kevin-mclaughlin

If Kyrsten Sinema was the first Democrat to breach the gates of the Biden administration’s domestic agenda, Joe Manchin kicked the door wide open and showed others the way.

Just before a weary nation paused for the holiday weekend, the West Virginia Democrat took a hatchet to the Democrats’ $3.5 trillion spending package, which has become the crown jewel on the lefts legislative wish list.

In a guest Wall Street Journal column, Manchin accurately accused the bill of having, "no regard to rising inflation, crippling debt or the inevitability of future crises" and said "ignoring the fiscal consequences of our policy choices will create a disastrous future for the next generation of Americans."

Of course, Manchin has perfected the kabuki dance of talking the moderate talk before falling in line with his party’s liberals. In 2021 alone, he cast the tie-breaking vote for Biden’s first $1.9 trillion spending package and the so-called For The People Act in June.

But if Manchin’s opposition is genuine, it marks the latest blow in a sea of setbacks for Biden. With his razor-thin congressional majorities, the president’s domestic agenda was already on thin ice. The fiasco in Afghanistan robbed Biden of precious political capital. Arizona’s Sinema has remained steadfast in her opposition.

#### That sinks the bipartisan bill too

Tyler Olson 9/13, Politics Reporter for Fox News, “'Squad' Dem Bowman doesn't rule out torpedoing infrastructure bill if Manchin doesn't budge on reconciliation”, Fox Business, 9/13/21, <https://www.foxbusiness.com/politics/bowman-manchin-democrats-infrastructure-reconciliation>

Progressive Rep. Jamaal Bowman Monday refused to rule out voting against the bipartisan infrastructure bill if Sen. Joe Manchin doesn't budge on his demand that Democrats' reconciliation bill cost $1.5 trillion or less – not even half the current $3.5 trillion price tag.

"We'll see when we get there," Bowman, D-N.Y., said on MSNBC when pressed about whether he would vote against a bill that costs significantly less than the $3.5 trillion number many left-leaning Democrats have said is their floor.

"But we still have several weeks, weeks of negotiation to make sure we are all on the same page before it's time to vote," Bowman added.

The comment from Bowman is similar to statements by many House progressives and "Squad" members in recent weeks that they'll vote against infrastructure if reconciliation doesn't pass. And progressives have been vocal that they want a $3.5 trillion topline number on the reconciliation bill.

But Bowman is among the first to be asked about what he would do on infrastructure if the reconciliation is downsized to placate moderates like Manchin, D-W.Va.

This is slightly different than other recent threats from progressives conditioning their votes for infrastructure on the passage of reconciliation without explicitly mentioning the price.

And Bowman's comment – days after Manchin's $1.5 trillion price demand became public – indicates progressives may be willing to sink one of President Biden's biggest priorities if they don't get their way on reconciliation.

#### But even if not, it won’t meet the deadline

Yueqi Yang 9/12, Financial Industry Reporter for Bloomberg News, and Rich Miller, Reporter at Bloomberg News, “Manchin Sees Delay in Congress for Vote on Biden’s Agenda”, Bloomberg News, 9/12/21, https://www.bloomberg.com/news/articles/2021-09-12/manchin-says-congress-can-t-meet-sept-27-goal-on-biden-s-agenda?srnd=premium

Senator Joe Manchin cast doubt on the timeline for pushing President Joe Biden’s economic agenda through Congress, suggesting that a late September target for a House vote on infrastructure spending is unrealistic.

Manchin, a Democrat whose vote is crucial in the evenly split U.S. Senate, renewed his objections to a $3.5 trillion plan that includes tax hikes and increases in social spending. He said he can’t support the price tag, doesn’t see the urgency and is concerned about inflation and the impact of higher corporate taxes on U.S. competitiveness.

With House Democrats seeking to move the package forward in tandem with a bipartisan $550 billion infrastructure bill that the Senate has passed, the West Virginia senator said he doesn’t see the lower chamber meeting a Sept. 27 deadline by Speaker Nancy Pelosi for a vote on the infrastructure plan.

“There’s no way we can get this done by the 27th -- if we do our jobs,” Manchin said on CNN’s “State of the Union” on Sunday. “There’s so much differences that we have here.”

Pelosi’s deadline is putting pressure on Democratic lawmakers to work out policy details to underpin the $3.5 trillion plan. Some of the divisions were on display in dueling interviews by Manchin and Senate Budget Committee Chair Bernie Sanders on the Sunday political shows.

#### Won’t pass—Pelosi and uncertainty

Matt 1NR Reese and Dale Minyo, 9/14/2021 (staff, Ohio’s Country Journal, “Infrastructure bill moving forward,” <https://ocj.com/2021/09/infrastructure-bill-moving-forward/>, Retrieved 9/16/2021)

From the local bridge just around the corner to the locks and dams on the nation’s river system, agricultural viability depends heavily on infrastructure. After months of across-the-aisle negotiations, the Senate voted to pass the bipartisan infrastructure package (H.R. 3684) in August. “This is a very notable move forward. It passed through the Senate with a very bi-partisan vote of 69-30, 19 Republican Senators voted for the legislation. Early on this year, the topic of infrastructure was really expansive. There were a lot of things being discussed that really don’t have a lot to do with what most Americans regard as infrastructure. It has tightened up and we think that is a good thing,” said Mike Steenhoek, executive director of the Soy Transportation Coalition. “We appreciate there are a number of categories within this legislation that, if they come to fruition, would be beneficial to agriculture. There is funding directed at roads and bridges, many in rural areas. There is some funding for our inland waterways and ports. For an industry like soybeans, we rely on robust exports and we have got to have the multi-modal transportation system that can connect our supply with that demand. We think there are some very favorable things in this legislation.” With Senate passage, attention now shifts to the House on this legislation. “Very little proceeds on time in Washington, D.C., but it is moving forward. The big question is: does the House adhere to Speaker Pelosi’s stated desire that this bill only gets passed if that $3.5 trillion reconciliation package which involves much more social spending also gets passed? There is still a lot of uncertainty related to this. Clearly there are Democrats and Republicans who support this legislation and it is clearly a priority of the president. It is a big bill. Hopefully it won’t get polluted by some of these more controversial topics.” If the infrastructure package does get passed, it will hopefully build on existing progress. “This bill would amplify what is already happening. We have a 5-year Highway Bill that was passed in 2015 and is scheduled to be re-authorized this year,” Steenhoek said. “Last year we had the Water Resources Development Act that paved the way for more funding for the inland waterway system. This is not our only shot for moving the needle on infrastructure. Things are getting done. You could argue that more needs to be done and that is what this bill aspires to do.” Along with the big picture infrastructure items, there are also some smaller provisions in the legislation that could benefit agriculture, including support for biobased products. “There is a provision that calls attention to biobased products that have infrastructure implications,” Steenhoek said.“Soy-based asphalt sealants and soy-based concrete sealants that are made largely from soil oil are a sustainable way to elongate the life of roads and bridges and provide another market opportunity for soybeans.” There is plenty to watch as this continues to move forward. “This is not a perfect piece of legislation, but we do think when you look at the links in the supply chain that are important to farmers, there are certain investment levels and actions that will improve the supply chain. Overall we look at this legislation favorably,” Steenhoek said. “I think there is a good chance that this does get passed, but as the days progress toward an election year, then the probability of anything getting passed goes down.”

#### The bills are tied

Grace Segers 21, Staff Writer at The New Republic, “The Congressman Behind the House Infrastructure Bill Is Miffed About the Bipartisan Deal”, The New Republic, 8/2/21, https://newrepublic.com/article/163149/peter-defazio-infrastructure-bipartisan-deal

“We are not moving their so-called bipartisan bill until we have reconciliation in hand passed by the Senate,” DeFazio said about the prospects of the Senate bipartisan infrastructure bill in the House. “At this point, we don’t know what will be in it, but hopefully we will fix some of the issues that have been created by this so-called bipartisan bill.”

A number of Democrats in both chambers have insisted that they are unwilling to support the bipartisan bill unless they get commitments that a larger measure, which includes more of their key priorities, follows in its wake. This second bill would necessarily have to be passed through the reconciliation process, a complicated maneuver that would allow it to be approved in the Senate without any Republican votes.

DeFazio reiterated the bipartisan deal “is not going anywhere” until House Democrats could see “what we can fix and improve in the reconciliation process before making any final judgments.” The Senate may vote on a budget resolution, which lays out the instructions for budget reconciliation, as soon as this week, but the House is in recess until the end of September.

#### Whip counts confirm

Julia Rock 9/15, Reporter for The Daily Poster, “Whip Count: The Democrats Who Support The Progressive Reconciliation Strategy”, The Intercept, 9/15/21, https://theintercept.com/2021/09/15/democrats-reconciliation-infrastructure-whip-count/

The progressive strategy, which has been endorsed by House Speaker Nancy Pelosi and President Joe Biden, has been to pair the bipartisan infrastructure bill with the larger reconciliation package — either both pass or neither do. In August, a group led by Rep. Josh Gottheimer, D-N.J., backed by the dark-money group No Labels, successfully split the two packages apart by winning a promise of a vote on the bipartisan bill on September 27. In order to keep the two together, progressives must either complete work on their larger bill by that date, or defeat or stall the bipartisan bill on September 27. Gottheimer was offered a vote, not passage, after all.

Backers of the bipartisan bill say they expect Republican support to be in the low double digits; Rep. Henry Cuellar, D-Texas, pegged it at 10 to 12 in August, though that number may have fallen as Minority Leader Kevin McCarthy and former President Donald Trump have been discouraging Republicans from giving Democrats a win.

The math is straightforward: Democrats have a four-seat majority, so adding 12 Republicans gives a cushion of 16 votes — meaning progressives have just enough committed “no” votes for a razor-thin margin. Dozens of Democrats did not immediately respond to our request for comment, so the figure of 17 may undershoot the count, and this article will be updated as new responses come in. The Congressional Progressive Caucus has previously said that it has the private commitments of a majority of their 95 members for the two-track strategy.

“There are a lot more but not everyone is ready to be public,” said Rep. Pramila Jayapal, D-Wash., chair of the CPC. “We had the majority of our caucus in our previous whip counts and we expect the same now. We will release names later if we have to. But I feel confident of our numbers.”

#### Biden statements prove AND won’t pass

Mary C. Curtis 9/10, Reporter and Editor at The New York Times, interviewing Norm Ornstein, American political scientist and a resident scholar at the American Enterprise Institute, “Explaining reconciliation and the social issues at stake, with Mary C. Curtis”, 9/10/21, https://www.rollcall.com/2021/09/10/explaining-reconciliation-and-the-social-issues-at-stake-with-mary-c-curtis/

At one point, President Biden made ... I think you could say at least a political mistake in saying he would not sign the bipartisan bill unless it came simultaneously with this broader reconciliation bill. Republicans revolted and he stepped back a little bit and they were able to get the support in the Senate for that bipartisan package. But in the House, some of the more moderate Democrats said, we don’t want to join these bills at all, we have an urgent need for that bipartisan bill [to get] passed or we won’t vote for anything. And the compromise that Speaker Pelosi worked out was they would pass the budget resolution, which sets the table for reconciliation, and guarantee a vote on that bipartisan package by Sept. 27.

Now, in the meantime, the Senate is trying to work out some compromise on that reconciliation package that will get the 50 votes that they need. And they’re only going to get them from Democrats. And of course, we know that there are some Democrats, Joe Manchin, in particular, and Kyrsten Sinema, who are revolting against that large package. And now we’re waiting to see whether they can bring that package together. If not, we will get that vote on Sept. 27. And if I had to guess right now, my guess is that progressive Democrats will not vote for the bill. And then we’ll have to wait and see what happens with the two packages and whether they can work something out that will satisfy all the Democrats.

#### Approval rates thump

Alexander Bolton 9/8, Senior Reporter at The Hill, “Biden's muscle questioned amid falling polls”, The Hill, 9/8/21, https://thehill.com/homenews/senate/571190-bidens-muscle-questioned-amid-falling-polls

President Biden’s sagging approval ratings, especially among independents, are raising questions about his ability to move his agenda through a House and Senate where centrist and liberal Democrats are battling one another.

Democrats aren’t running away from the president, but the approval rating hit could make it tougher for Biden to muscle moderates such as Sens. Kyrsten Sinema (Ariz.) and Joe Manchin (W.Va.) who are balking at the $3.5 trillion cost of his budget reconciliation measure.

#### It’s uniquely bipartisan and outweighs the link---it cements internet freedom, checks ICANN mission creep, and prevents foreign capture

Simon Rosenberg 15, President and founder of the progressive think tank NDN, “Who Controls the Future of the Internet?”, U.S. News, 2/6/15, https://www.usnews.com/opinion/articles/2015/02/06/congress-must-be-involved-in-the-icann-iana-internet-transfer-of-power

Among the more promising contributions to this still nascent debate came last week in a proposal from GOP Sens. Orrin Hatch of Utah and Roy Blunt of Missouri and Democratic Sens. Chris Coons of Delaware and Mark Warner of Virginia. In it they lay out seven reasonable conditions ICANN must meet prior to the transfer, including that the institution itself must become more accountable to the stakeholder community (one way to do this is to have formal “members” representing the various constituencies). It is not only a smart contribution to the debate, but that it was bipartisan puts ICANN and the administration on notice that Congress is now forcefully moving into the debate about how to keep the Internet open and free. And for good reason: In recent months there have been legitimate reasons for concern about institutional mission creep and foreign government capture of ICANN, something the U.S. simply cannot allow.

#### There’s been consistent bipartisan consensus for years

Phillip Corwin 09, Founding principal at Virtualaw LLC, “Congressional ICANN Oversight Hearing Has A Bipartisan Theme – It’s Too Soon To End U.S. Oversight”, Internet Commerce Association, 6/5/09, https://www.internetcommerce.org/congressional-icann-oversight-hearing-has-bipartisan-theme-its-too-soon-end-u-s-oversight/

What does all this mean for the termination or extension of the JPA? Too much should not be read into this particular episode because many Congressional hearings involve dramatic posturing and it is the Obama Administration, not Congress, which will make the ultimate call. But the strong bipartisan concern about the inconsistency

Mkd

of ICANN’s rhetoric with the reality of its performance is hardly confined to this Subcommittee – on May 19th, Senators Olympia Snowe and Bill Nelson, both serving on the Senate Commerce Committee, sent a joint letter to Commerce Secretary Gary Locke expressing the view that “ICANN has considerable work ahead to reach the point where it can stand alone as a stable, accountable, transparent and, most importantly, secure global organization” and essentially endorsing the view that the JPA be at least temporarily extended “to allow time to design and deploy new accountability mechanisms for ICANN”. Post-hearing press reports indicate that Chairman Boucher will be joining other Committee members in their own letter to the Commerce Department recommending a one-year extension.

#### It won’t be publicized OR noticed

Ed Vaizey 16, Contributor at Tech Crunch, Former Minister in the UK Government, Responsible for Digital and Technology Policy, “ICANN’s Globalization Creates Peril and Promise”, Tech Crunch, 9/2/2016, https://techcrunch.com/2016/09/02/icanns-globalization-creates-peril-and-promise/

In a quiet blogpost, Larry Strickling, the US government’s assistant secretary for communications and information announced that he had “informed ICANN…that…[the US government] intends to allow the IANA functions contract to expire as of October 1”.

mkd

That sentence may not mean a whole lot to many people, but this move is of huge global significance in how the internet is managed and governed.

ICANN is the Internet Corporation for Assigned Names and Numbers, a private non-profit organisation based on the west coast of the United States.

It’s not responsible for running the internet entirely, of course (no one is) but it’s an important – vital – part of the jigsaw. It’s responsible, in effect, for maintaining the internet. Without an organization like ICANN, and the IANA (Internet Assigned Numbers Authority) function it undertakes, we wouldn’t have domain names and IP addresses.

For almost twenty years, ICANN has carried out its functions on the basis of a contract with the US Department of Commerce, who set it up to formalize the process for managing domain names.

But ICANN’s future is part of a much wider debate about how the internet is governed. For something that is now so fundamental to how our world works, it is surprising how little this debate has actually played out in the mainstream.

In effect, the internet is “governed” by the Internet Governance Forum – the IGF – which was set up just over ten years ago, and had its mandate renewed last year. Its council is a multi-stakeholder advisory group, with a mix of representatives from government, civil society, business and academia.

It remains pretty fluid and informal, and very much under the radar. It meets once a year, in a different country, for about a week. Several thousand people attend, but there are regional IGF meetings throughout the year. Being part of the IGF tour can almost be a full time job for many people.